MapReduce Service

Guía del usuario

Edición	01
Fecha	2025-02-26

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Marcas registradas y permisos

El logotipo HUAWEI y otras marcas registradas de Huawei pertenecen a Huawei Technologies Co., Ltd.
Todas las demás marcas registradas y los otros nombres comerciales mencionados en este documento son propiedad de sus respectivos titulares.

Aviso

Es posible que la totalidad o parte de los productos, las funcionalidades y/o los servicios que figuran en el presente documento no se encuentren dentro del alcance de un contrato vigente entre Huawei Cloud y el cliente. Las funcionalidades, los productos y los servicios adquiridos se limitan a los estipulados en el respectivo contrato. A menos que un contrato especifique lo contrario, ninguna de las afirmaciones, informaciones ni recomendaciones contenidas en el presente documento constituye garantía alguna, ni expresa ni implícita.

Huawei está permanentemente preocupada por la calidad de los contenidos de este documento; sin embargo, ninguna declaración, información ni recomendación aquí contenida constituye garantía alguna, ni expresa ni implícita. La información contenida en este documento se encuentra sujeta a cambios sin previo aviso.

Índice

1 Preparación de un usuario

1.1 Configuración de permisos de servicio en la nube

La consola de MapReduce Service (MRS) puede interactuar con los clústeres MRS para proporcionar funciones relacionadas y supervisar el estado del clúster. La asignación de permisos es necesaria cuando se utiliza MRS por primera vez.

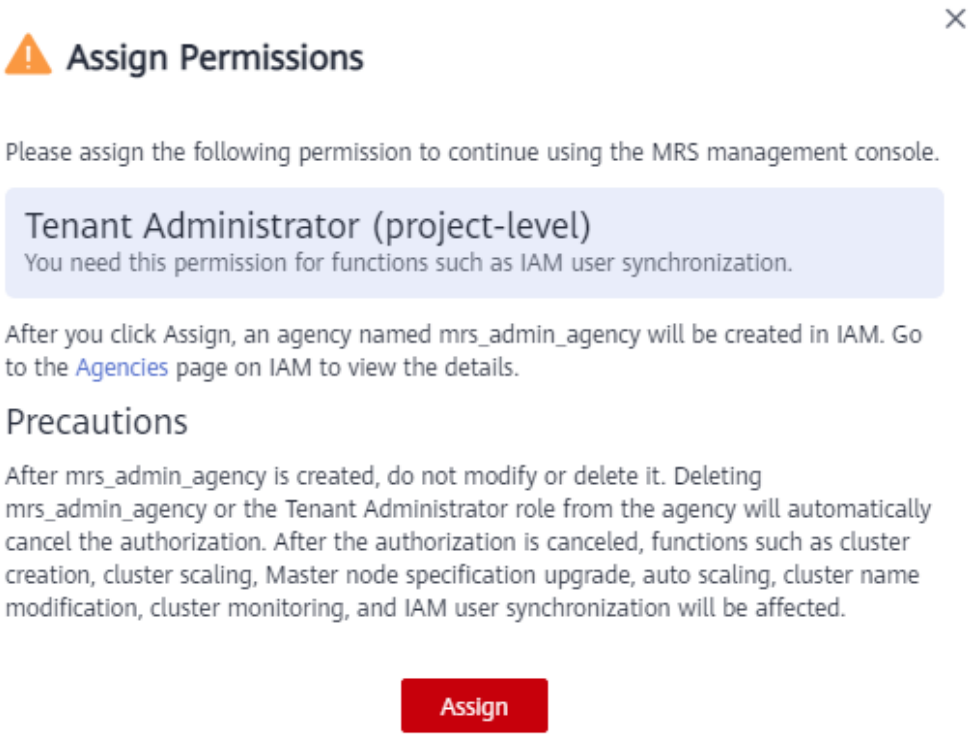
Después de la asignación de permisos, MRS crea una delegación llamada **mrs_admin_agency** en Identity and Access Management (IAM). Una vez creada la delegación, no la modifique ni la elimine. La eliminación de la delegación o el rol de Tenant Administrator en la delegación cancelará automáticamente la asignación de permiso. Si se cancela la asignación de permisos, se verán afectadas funciones como la creación de clústeres, el escalado de entrada/salida de clústeres, la actualización de la especificación del nodo maestro, el escalado automático, la modificación del nombre del clúster y la sincronización de usuarios de IAM, y no se podrá supervisar el estado de ejecución del clúster.

Procedimiento

Paso 1 Inicie sesión en la consola de gestión.

Paso 2 Elija **Big Data > MapReduce Service** en la lista de servicios. Se muestra la página **Assign Permissions**.

Figura 1-1 Asignación de permisos



Paso 3 Haga clic en **Assign**.

Después de que se acuerde la asignación, se creará una delegación llamada **mrs_admin_agency** en IAM. No modifique ni elimine la delegación después de su creación. Una vez creada la delegación, puede utilizar MRS.

NOTA

Después de la asignación, si la delegación no se crea, es probablemente porque el número de agencias ya alcanza el límite superior. En este caso, inicie sesión en la consola de IAM y elimine agencias innecesarias, o póngase en contacto con el administrador para aumentar la cuota de delegación.

----Fin

1.2 Creación de un usuario de MRS

Utilice **IAM** para implementar un control de permisos detallado sobre su MRS. Con IAM, usted puede:

- Cree usuarios de IAM bajo su cuenta de Huawei Cloud para empleados en función de la estructura organizativa de su empresa para que cada empleado pueda acceder a los recursos de MRS utilizando su credencial de seguridad única (usuario de IAM).
- Conceder sólo los permisos necesarios para que los usuarios realicen una tarea específica.
- Confíe una cuenta de Huawei Cloud o un servicio en la nube para realizar operaciones eficientes en sus recursos de MRS.

Si su cuenta de Huawei Cloud no requiere usuarios de IAM, omita esta sección.

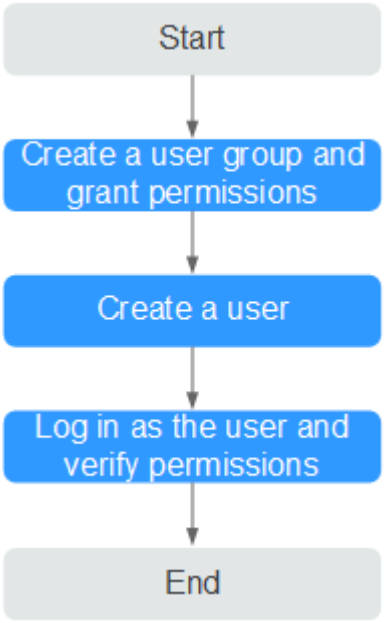
En esta sección se describe el procedimiento para conceder permisos (consulte **Figura 1-2**).

Prerrequisitos

Obtenga información sobre los permisos admitidos por MRS haciendo referencia a **Gestión de permiso**. Para obtener los permisos de otros servicios, consulte **Descripción de permiso**.

Flujo de proceso

Figura 1-2 Proceso para la concesión de permisos de MRS



1. **Creación de un grupo de usuario y asignación de permisos**

   Cree un grupo de usuarios en la consola de IAM y asigne permisos de MRS al grupo.

2. **Crear un usuario y agregarlo a un grupo de usuarios**.

   Cree un usuario en la consola de IAM y agregue el usuario al grupo creado en **1. Cree un grupo de usuarios y asígnele permisos**.

3. **Iniciar sesión** y verificar los permisos.

   Inicie sesión en la consola mediante el usuario creado y compruebe que el usuario tiene los permisos concedidos.

   - Elija **Service List** >**Analytics** >**MapReduce Service**. Haga clic en **Buy Cluster** en la consola de MRS. Si no puede comprar un clúster de MRS (suponga que solo tiene el permiso **MRS ReadOnlyAccess**), la política **MRS ReadOnlyAccess** tiene efecto.
   - Elija cualquier otro servicio en **Service List**. Si aparece un mensaje que indica que no tiene permisos suficientes para acceder al servicio, la política **MRS ReadOnlyAccess** ya tiene efecto.

Descripción de permiso de MRS

De forma predeterminada, los nuevos usuarios de IAM no tienen permisos. Para asignar permisos a un usuario, agregue el usuario a uno o más grupos y asigne políticas o roles de

permisos a estos grupos. A continuación, el usuario hereda los permisos de los grupos de los que es miembro y puede realizar operaciones específicas en servicios en la nube basadas en los permisos.

MRS es un servicio a nivel de proyecto implementado y accedido en regiones físicas específicas. Para asignar permisos a un grupo de usuarios, especifique **Scope** como **Region-specific projects** y seleccione proyectos en la región correspondiente para que los permisos surtan efecto. Si se selecciona **All projects**, los permisos surtirán efecto para el grupo de usuarios en todos los proyectos específicos de la región. Al acceder a MRS, los usuarios necesitan cambiar a una región en la que han sido autorizados para usar el servicio MRS.

Puede conceder permisos a los usuarios mediante roles y políticas.

- Roles: Un tipo de mecanismo de autorización de grano grueso que define permisos relacionados con las responsabilidades del usuario. Este mecanismo proporciona solo un número limitado de roles de nivel de servicio para la autorización. Al usar roles para conceder permisos, también debe asignar otros roles de los que dependen los permisos para que surtan efecto. Sin embargo, los roles no son una opción ideal para la autorización detallada y el control de acceso seguro.
- Políticas: Un tipo de mecanismo de autorización detallado que define los permisos necesarios para realizar operaciones en recursos de nube específicos bajo ciertas condiciones. Este mecanismo permite una autorización más flexible basada en políticas, cumpliendo los requisitos para un control de acceso seguro. Por ejemplo, puede conceder a los usuarios de MRS únicamente los permisos para realizar operaciones especificadas en clústeres de MRS, como crear un clúster y consultar una lista de clústeres en lugar de eliminar un clúster. La mayoría de las políticas definen permisos basados en API. Para ver las acciones API admitidas por MRS, consulte **Políticas de permisos y acciones admitidas**.

Tabla 1-1 enumera todas las políticas de sistema admitidas por MRS.

Tabla 1-1 Políticas del sistema de MRS

Política	Descripción	Tipo
MRS FullAccess	Permisos de administrador para MRS. Los usuarios con estos permisos pueden operar y usar todos los recursos MRS.	Fine-grained policy
MRS CommonOperations	Permisos de usuario comunes para MRS. Los usuarios con estos permisos pueden usar MRS pero no pueden agregar ni eliminar recursos.	Fine-grained policy
MRS ReadOnlyAccess	Permiso de sólo lectura para MRS. Los usuarios a los que se han concedido estos permisos sólo pueden ver los recursos de MRS.	Fine-grained policy

Política	Descripción	Tipo
MRS Administrator	Permisos: ● Todas las operaciones en MRS ● Los usuarios con permisos de esta política también deben tener permisos de las políticas **Tenant Guest** y **Server Administrator**.	RBAC policy

Tabla 1-2 enumera las operaciones comunes soportadas por cada política definida por el sistema o función de MRS. Seleccione las políticas según sea necesario.

Tabla 1-2 Operaciones comunes apoyadas por cada política definida por el sistema

Operación	MRS FullAccess	MRS CommonOperations	MRS ReadOnlyAccess	MRS Administrator
Creación de un clúster	√	x	x	√
Cambiar el tamaño de un clúster	√	x	x	√
Actualización de especificaciones de nodo	√	x	x	√
Eliminación de un clúster	√	x	x	√
Consulta de detalles del clúster	√	√	√	√
Consulta de una lista de clúster	√	√	√	√
Configuración de una regla de escalado automático	√	x	x	√
Consulta de una lista de host	√	√	√	√

Operación	MRS FullAccess	MRS CommonOperations	MRS ReadOnlyAccess	MRS Administrator
Consulta de logs de operación	√	√	√	√
Creación y ejecución de un trabajo	√	√	x	√
Detener un trabajo	√	√	x	√
Supresión de un solo trabajo	√	√	x	√
Supresión de trabajos en lotes	√	√	x	√
Consulta de detalles de trabajo	√	√	√	√
Consulta de una lista de trabajo	√	√	√	√
Creación de una carpeta	√	√	x	√
Eliminación de archivos	√	√	x	√
Consulta de una lista de archivo	√	√	√	√
Operación de etiquetas de clúster en lotes	√	√	x	√
Creación de una única etiqueta de clúster	√	√	x	√
Eliminación de una única etiqueta de clúster	√	√	x	√

Operación	MRS FullAccess	MRS CommonOperations	MRS ReadOnlyAccess	MRS Administrator
Consulta de una lista de recursos por etiqueta	√	√	√	√
Consulta de etiquetas de clúster	√	√	√	√
Administrador de acceso	√	√	x	√
Consulta de una lista de parches	√	√	√	√
Instalación de un parche	√	√	x	√
Desinstalación de un parche	√	√	x	√
Autorización de canales de O&M	√	√	x	√
Compartir logs de canales de O&M	√	√	x	√
Consulta de una lista de alarmas	√	√	√	√
Suscripción a la notificación de alarma	√	√	x	√
Envío de una sentencia de SQL	√	√	x	√
Consulta de resultados de SQL	√	√	x	√

Operación	MRS FullAccess	MRS CommonOperations	MRS ReadOnlyAccess	MRS Administrator
Cancelación de una tarea de ejecución de SQL	√	√	x	√

1.3 Creación de una política personalizada

Se pueden crear políticas personalizadas para complementar las políticas definidas por el sistema de MRS. Para ver las acciones que se pueden agregar a las políticas personalizadas, consulte **Políticas de permisos y acciones admitidas**.

Puede crear las políticas personalizadas de cualquiera de las siguientes maneras:

- Editor visual: Seleccione servicios en la nube, acciones, recursos y condiciones de solicitud. Esto no requiere conocimiento de la sintaxis de políticas.
- JSON: Edite las políticas de JSON desde cero o basándose en una política existente.

Para obtener más información, consulte **Creación de una política personalizada**.

NOTA

Las modificaciones de políticas personalizadas no surten efecto inmediatamente. Tiene que esperar unos 15 minutos.

Esta sección proporciona ejemplos de políticas personalizadas.

Ejemplo de las políticas personalizadas

- Ejemplo 1: Permitir a los usuarios crear clústeres MRS únicamente

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "mrs:cluster:create",
                "ecs:*:*",
                "bms:*:*",
                "evs:*:*",
                "vpc:*:*",
                "smn:*:*"
            ]
        }
    ]
}
```

- Ejemplo 2: Permitir a los usuarios cambiar el tamaño de un clúster MRS

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "mrs:cluster:resize"
            ]
```



```
        }
    ]
}
```

- Ejemplo 3: Permitir a los usuarios crear un clúster, crear y ejecutar un trabajo y eliminar un solo trabajo, pero denegar la eliminación del clúster

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "mrs:cluster:create",
                "mrs:job:submit",
                "mrs:job:delete"
            ]
        },
        {
            "Effect": "Deny",
            "Action": [
                "mrs:cluster:delete"
            ]
        }
    ]
}
```

- Ejemplo 4: Permitir a los usuarios crear un clúster de ECS con el permiso mínimo

  NOTA

  - Si necesita un par de claves para crear un clúster, agregue los siguientes permisos: **ecs:serverKeypairs:get** y **ecs:serverKeypairs:list**.
  - Agregue el permiso **kms:cmk:list** al cifrar discos de datos durante la creación del clúster.
  - Agregue el permiso **mrs:alarm:subscribe** para habilitar la función de alarma durante la creación del clúster.
  - Agregue el permiso **rds:instance:list** para usar orígenes de datos externos durante la creación del clúster.

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "mrs:cluster:create"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ecs:cloudServers:updateMetadata",
                "ecs:cloudServerFlavors:get",
                "ecs:cloudServerQuotas:get",
                "ecs:servers:list",
                "ecs:servers:get",
                "ecs:cloudServers:delete",
                "ecs:cloudServers:list",
                "ecs:serverInterfaces:get",
                "ecs:serverGroups:manage",
                "ecs:servers:setMetadata",
                "ecs:cloudServers:get",
                "ecs:cloudServers:create"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "vpc:securityGroups:create",
```



```
                "vpc:securityGroupRules:delete",
                "vpc:vpcs:create",
                "vpc:ports:create",
                "vpc:securityGroups:get",
                "vpc:subnets:create",
                "vpc:privateIps:delete",
                "vpc:quotas:list",
                "vpc:networks:get",
                "vpc:publicIps:list",
                "vpc:securityGroups:delete",
                "vpc:securityGroupRules:create",
                "vpc:privateIps:create",
                "vpc:ports:get",
                "vpc:ports:delete",
                "vpc:publicIps:update",
                "vpc:subnets:get",
                "vpc:publicIps:get",
                "vpc:ports:update",
                "vpc:vpcs:list"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "evs:quotas:get",
                "evs:types:get"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "bms:serverFlavors:get"
            ]
        }
    ]
}
```

- Ejemplo 5: Permitir a los usuarios crear un clúster de BMS con el permiso mínimo

  NOTA

  - Si necesita un par de claves para crear un clúster, agregue los siguientes permisos: **ecs:serverKeypairs:get** y **ecs:serverKeypairs:list**.
  - Agregue el permiso **kms:cmk:list** al cifrar discos de datos durante la creación del clúster.
  - Agregue el permiso **mrs:alarm:subscribe** para habilitar la función de alarma durante la creación del clúster.
  - Agregue el permiso **rds:instance:list** para usar orígenes de datos externos durante la creación del clúster.

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "mrs:cluster:create"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ecs:servers:list",
                "ecs:servers:get",
                "ecs:cloudServers:delete",
                "ecs:serverInterfaces:get",
                "ecs:serverGroups:manage",
                "ecs:servers:setMetadata",
                "ecs:cloudServers:create",
```



```
                "ecs:cloudServerFlavors:get",
                "ecs:cloudServerQuotas:get"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "vpc:securityGroups:create",
                "vpc:securityGroupRules:delete",
                "vpc:vpcs:create",
                "vpc:ports:create",
                "vpc:securityGroups:get",
                "vpc:subnets:create",
                "vpc:privateIps:delete",
                "vpc:quotas:list",
                "vpc:networks:get",
                "vpc:publicIps:list",
                "vpc:securityGroups:delete",
                "vpc:securityGroupRules:create",
                "vpc:privateIps:create",
                "vpc:ports:get",
                "vpc:ports:delete",
                "vpc:publicIps:update",
                "vpc:subnets:get",
                "vpc:publicIps:get",
                "vpc:ports:update",
                "vpc:vpcs:list"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "evs:quotas:get",
                "evs:types:get"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "bms:servers:get",
                "bms:servers:list",
                "bms:serverQuotas:get",
                "bms:servers:updateMetadata",
                "bms:serverFlavors:get"
            ]
        }
    ]
}
```

- Ejemplo 6: Permitir a los usuarios crear un clúster de ECS y BMS híbrido con el permiso mínimo

  NOTA

  - Si necesita un par de claves para crear un clúster, agregue los siguientes permisos: **ecs:serverKeypairs:get** y **ecs:serverKeypairs:list**.
  - Agregue el permiso **kms:cmk:list** al cifrar discos de datos durante la creación del clúster.
  - Agregue el permiso **mrs:alarm:subscribe** para habilitar la función de alarma durante la creación del clúster.
  - Agregue el permiso **rds:instance:list** para usar orígenes de datos externos durante la creación del clúster.

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
```



```
                "mrs:cluster:create"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ecs:cloudServers:updateMetadata",
                "ecs:cloudServerFlavors:get",
                "ecs:cloudServerQuotas:get",
                "ecs:servers:list",
                "ecs:servers:get",
                "ecs:cloudServers:delete",
                "ecs:cloudServers:list",
                "ecs:serverInterfaces:get",
                "ecs:serverGroups:manage",
                "ecs:servers:setMetadata",
                "ecs:cloudServers:get",
                "ecs:cloudServers:create"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "vpc:securityGroups:create",
                "vpc:securityGroupRules:delete",
                "vpc:vpcs:create",
                "vpc:ports:create",
                "vpc:securityGroups:get",
                "vpc:subnets:create",
                "vpc:privateIps:delete",
                "vpc:quotas:list",
                "vpc:networks:get",
                "vpc:publicIps:list",
                "vpc:securityGroups:delete",
                "vpc:securityGroupRules:create",
                "vpc:privateIps:create",
                "vpc:ports:get",
                "vpc:ports:delete",
                "vpc:publicIps:update",
                "vpc:subnets:get",
                "vpc:publicIps:get",
                "vpc:ports:update",
                "vpc:vpcs:list"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "evs:quotas:get",
                "evs:types:get"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "bms:servers:get",
                "bms:servers:list",
                "bms:serverQuotas:get",
                "bms:servers:updateMetadata",
                "bms:serverFlavors:get"
            ]
        }
    ]
}
```

1.4 Sincronización de usuarios de IAM a MRS

La sincronización de usuarios de IAM es para sincronizar los usuarios de IAM vinculados con las políticas de MRS con el sistema de MRS y crear cuentas con los mismos nombres de usuario pero diferentes contraseñas que los usuarios de IAM. A continuación, puede utilizar un nombre de usuario de IAM (la contraseña debe ser restablecida por el usuario **admin** de Manager) para iniciar sesión en Manager para la gestión de clústeres y enviar trabajos en la GUI en un clúster con autenticación de Kerberos habilitada.

Tabla 1-3 compara las políticas de permisos de los usuarios de IAM y los permisos de los usuarios sincronizados en MRS. Para obtener más información sobre los permisos predeterminados en Manager, consulte **Información de permisos predeterminados**.

Tabla 1-3 Asignación de políticas y permisos después de la sincronización

Tipo de política	Política de IAM	Permisos predeterminados del usuario en MRS después de la sincronización	Tener permiso para realizar la sincronización	Tener permiso para enviar trabajos
Grano fino	MRS ReadOnlyAccess	Manager_viewer	No	No
	MRS CommonOperations	● Manager_viewer ● default ● launcher-job	No	Yes
	MRS FullAccess	● Manager_administrator ● Manager_auditor ● Manager_operator ● Manager_tenant ● Manager_viewer ● System_administrator ● default ● launcher-job	Sí	Sí

Tipo de política	Política de IAM	Permisos predeterminados del usuario en MRS después de la sincronización	Tener permiso para realizar la sincronización	Tener permiso para enviar trabajos
RBAC	MRS Administrator	● Manager_administrator ● Manager_auditor ● Manager_operator ● Manager_tenant ● Manager_viewer ● System_administrator ● default ● launcher-job	No	Sí
	Server Administrator, Tenant Guest, y MRS Administrator	● Manager_administrator ● Manager_auditor ● Manager_operator ● Manager_tenant ● Manager_viewer ● System_administrator ● default ● launcher-job	Sí	Sí

Tipo de política	Política de IAM	Permisos predeterminados del usuario en MRS después de la sincronización	Tener permiso para realizar la sincronización	Tener permiso para enviar trabajos
	Tenant Administrator	• Manager_administrator • Manager_auditor • Manager_operator • Manager_tenant • Manager_viewer • System_administrator • default • launcher-job	Sí	Sí

Tipo de política	Política de IAM	Permisos predeterminados del usuario en MRS después de la sincronización	Tener permiso para realizar la sincronización	Tener permiso para enviar trabajos
Custom	Custom policy	● Manager_viewer ● default ● launcher-job	● Si las políticas personalizadas usan políticas de RBAC como plantilla, consulte las políticas de RBAC. ● Si las políticas personalizadas usan políticas de grano fino como plantilla, consulte las políticas de grano fino. Se recomiendan las políticas de grano fino.	Sí

NOTA

Para facilitar la gestión de permisos de usuario, utilice políticas detalladas en lugar de políticas de RBAC. En las políticas de grano fino, la acción Deny tiene prioridad sobre otras acciones.

- Un usuario tiene permiso para sincronizar usuarios de IAM solo cuando el usuario tiene el rol de Tenant Administrator o tiene los roles Server Administrator, Tenant Guest, y MRS Administrator al mismo tiempo.
- Un usuario con la política **action:mrs:cluster:syncUser** tiene permiso para sincronizar usuarios de IAM.

Procedimiento

Paso 1 Crear un usuario y autorizar al usuario a utilizar MRS. Para más detalles, consulte **Creación de un usuario de MRS**.

Paso 2 Inicie sesión en la consola de gestión de MRS y cree un clúster. Para obtener más información, consulte **Compra de un clúster personalizado**.

Paso 3 En el panel de navegación de la izquierda, elija **Clusters** > **Active Clusters**. Haga clic en el nombre del clúster para ir a la página de detalles del clúster.

Paso 4 En la página de pestaña **Dashboard**, haga clic en **Click to synchronize** junto a **IAM User Sync** para sincronizar los usuarios de IAM.

Paso 5 Después de enviar una solicitud de sincronización, elija **Operation Logs** en el panel de navegación izquierdo de la consola de MRS para comprobar si la sincronización se realiza correctamente. Para obtener más información sobre los registros, consulte **Consulta de registros de operaciones de MRS**.

Paso 6 Una vez que la sincronización se realiza correctamente, utilice el usuario sincronizado con IAM para realizar operaciones posteriores.

NOTA

- Cuando la política del grupo de usuarios al que pertenece el usuario de IAM cambie de **MRS ReadOnlyAccess** a **MRS CommonOperations**, **MRS FullAccess** o **MRS Administrator**, espere 5 minutos hasta que la nueva política entre en vigor una vez completada la sincronización porque la caché **SSSD** (System Security Services Daemon) de los nodos del clúster necesita tiempo para actualizarse. Luego, envíe un trabajo. De lo contrario, es posible que el trabajo no se envíe.
- Cuando la política del grupo de usuarios al que pertenece el usuario de IAM cambie de **MRS CommonOperations**, **MRS FullAccess** o **MRS Administrator** a **MRS ReadOnlyAccess**, espere 5 minutos hasta que la nueva política surta efecto una vez completada la sincronización porque la caché **SSSD** de los nodos del clúster necesita tiempo para actualizarse.
- Después de hacer clic en **Synchronize** en el lado derecho de **IAM User Sync**, la página de detalles del clúster queda en blanco durante un corto período de tiempo, porque se sincronizan los datos del usuario. La página se mostrará correctamente una vez completada la sincronización de datos.

- Enviar trabajos en un clúster de seguridad: Los usuarios pueden enviar trabajos mediante la función de gestión de trabajos en la GUI del clúster de seguridad. Para obtener más información, consulte **Ejecución de un trabajo de MapReduce**.
- Todas las pestañas se muestran en la página de detalles del clúster, incluidos **Components**, **Tenants** y **Backups & Restorations**.
- Iniciar sesión en Manager
  a. Inicie sesión en Manager como usuario **admin**. Para obtener más información, consulte **Acceder a Manager**.
  b. Inicialice la contraseña del usuario sincronizado con IAM. Para obtener más información, véase **Inicialización de la contraseña de un usuario del sistema**.
  c. Modifique el rol enlazado al grupo de usuarios al que pertenece el usuario para controlar los permisos de usuario en Manager. Para más detalles, consulte **Tareas relacionadas**. Para obtener más información acerca de cómo crear y modificar un rol, consulte **Creación de un rol**. Después de modificar el rol de componente enlazado al grupo de usuarios al que pertenece el usuario, los permisos de rol tardan algún tiempo en surtir efecto.
  d. Inicie sesión en el Manager con el usuario sincronizado con IAM y la contraseña después de la inicialización de **Paso 6.b**.

NOTA

Si cambia el permiso del usuario de IAM, vaya a **Paso 4** para realizar una segunda sincronización. Después de la segunda sincronización, los permisos de un usuario del sistema son la unión de los permisos definidos en la política del sistema de IAM y los permisos de los roles agregados por el usuario del sistema en Manager. Después de la segunda sincronización, los permisos de un usuario personalizado están sujetos a los permisos configurados en Manager.

- Usuario del sistema: si todos los grupos de usuarios a los que pertenece un usuario de IAM están enlazados a políticas del sistema (las políticas RABC y las políticas detalladas pertenecen a políticas del sistema), el usuario de IAM es un usuario del sistema.
- Usuario personalizado: si el grupo de usuarios al que pertenece un usuario de IAM está enlazado a cualquier política personalizada, el usuario de IAM es un usuario personalizado.

----Fin

2 Configuración de un clúster

2.1 ¿Cómo comprar un clúster de MRS?

Esta sección describe cómo comprar un clúster de MRS.

- **Comprar rápidamente un clúster de análisis de Hadoop**: En la página de pestaña **Quick Config**, puede configurar rápidamente los parámetros para comprar un clúster de análisis de Hadoop en pocos minutos, facilitando el análisis y las consultas de grandes cantidades de datos.
- **Comprar rápidamente un clúster de consultas de HBase**: En la página de pestaña **Quick Config**, puede configurar rápidamente los parámetros para comprar un clúster de consultas HBase en pocos minutos, lo que facilita el almacenamiento y la computación distribuida de grandes cantidades de datos.
- **Quickly Buying a Kafka Streaming Cluster**: En la página de pestaña **Quick Config**, puede configurar rápidamente los parámetros para comprar un clúster de streaming de Kafka en pocos minutos, lo que facilita la ingesta de datos de streaming, así como el procesamiento y almacenamiento de datos en tiempo real.
- **Comprar rápidamente un clúster de ClickHouse**: Puede comprar rápidamente un clúster de ClickHouse. ClickHouse es un sistema de gestión de bases de datos columnar utilizado para el análisis en línea. Cuenta con una tasa de compresión óptima y un rendimiento de consulta rápido.
- **Comprar rápidamente un clúster de análisis en tiempo real**: Puede comprar un clúster de análisis en tiempo real en unos minutos para recopilar, analizar y consultar rápidamente una gran cantidad de datos.
- **Compra de un clúster personalizado**: En la página de pestaña **Custom Config**, puede configurar de forma flexible los parámetros para comprar clústeres en función de escenarios de aplicación, como las especificaciones de ECS del modo de facturación para que se adapten mejor a sus requisitos de servicio.

Si se ha registrado en Huawei Cloud, inicie sesión en la consola de gestión y acceda a su MRS. Si no tiene una cuenta, registre una en Huawei Cloud. Después del registro, su cuenta se puede utilizar para acceder a todos los servicios de nube pública, incluido su MRS.

Registro con Huawei Cloud

Si ya tiene una cuenta de Huawei Cloud, omita esta parte. Si no tiene una cuenta de Huawei Cloud, realice las siguientes operaciones para crear una cuenta:

Paso 1 Visite **Huawei Cloud**.

Paso 2 Haga clic en **Register** y complete el registro según las instrucciones.

Después de registrarse con éxito, el sistema le redirige automáticamente a su página de información personal.

----Fin

2.2 Comprar rápidamente un clúster MRS

2.2.1 Comprar rápidamente un clúster de análisis de Hadoop

Esta sección describe cómo comprar rápidamente un clúster de análisis de Hadoop para el análisis y la consulta de grandes cantidades de datos. En el ecosistema de Hadoop de código abierto, Hadoop utiliza YARN para gestionar recursos de clúster, Hive y Spark para proporcionar almacenamiento y computación fuera de línea de datos distribuidos a gran escala, Spark Streaming y Flink para ofrecer computación de datos de streaming, y Presto para permitir consultas interactivas, Tez para proporcionar un marco de cálculo distribuido de gráficos acíclicos dirigidos (DAG).

El clúster de análisis de Hadoop consta de los siguientes componentes:

- MRS 1.9.2: Hadoop 2.8.3, Spark 2.2.2, Hive 2.3.3, Presto 0.216, Tez 0.9.1, Ranger 1.0.1, y Flink 1.7.0.
- MRS 3.1.0: Hadoop 3.1.1, Hive 3.1.0, Spark2x 2.4.5, Flink 1.12.0, ZooKeeper 3.5.6, Ranger 2.0.0, Tez 0.9.2, y Presto 333.
- MRS 3.1.2-LTS.3: Hadoop 3.1.1, Hive 3.1.0, Spark2x 3.1.1, Flink 1.12.2, ZooKeeper 3.6.3, Ranger 2.0.0, y Tez 0.9.2.
- MRS 3.1.5: Hadoop 3.1.1, Hive 3.1.0, Spark2x 3.1.1, Tez 0.9.2, Flink 1.12.2, ZooKeeper 3.6.3, Ranger 2.0.0, y Presto 333.

Compra rápida de un clúster de análisis de Hadoop

Paso 1 Inicie sesión en la consola de MRS.

Paso 2 Haga clic en **Buy Cluster**. Se muestra la página para comprar un clúster.

Paso 3 En la página para comprar un clúster, haga clic en la pestaña **Quick Config**.

Paso 4 Configure la información básica del clúster. Para obtener más información sobre los parámetros, consulte **Compra de un clúster personalizado**.

- **Region**: Utilice el valor predeterminado.
- **Billing Mode**: Seleccione **Pay-per-use**.
- **Cluster Name**: Puede utilizar el nombre predeterminado. Sin embargo, se recomienda incluir una abreviatura de nombre de proyecto o fecha para la memoria consolidada y fácil de distinguir, por ejemplo, **mrs_20180321**.

- **Version Type**: **Normal** está seleccionado de forma predeterminada. (Los componentes varían según el tipo de versión. Seleccione un tipo de versión según sea necesario.)
- **Cluster Version**: Seleccione la última versión, que es el valor predeterminado. (Los componentes proporcionados por un clúster varían según la versión del clúster. Seleccione una versión de clúster basada en los requisitos del sitio.)
- **Component**: Seleccione **Hadoop analysis cluster**.
- **AZ**: Utilice el valor predeterminado.
- **Enterprise Project**: Conserve el valor predeterminado.
- **VPC**: Utilice el valor predeterminado. Si no hay una VPC disponible, haga clic en **View VPC** para acceder a la consola de VPC y crear una nueva VPC.
- **Subnet**: Utilice el valor predeterminado.
- **CPU Architecture**: Utilice el valor predeterminado.
- **Cluster Node**: Seleccione el número de nodos del clúster y las especificaciones de nodos según los requisitos del sitio. Para MRS 3.*x* o posterior, la memoria del nodo de master debe ser mayor que 64 GB.
- **Kerberos Authentication**: Si se debe habilitar la autenticación de Kerberos. El estado del control deslizante no se puede cambiar una vez que el clúster se ha comprado.
- **Username**: El valor predeterminado es **root/admin**. El usuario **root** se utiliza para iniciar sesión de forma remota en los ECS, y el usuario **admin** se utiliza para acceder a la página de gestión del clúster.
- **Password**: Establecer una contraseña para el usuario **root/admin**.
- **Confirm Password**: Ingrese la contraseña del usuario **root/admin** de nuevo.

Figura 2-1 Clúster de análisis de Hadoop

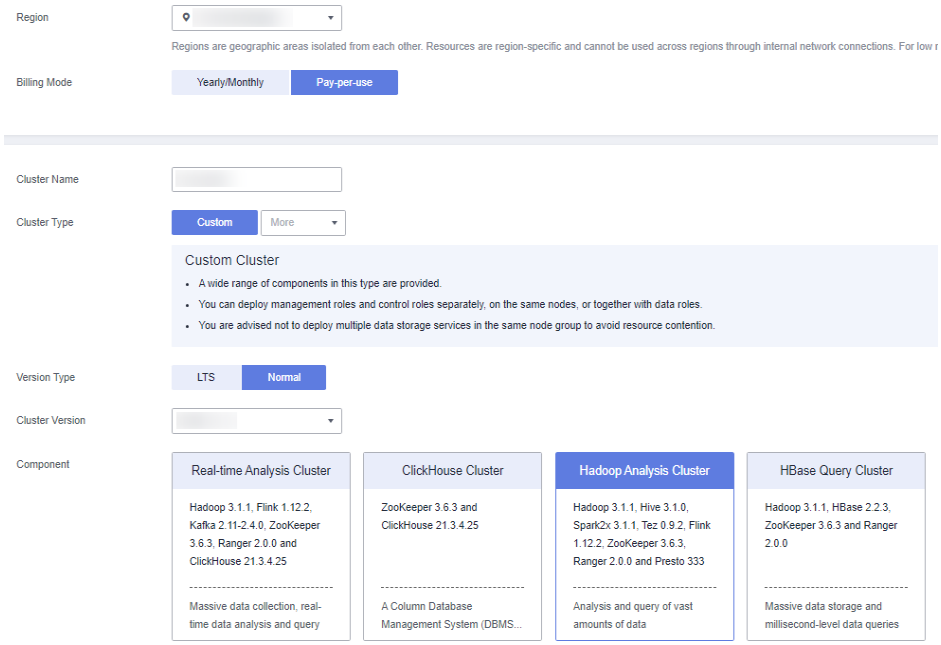
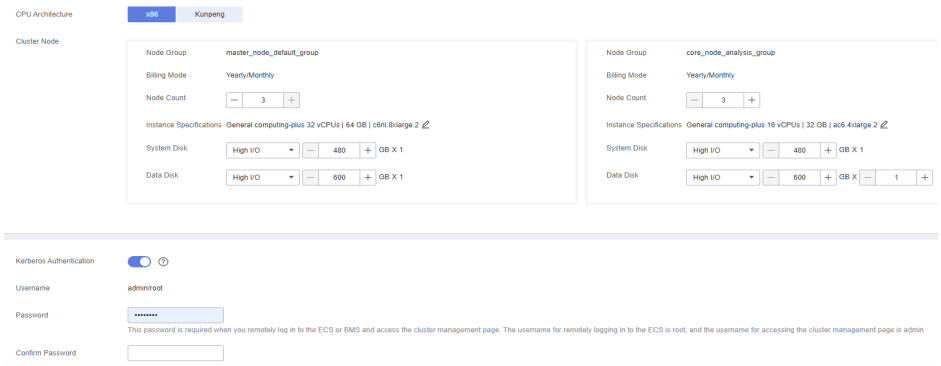


Figura 2-2 Configuraciones de nodos de clúster



Paso 5 Seleccione **Enable** para habilitar las comunicaciones seguras. Para obtener más información, consulte **Autorización de seguridad de comunicación**.

Paso 6 Haga clic en **Buy Now**.

Si la autenticación de Kerberos está habilitada, compruebe si esta función es necesaria. Si lo es, haga clic en **Continue**. Si no es así, haga clic en **Back** para desactivarlo y, a continuación, continúe con el paso siguiente. El estado del control deslizante no se puede cambiar una vez que el clúster se ha comprado.

NOTA

Para cualquier duda sobre el precio, haga clic en **Pricing details** en la esquina inferior izquierda.

Paso 7 Haga clic en **Back to Cluster List** para ver el estado del clúster. Haga clic en **Access Cluster** para ver los detalles del clúster.

Para obtener más información sobre el estado del clúster durante la creación, consulte la descripción de los parámetros de estado en **Tabla 3-4**.

Se necesita algún tiempo para crear un clúster. El estado inicial del clúster es **Starting**. Una vez que el clúster se ha creado correctamente, el estado del clúster pasa a ser **Running**.

En la consola de gestión de MRS, se puede crear simultáneamente un máximo de 10 clústeres y se puede gestionar un máximo de 100 clústeres.

----Fin

2.2.2 Comprar rápidamente un clúster de consultas de HBase

Esta sección describe cómo comprar rápidamente un clúster de consultas de HBase. El clúster de HBase utiliza los componentes de Hadoop y HBase para proporcionar un sistema de almacenamiento en la nube distribuido orientado a columnas que ofrece una confiabilidad mejorada, un rendimiento excelente y una escalabilidad elástica. Es aplicable al almacenamiento y al cómputo distribuido de cantidades masivas de datos. HBase puede utilizarse para construir un sistema de almacenamiento capaz de almacenar datos a nivel de TB o incluso de PB. Con HBase, puede filtrar y analizar datos con facilidad, y obtener respuestas en milisegundos, así como extraer valor de los datos rápidamente.

El clúster de análisis de HBase consta de los siguientes componentes:

- MRS 1.9.2: Hadoop 2.8.3, HBase 1.3.1, y Ranger 1.0.1.
- MRS 3.1.0: Hadoop 3.1.1, HBase 2.2.3, ZooKeeper 3.5.6, y Ranger 2.0.0.

- MRS 3.1.2-LTS.3: Hadoop 3.1.1, HBase 2.2.3, ZooKeeper 3.6.3, y Ranger 2.0.0.
- MRS 3.1.5: Hadoop 3.1.1, HBase 2.2.3, ZooKeeper 3.6.3, y Ranger 2.0.0.

Comprar rápidamente un clúster de consultas de HBase

Paso 1 Inicie sesión en la consola de MRS.

Paso 2 Haga clic en **Buy Cluster**. Se muestra la página para comprar un clúster.

Paso 3 En la página para comprar un clúster, haga clic en la pestaña **Quick Config**.

Paso 4 Configurar la información básica del clúster. Para obtener más información sobre los parámetros, consulte **Compra de un clúster personalizado**.

- **Region**: Utilice el valor predeterminado.
- **Billing Mode**: Seleccione **Pay-per-use**.
- **Cluster Name**: Puede utilizar el nombre predeterminado. Sin embargo, se recomienda incluir una abreviatura de nombre de proyecto o fecha para la memoria consolidada y fácil de distinguir, por ejemplo, **mrs_20180321**.
- **Version Type**: **Normal** está seleccionado de forma predeterminada. (Los componentes varían según el tipo de versión. Seleccione un tipo de versión según sea necesario.)
- **Cluster Version**: Seleccione la última versión, que es el valor predeterminado. (Los componentes proporcionados por un clúster varían según la versión del clúster. Seleccione una versión de clúster basada en los requisitos del sitio.)
- **Component**: Seleccione **HBase Query Cluster**.
- **AZ**: Utilice el valor predeterminado.
- **Enterprise Project**: Conserve el valor predeterminado.
- **VPC**: Utilice el valor predeterminado. Si no hay una VPC disponible, haga clic en **View VPC** para acceder a la consola de VPC y crear una nueva VPC.
- **Subnet**: Utilice el valor predeterminado.
- **CPU Architecture**: Utilice el valor predeterminado.
- **Cluster Node**: Seleccione el número de nodos del clúster y las especificaciones de nodos según los requisitos del sitio. Para MRS 3.*x* o posterior, la memoria del nodo de master debe ser mayor que 64 GB.
- **Kerberos Authentication**: Si se debe habilitar la autenticación de Kerberos. El estado del control deslizante no se puede cambiar una vez que el clúster se ha comprado.
- **Username**: El valor predeterminado es **root/admin**. El usuario **root** se utiliza para iniciar sesión de forma remota en los ECS, y el usuario **admin** se utiliza para acceder a la página de gestión del clúster.
- **Password**: Establecer una contraseña para el usuario **root**/**admin**.
- **Confirm Password**: Ingrese la contraseña del usuario **root**/**admin** de nuevo.

Figura 2-3 Clúster de consultas de HBase

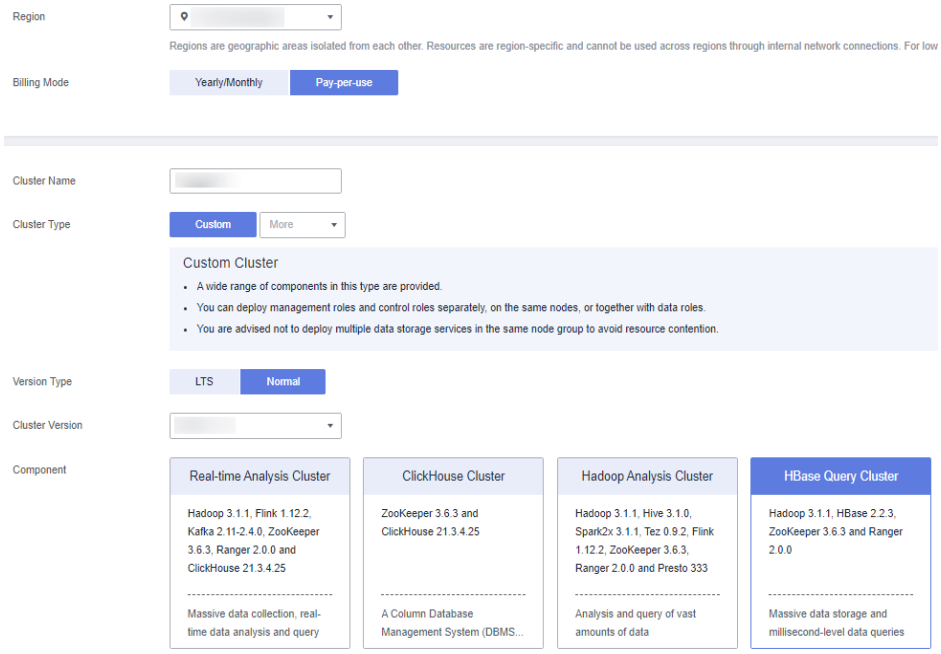
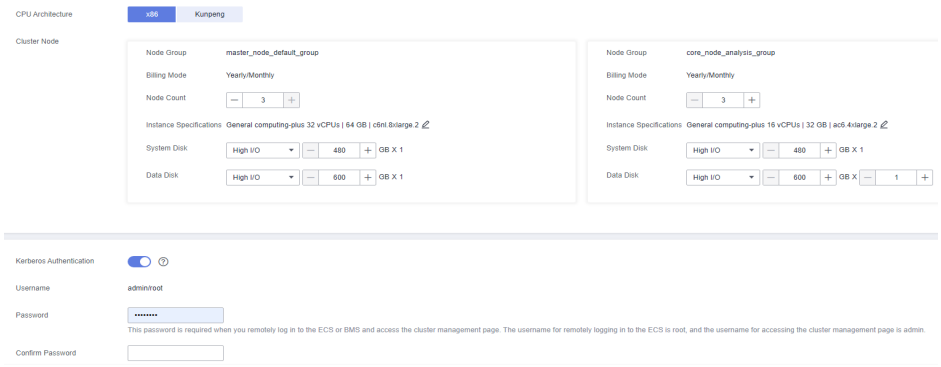


Figura 2-4 Configuraciones de nodos de clúster



Paso 5 Seleccione **Enable** para habilitar las comunicaciones seguras. Para obtener más información, consulte **Autorización de seguridad de comunicación**.

Paso 6 Haga clic en **Buy Now**.

Si la autenticación de Kerberos está habilitada, compruebe si esta función es necesaria. Si lo es, haga clic en **Continue**. Si no es así, haga clic en **Back** para desactivarlo y, a continuación, continúe con el paso siguiente. El estado del control deslizante no se puede cambiar una vez que el clúster se ha comprado.

NOTA

Para cualquier duda sobre el precio, haga clic en **Pricing details** en la esquina inferior izquierda.

Paso 7 Haga clic en **Back to Cluster List** para ver el estado del clúster. Haga clic en **Access Cluster** para ver los detalles del clúster.

Para obtener más información sobre el estado del clúster durante la creación, consulte la descripción de los parámetros de estado en **Tabla 3-4**.

Se necesita algún tiempo para crear un clúster. El estado inicial del clúster es **Starting**. Una vez que el clúster se ha creado correctamente, el estado del clúster pasa a ser **Running**.

En la consola de gestión de MRS, se puede crear simultáneamente un máximo de 10 clústeres y se puede gestionar un máximo de 100 clústeres.

----Fin

2.2.3 Quickly Buying a Kafka Streaming Cluster

This section describes how to quickly buy a Kafka streaming cluster. The Kafka cluster uses the Kafka and Storm components to provide an open source messaging system with high throughput and scalability. It is widely used in scenarios such as log collection and monitoring data aggregation to implement efficient streaming data collection and real-time data processing and storage.

The Kafka streaming cluster consists of the following components:

- MRS 1.9.2: Kafka 1.1.0 and Storm 1.2.1

Quickly Buying a Kafka Streaming Cluster

Paso 1 Log in to the MRS management console.

Paso 2 Click **Buy Cluster**. The page for buying a cluster is displayed.

Paso 3 On the page for buying a cluster, click the **Quick Config** tab.

Paso 4 Configure basic cluster information. For details about the parameters, see **Compra de un clúster personalizado**.

- **Region**: Use the default value.
- **Billing Mode**: Select **Pay-per-use**.
- **Cluster Name**: You can use the default name. However, you are advised to include a project name abbreviation or date for consolidated memory and easy distinguishing, for example, **mrs_20200321**.
- **Version Type**: **Normal** está seleccionado de forma predeterminada. (Los componentes varían según el tipo de versión. Seleccione un tipo de versión según sea necesario.)
- **Cluster Version**: The components provided by a cluster vary according to the cluster version. Select a cluster version based on site requirements.
- **Component**: Select **Kafka streaming cluster**.
- **AZ**: Use the default value.
- **Enterprise Project**: Retain the default value.
- **VPC**: Use the default value. If there is no available VPC, click **View VPC** to access the VPC console and create a new VPC.
- **Subnet**: Use the default value.
- **CPU Architecture**: Use the default value. This parameter is unavailable in MRS 3.*x*.
- **Cluster Node**: Select the number of cluster nodes and node specifications based on site requirements. For MRS 3.*x* or later, the memory of the master node must be greater than 64 GB.
- LVM: Use the default value. This parameter is not available in MRS 3.*x*.
- **Kerberos Authentication**: Whether to enable Kerberos authentication. The slider status cannot be changed once the cluster is bought.

- **Username**: The default value is **root/admin**. User **root** is used to remotely log in to ECSs, and user **admin** is used to access the cluster management page.
- **Password**: Set a password for user **root**/**admin**.
- **Confirm Password**: Enter the password of user **root**/**admin** again.

Figura 2-5 Kafka Streaming Cluster

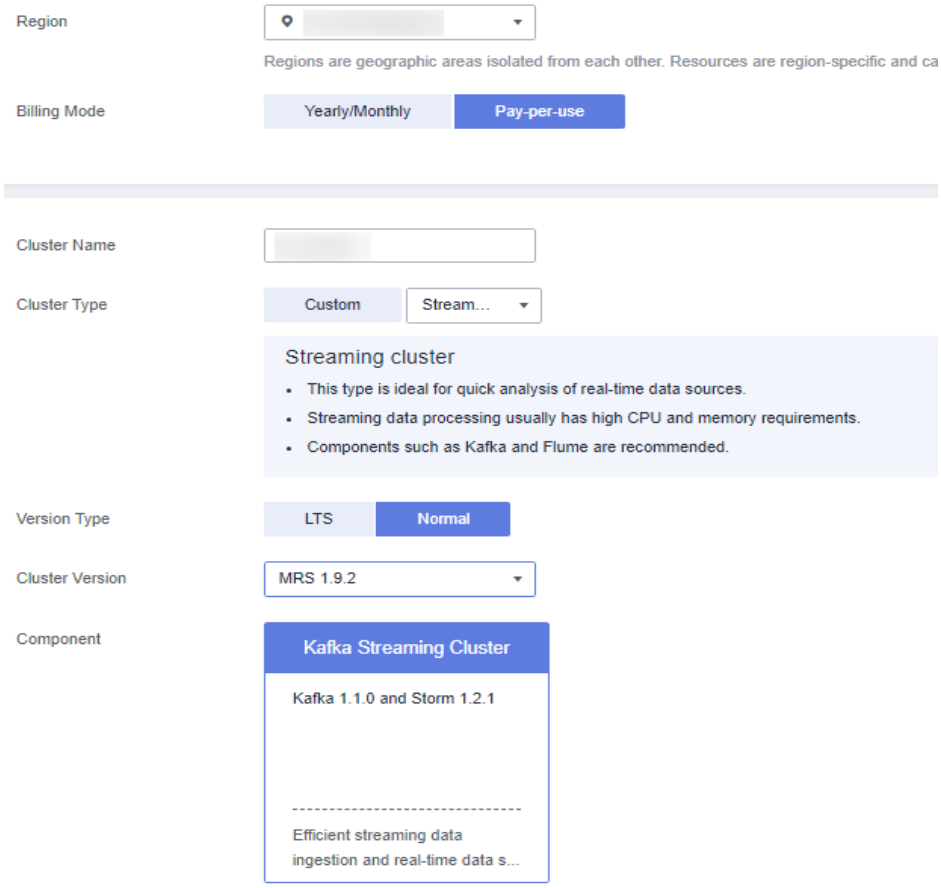
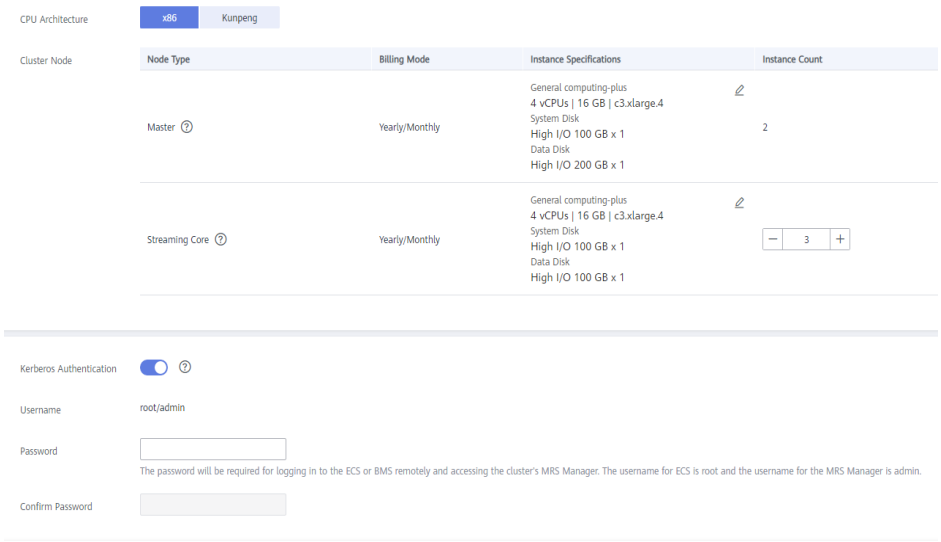


Figura 2-6 Cluster node configurations



Paso 5 Select **Enable** to enable secure communications. For details, see **Autorización de seguridad de comunicación**.

Paso 6 Click **Buy Now**.

If Kerberos authentication is enabled, check whether this function is required. If it is, click **Continue**. If not, click **Back** to disable it and then proceed with the subsequent step. The slider status cannot be changed once the cluster is bought.

NOTA

For any doubt about the pricing, click **Pricing details** in the lower left corner.

Paso 7 Click **Back to Cluster List** to view the cluster status. Click **Access Cluster** to view cluster details.

For details about cluster status during creation, see the description of the status parameters in **Tabla 3-4**.

It takes some time to create a cluster. The initial status of the cluster is **Starting**. After the cluster has been created successfully, the cluster status becomes **Running**.

On the MRS management console, a maximum of 10 clusters can be concurrently created, and a maximum of 100 clusters can be managed.

----Fin

2.2.4 Comprar rápidamente un clúster de ClickHouse

Esta sección describe cómo comprar rápidamente un clúster de ClickHouse. ClickHouse es un sistema de gestión de bases de datos columnar utilizado para el análisis en línea. Cuenta con una tasa de compresión óptima y un rendimiento de consulta rápido. Es ampliamente utilizado en publicidad en Internet, aplicaciones y análisis de tráfico web, telecomunicaciones, finanzas y campos de IoT.

El clúster ClickHouse consta de los siguientes componentes:

- MRS 3.1.0: ClickHouse 21.3.4.25 y ZooKeeper 3.5.6.

- MRS 3.1.2-LTS.3: .
- MRS 3.1.5: ClickHouse 21.3.4.25 y ZooKeeper 3.6.3.

El motor de tabla de clúster de ClickHouse que utiliza Kunpeng como arquitectura de CPU no admite HDFS ni Kafka.

Comprar rápidamente un clúster de ClickHouse

Paso 1 Inicie sesión en la consola de MRS.

Paso 2 Haga clic en **Buy Cluster**. Se muestra la página para comprar un clúster.

Paso 3 En la página para comprar un clúster, haga clic en la pestaña **Quick Config**.

Paso 4 Configure la información básica del clúster. Para obtener más información sobre los parámetros, consulte **Compra de un clúster personalizado**.

- **Region**: Utilice el valor predeterminado.
- **Billing Mode**: Seleccione **Pay-per-use**.
- **Cluster Name**: Puede utilizar el nombre predeterminado. Sin embargo, se recomienda incluir una abreviatura del nombre del proyecto o una fecha para la memoria consolidada y fácil de distinguir, Ejemplo: **mrs_20201121**.
- **Version Type**: **Normal** está seleccionado de forma predeterminada. (Los componentes varían según el tipo de versión. Seleccione un tipo de versión según sea necesario.)
- **Cluster Version**: Seleccione la última versión, que es el valor predeterminado. (Los componentes proporcionados por un clúster varían según la versión del clúster. Seleccione una versión de clúster basada en los requisitos del sitio.)
- **Component**: Seleccione **ClickHouse cluster**.
- **AZ**: Utilice el valor predeterminado.
- **Enterprise Project**: Conserve el valor predeterminado.
- **VPC**: Utilice el valor predeterminado. Si no hay una VPC disponible, haga clic en **View VPC** para acceder a la consola de VPC y crear una nueva VPC.
- **Subnet**: Utilice el valor predeterminado.
- **CPU Architecture**: Utilice el valor predeterminado.
- **Cluster Node**: Seleccione el número de nodos del clúster y las especificaciones de nodos según los requisitos del sitio. Para MRS 3.*x* o posterior, la memoria del nodo de master debe ser mayor que 64 GB.
- **Kerberos Authentication**: Si se debe habilitar la autenticación de Kerberos. El estado del control deslizante no se puede cambiar una vez que el clúster se ha comprado.
- **Username**: El valor predeterminado es **root/admin**. El usuario **root** se utiliza para iniciar sesión de forma remota en los ECS, y el usuario **admin** se utiliza para acceder a la página de gestión del clúster.
- **Password**: Establecer una contraseña para el usuario **root/admin**.
- **Confirm Password**: Ingrese la contraseña del usuario **root/admin** de nuevo.

Figura 2-7 Clúster de ClickHouse

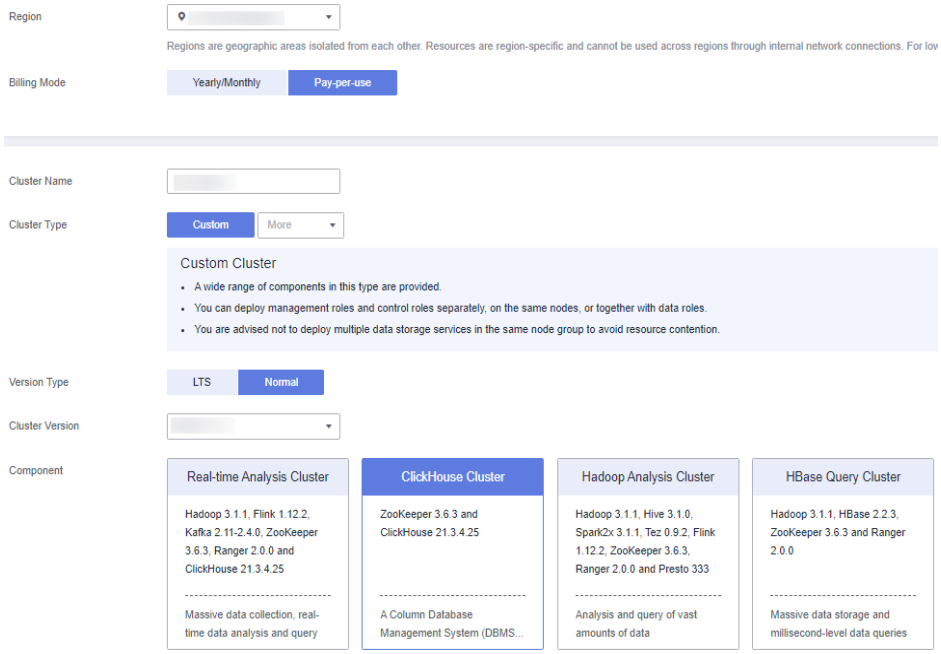
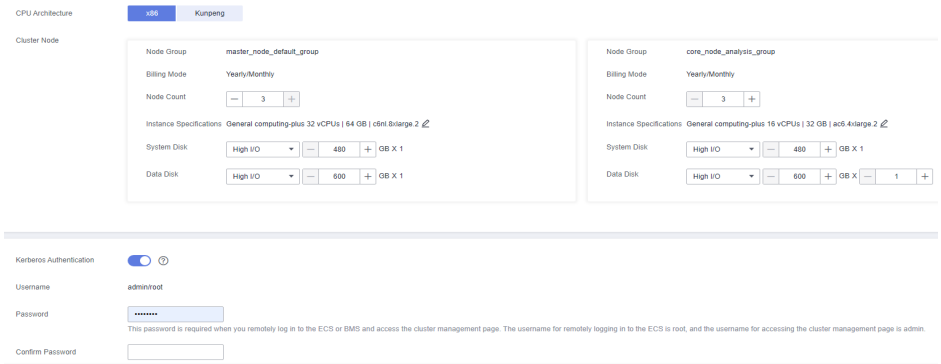


Figura 2-8 Configuraciones de nodos de clúster



Paso 5 Seleccione **Enable** para habilitar las comunicaciones seguras. Para obtener más información, consulte **Autorización de seguridad de comunicación**.

Paso 6 Haga clic en **Buy Now**.

Si la autenticación de Kerberos está habilitada, compruebe si esta función es necesaria. Si lo es, haga clic en **Continue**. Si no es así, haga clic en **Back** para desactivarlo y, a continuación, continúe con el paso siguiente. El estado del control deslizante no se puede cambiar una vez que el clúster se ha comprado.

NOTA

Para cualquier duda sobre el precio, haga clic en **Pricing details** en la esquina inferior izquierda.

Paso 7 Haga clic en **Back to Cluster List** para ver el estado del clúster. Haga clic en **Access Cluster** para ver los detalles del clúster.

Para obtener más información sobre el estado del clúster durante la creación, consulte la descripción de los parámetros de estado en **Tabla 3-4**.

Se necesita algún tiempo para crear un clúster. El estado inicial del clúster es **Starting**. Una vez que el clúster se ha creado correctamente, el estado del clúster pasa a ser **Running**.

En la consola de gestión de MRS, se puede crear simultáneamente un máximo de 10 clústeres y se puede gestionar un máximo de 100 clústeres.

----Fin

2.2.5 Comprar rápidamente un clúster de análisis en tiempo real

Esta sección describe cómo comprar rápidamente un clúster de análisis en tiempo real. El clúster de análisis en tiempo real utiliza Hadoop, Kafka, Flink y ClickHouse para recopilar, analizar y consultar una gran cantidad de datos en tiempo real.

El clúster de análisis en tiempo real consta de los siguientes componentes:

- MRS 3.1.0: Hadoop 3.1.1, Kafka 2.11-2.4.0, Flink 1.12.0, ClickHouse 21.3.4.25, ZooKeeper 3.5.6, y Ranger 2.0.0.
- MRS 3.1.2-LTS.3: Hadoop 3.1.1, Kafka 2.11-2.4.0, Flink 1.12.2, ClickHouse 21.3.4.25, ZooKeeper 3.6.3, y Ranger 2.0.0.
- MRS 3.1.5: Hadoop 3.1.1, Kafka 2.11-2.4.0, Flink 1.12.2, ClickHouse 21.3.4.25, ZooKeeper 3.6.3, y Ranger 2.0.0.

Comprar rápidamente un clúster de análisis en tiempo real

Paso 1 Inicie sesión en la consola de MRS.

Paso 2 Haga clic en **Buy Cluster**. Se muestra la página para comprar un clúster.

Paso 3 En la página para comprar un clúster, haga clic en la pestaña **Quick Config**.

Paso 4 Configure la información básica del clúster. Para obtener más información sobre los parámetros, consulte **Compra de un clúster personalizado**.

- **Region**: Utilice el valor predeterminado.
- **Billing Mode**: Seleccione **Pay-per-use**.
- **Cluster Name**: Puede utilizar el nombre predeterminado. Sin embargo, se recomienda incluir una abreviatura del nombre del proyecto o una fecha para la memoria consolidada y fácil de distinguir, Ejemplo: **mrs_20201130**.
- **Version Type**: **Normal** está seleccionado de forma predeterminada. (Los componentes varían según el tipo de versión. Seleccione un tipo de versión según sea necesario.)
- **Cluster Version**: Seleccione la última versión, que es el valor predeterminado. (Los componentes proporcionados por un clúster varían según la versión del clúster. Seleccione una versión de clúster basada en los requisitos del sitio.)
- **Component**: Seleccione **Real-time Analysis Cluster**.
- **AZ**: Utilice el valor predeterminado.
- **VPC**: Utilice el valor predeterminado. Si no hay una VPC disponible, haga clic en **View VPC** para acceder a la consola de VPC y crear una nueva VPC.
- **Subnet**: Utilice el valor predeterminado.
- **Enterprise Project**: Utilice el valor predeterminado.
- **CPU Architecture**: Utilice el valor predeterminado.

- **Cluster Node**: Seleccione el número de nodos del clúster y las especificaciones de nodos según los requisitos del sitio. Para MRS 3.*x* o posterior, la memoria del nodo de master debe ser mayor que 64 GB.
- **Kerberos Authentication**: Si se debe habilitar la autenticación de Kerberos. El estado del control deslizante no se puede cambiar una vez que el clúster se ha comprado.
- **Username**: El valor predeterminado es **root/admin**. El usuario **root** se utiliza para iniciar sesión de forma remota en los ECS, y el usuario **admin** se utiliza para acceder a la página de gestión del clúster.
- **Password**: Establecer una contraseña para el usuario **root**/**admin**.
- **Confirm Password**: Ingrese la contraseña del usuario **root**/**admin** de nuevo.

Figura 2-9 Clúster de análisis en tiempo real

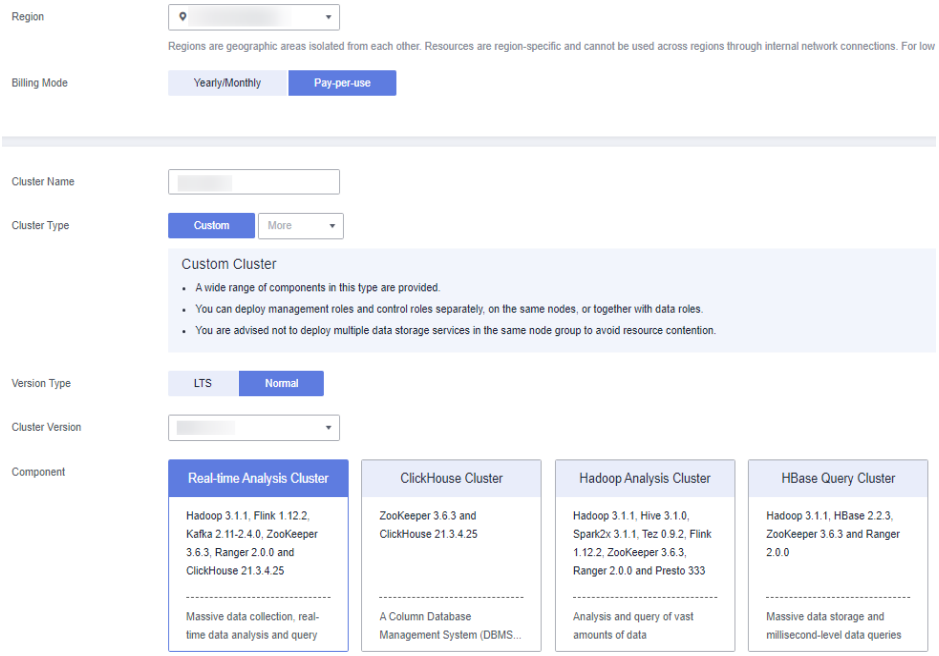
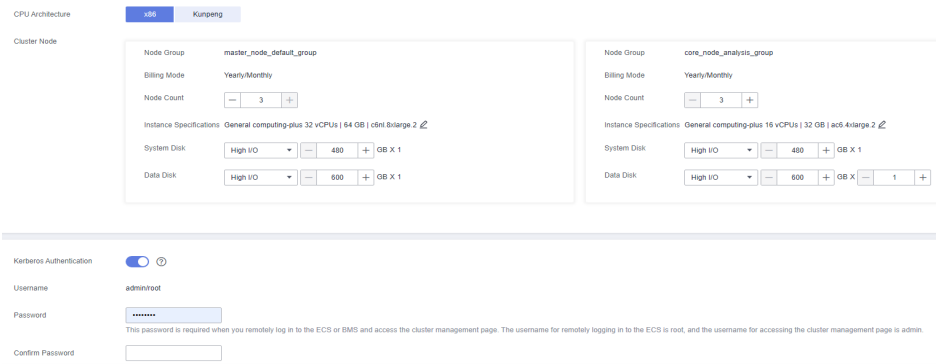


Figura 2-10 Configuraciones de nodos de clúster



Paso 5 Seleccione **Enable** para habilitar las comunicaciones seguras. Para obtener más información, consulte **Autorización de seguridad de comunicación**.

Paso 6 Haga clic en **Buy Now**.

Si la autenticación de Kerberos está habilitada, compruebe si esta función es necesaria. Si lo es, haga clic en **Continue**. Si no es así, haga clic en **Back** para desactivarlo y, a continuación,

continúe con el paso siguiente. El estado del control deslizante no se puede cambiar una vez que el clúster se ha comprado.

NOTA

Para cualquier duda sobre el precio, haga clic en **Pricing details** en la esquina inferior izquierda.

Paso 7 Haga clic en **Back to Cluster List** para ver el estado del clúster. Haga clic en **Access Cluster** para ver los detalles del clúster.

Para obtener más información sobre el estado del clúster durante la creación, consulte la descripción de los parámetros de estado en **Tabla 3-4**.

Se necesita algún tiempo para crear un clúster. El estado inicial del clúster es **Starting**. Una vez que el clúster se ha creado correctamente, el estado del clúster pasa a ser **Running**.

En la consola de gestión de MRS, se puede crear simultáneamente un máximo de 10 clústeres y se puede gestionar un máximo de 100 clústeres.

----Fin

2.3 Compra de un clúster personalizado

Para usar MRS, compre un clúster en la consola de gestión de MRS.

Puede crear un usuario o grupo de usuarios de IAM en la consola de gestión de IAM y concederle permisos de operación específicos para realizar una gestión de recursos perfeccionada después de registrar una cuenta. Para obtener más información, consulte **Creación de un usuario de MRS**.

Paso 1 Inicie sesión en la consola de gestión de MRS.

Paso 2 Haga clic en **Buy Cluster**. Se muestra la página para comprar un clúster.

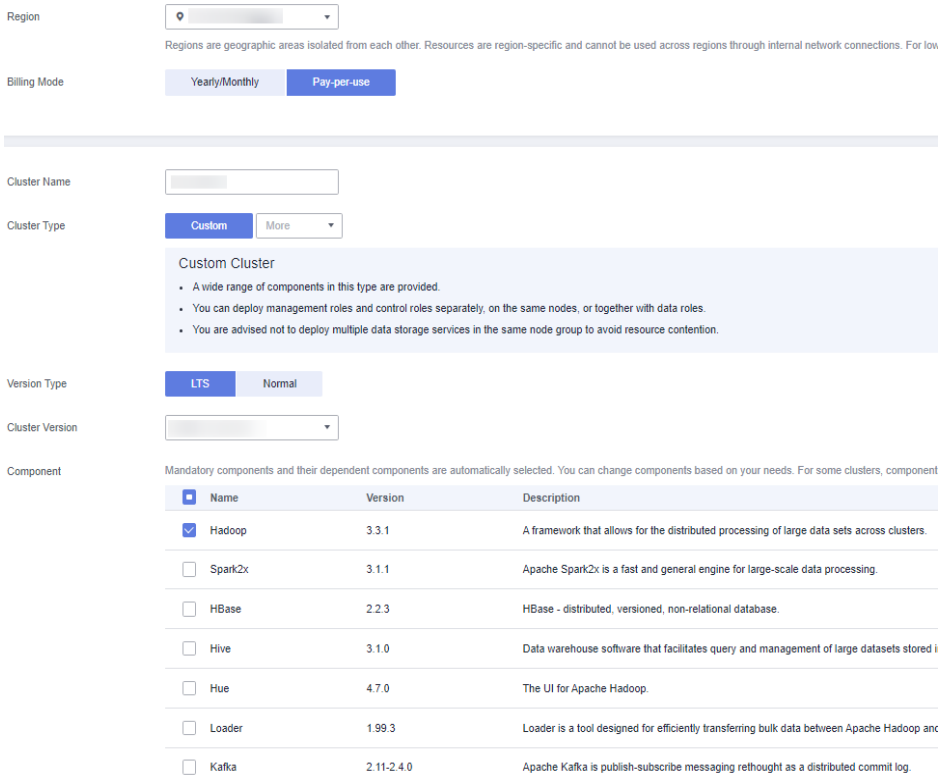
NOTA

Al crear un clúster, preste atención a la notificación de cuota. Si una cuota de recursos es insuficiente, aumente la cuota de recursos según se le solicite y cree un clúster.

Paso 3 En la página para comprar un clúster, haga clic en la pestaña **Custom Config**.

Paso 4 Configure la información del clúster haciendo referencia a **Configuraciones de software** y haga clic en **Next**.

Figura 2-11 Configurar software

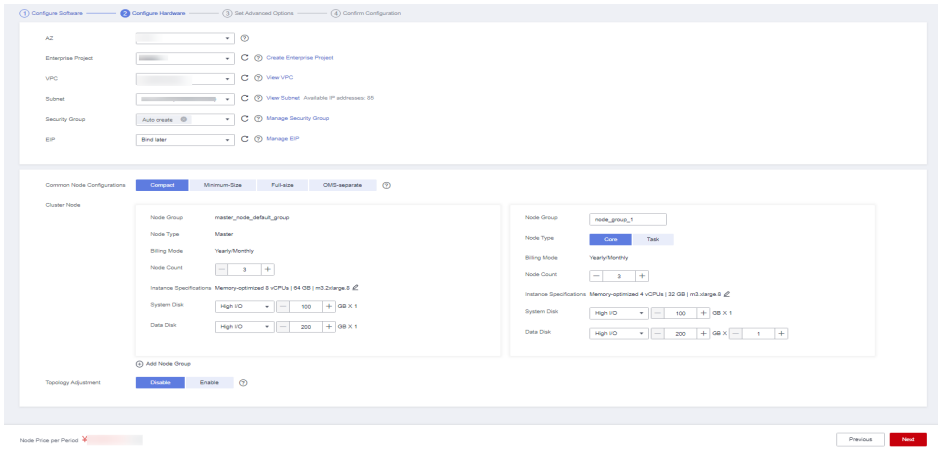


NOTA

Solo se admite un modo de facturación en algunas regiones. Para obtener más información, consulte la consola de gestión.

Paso 5 Configure la información del clúster haciendo referencia a **Configuraciones de hardware** y haga clic en **Next**.

Figura 2-12 Configurar hardware



Para agregar un grupo de nodos de tarea en el clúster MRS actual para escalar automáticamente, realice las siguientes operaciones:

Agregar un task de análisis de grupo de nodo.

- Para un clúster cuyo **Cluster Type** sea **Analysis cluster** o **Hybrid cluster**:

  El sistema agrega automáticamente el grupo de nodo de tarea de análisis **task_node_analysis_group**. Establezca el número de nodos, especificaciones de instancia y configuraciones de disco de nodo según sea necesario.

  Si el grupo de nodos de tareas de análisis no es necesario, puede eliminarlo manualmente.

- Para un clúster cuyo **Cluster Type** es de **Custom**:

  a. En el área de configuración de nodos de clúster, haga clic en **Add Node Group** para agregar manualmente un grupo de nodos.

  b. Ajuste **Topology Adjustment** a **Enable**.

  c. Seleccione manualmente la topología de rol para que el grupo de nodos contenga sólo el rol NodeManager (NM).

  También puede agregar manualmente un grupo de nodos de tarea después de crear el clúster. Para obtener más información, consulte **Adición de un nodo de Task**.

Agrear un grupo de nodos de streaming de flujo (compatible solo con MRS 1.9.2):

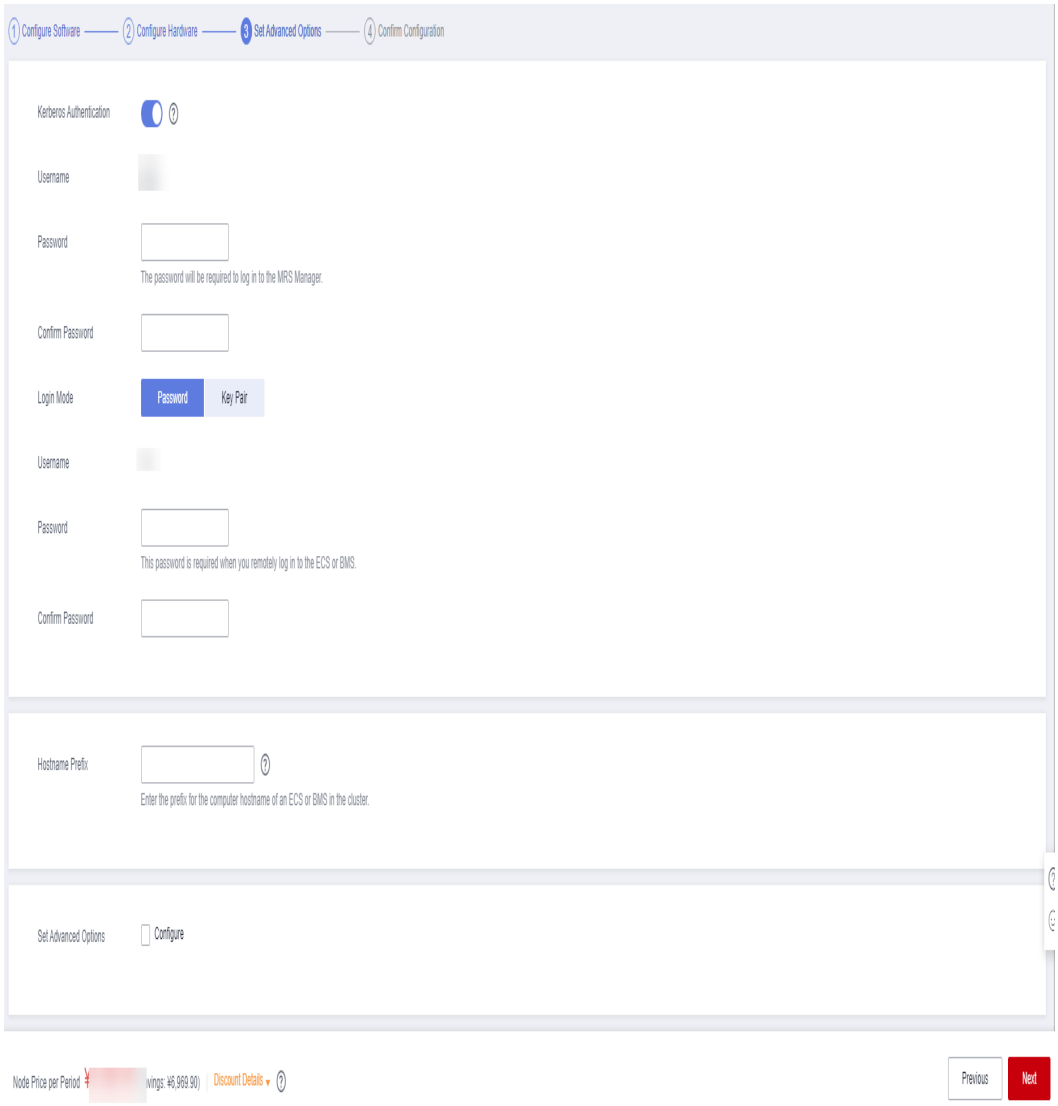
Para un clúster cuyo **Cluster Type** sea **Streaming cluster** o **Hybrid cluster**:

El sistema agrega automáticamente el **task_node_streaming_group** del grupo de nodos de task de streaming. Establezca el número de nodos, especificaciones de instancia y configuraciones de disco de nodo según sea necesario.

Si el grupo de nodos de task de streaming no es necesario, puede eliminarlo manualmente.

Paso 6 Establezca las opciones avanzadas haciendo referencia a **Opciones avanzadas**A continuación, haga clic en **Next**.

Figura 2-13 Configurar opciones avanzadas



Paso 7 En la página **Confirm Configuration**, compruebe la información de configuración del clúster. Si necesita ajustar la configuración, haga clic en para ir a la pestaña correspondiente y configurar los parámetros de nuevo.

Paso 8 Seleccione **Enable** para habilitar las comunicaciones seguras. Para obtener más información, consulte **Autorización de seguridad de comunicación**.

Paso 9 Haga clic en **Buy Now**.

Si la autenticación Kerberos está habilitada, compruebe si esta función es necesaria. Si lo es, haga clic en **Continue**. Si no es así, haga clic en **Back** para desactivarlo y, a continuación, continúe con el paso siguiente. El estado del control deslizante no se puede cambiar una vez que el clúster se ha comprado.

NOTA

Para cualquier duda sobre el precio, haga clic en **Pricing details** en la esquina inferior izquierda.

Paso 10 Haga clic en **Back to Cluster List** para ver el estado del clúster.

Para obtener más información sobre el estado del clúster durante la creación, consulte la descripción de los parámetros de estado en **Tabla 3-4**.

Se necesita algún tiempo para crear un clúster. El estado inicial del clúster es **Starting**. Una vez que el clúster se ha creado correctamente, el estado del clúster pasa a ser **Running**.

En la consola de gestión de MRS, se puede crear simultáneamente un máximo de 10 clústeres y se puede gestionar un máximo de 100 clústeres.

----Fin

Configuraciones de software

Tabla 2-1 Configuración del software del clúster MRS

Parámetro	Descripción
Region	Seleccione una **región**. Los productos de servicios en la nube de diferentes regiones no pueden comunicarse entre sí a través de una intranet. Para obtener una baja latencia de red y un rápido acceso a los recursos, seleccione la región más cercana.
Billing Mode	MRS proporciona dos modos de facturación. ● Anual/Mensual ● Pago por uso
Required Duration	Este parámetro es válido en modo de facturación anual/mensual e indica la duración de una suscripción de clúster. La duración mínima del clúster es de 1 mes y la duración máxima disponible del clúster es de 1 año. Si selecciona **Auto-renew**, las suscripciones mensuales se renuevan automáticamente cada mes y las suscripciones anuales se renuevan automáticamente cada año.
Cluster Name	El nombre del clúster debe ser único. Un nombre de clúster puede contener de 1 a 64 caracteres. Solo se permiten letras, dígitos, guiones medios (-) y guiones bajos (_). El nombre predeterminado es **mrs**_*xxxx*. *xxxx* es una colección aleatoria de letras y dígitos.

Parámetro	Descripción
Version Type	Los siguientes tipos de versión están disponibles: ● Normal: – Soporta operaciones básicas de clúster, como configuración, gestión y O&M. – Soporta componentes como Presto, Impala, Kudu, y Sqoop. ● LTS: – Además de las operaciones básicas del clúster, la versión LTS admite la actualización de la versión. – Soporta el despliegue de multi-AZ. – Soporta HetuEngine. El tipo de versión predeterminado es **Normal**.
Cluster Version	Actualmente, MRS 1.9.2, 3.1.0, 3.1.2-LTS.3, 3.1.5. La última versión de MRS se utiliza de forma predeterminada.
Cluster Type	Los tipos de clúster son los siguientes: ● **Analysis cluster**: se utiliza para el análisis de datos fuera de línea y proporciona componentes de Hadoop. ● **Streaming cluster**: se utiliza para tareas de streaming y proporciona componentes de procesamiento de stream. ● **Hybrid cluster** se utiliza tanto para el análisis de datos fuera de línea como para el procesamiento de streaming y proporciona componentes Hadoop y componentes de procesamiento de streaming. Se recomienda utilizar un clúster híbrido para realizar análisis de datos sin conexión y tareas de procesamiento de streaming al mismo tiempo. ● **Custom**: Puede ajustar el modo de despliegue del servicio de clúster en función de los requisitos del servicio. Para obtener más información, consulte **Compra de un clúster de topología personalizado**. (Este tipo solo está disponible actualmente en MRS 3.*x*.) **NOTA** ● Los clústeres de streaming de MRS no admiten funciones de gestión de archivos y trabajos. ● Para instalar todos los componentes de un clúster, seleccione **Custom**.
Component	Componentes del clúster de MRS. Para obtener más información sobre las versiones de componentes compatibles con diferentes versiones de clústeres MRS, consulte **Lista de versiones de componente de MRS**.

Parámetro	Descripción
Metadata	Si se utilizan fuentes de datos externas para almacenar metadatos. ● **Local**: Los metadatos se almacenan en el clúster local. ● **External data connection**: Se utilizan metadatos de fuentes de datos externas. Si el clúster es anormal o se elimina, los metadatos no se verán afectados. Este modo se aplica a escenarios en los que el almacenamiento y la computación están desacoplados. Los clústeres que admiten el componente Hive o Ranger admiten esta función.
Component	Este parámetro solo está disponible cuando **Metadata** está establecido en **External data connection**. Indica el tipo de origen de datos externo. ● Hive ● Ranger
Data Connection Type	Este parámetro solo está disponible cuando **Metadata** está establecido en **External data connection**. Indica el tipo de origen de datos externo. ● Hive admite los siguientes tipos de conexión de datos: – Base de datos de PostgreSQL de RDS – Base de datos de MySQL de RDS – Base de datos local ● Ranger admite los siguientes tipos de conexión de datos: – Base de datos de MySQL de RDS – Base de datos local
Data Connection Instance	Este parámetro solo es válido cuando **Data Connection Type** está establecido en **RDS PostgreSQL database** o **RDS MySQL database**. Este parámetro indica el nombre de la conexión entre el clúster de MRS y la base de datos de RDS. Esta instancia debe ser creada antes de ser referenciada aquí. Puede hacer clic en **Create Data Connection** para crear una conexión de datos. Para obtener más información, consulte **Configuración de conexiones de datos**.
Component port (supported only for the LTS version)	Política del puerto de comunicación predeterminado de cada componente en el clúster de MRS. ● Código abierto: Utilice el puerto proporcionado por el componente de código abierto. ● Personalizado: Personaliza un puerto para el componente. Para obtener más información sobre las diferencias entre el puerto de código abierto predeterminado y el puerto personalizado predeterminado, consulte **Interfaz de usuario web de componentes de código abierto**.

Configuraciones de hardware

Tabla 2-2 Configuración de hardware de clúster de MRS

Parámetro	Descripción
AZ	Seleccione **AZ** asociado a la región del clúster. Una zona de disponibilidad es un área física que utiliza energía independiente y recursos de red. Las AZ están físicamente aisladas, pero se interconectan a través de la red interna. Esto mejora la disponibilidad de las aplicaciones. Se recomienda crear clústeres en diferentes zonas de disponibilidad.
Enterprise Project	Seleccione el proyecto de empresa al que pertenece el clúster. Para utilizar un proyecto de empresa, cree uno en la página **Enterprise** > **Project Management**. La consola **Enterprise Management** del proyecto de empresa está diseñada para la gestión de recursos. Ayuda a las empresas a gestionar personal, recursos, permisos y finanzas basados en la nube de manera jerárquica, como la gestión de empresas, departamentos y proyectos.
VPC	Una VPC es un entorno de red seguro, aislado y lógico. Seleccione la VPC para la que desea crear un clúster y haga clic en **View VPC** para ver el nombre y el ID de la VPC. Si no hay ninguna VPC disponible, cree una.
Subnet	Una subred proporciona recursos de red dedicados que están aislados de otras redes, lo cual mejora la seguridad de la red. Seleccione la subred para la que desea crear un clúster. Haga clic en **View Subnet** para ver detalles sobre la subred seleccionada. Si no se crea ninguna subred en la VPC, vaya a la consola de la VPC y elija **Subnets** > **Create Subnet** para crear una. Para obtener detalles acerca de cómo configurar reglas de salida de ACL de red, vea **¿Cómo configuro una regla de salida de ACL de red?** **NOTA** El número de direcciones IP requeridas para crear un clúster MRS depende del número de nodos del clúster y de los componentes seleccionados, pero no del tipo de clúster. En MRS, las direcciones IP se asignan automáticamente a los clústeres durante la creación del clúster basándose básicamente en la siguiente fórmula: Cantidad de direcciones IP = Número de nodos de clúster + 2 (uno para Manager; uno para la base de datos). Además, si se seleccionan los componentes Hadoop, Hue, Sqoop y Presto o Loader y Presto durante el despliegue del clúster, se agrega una dirección IP para cada componente. Para un clúster de ClickHouse de forma independiente, el número de direcciones IP requeridas se calcula de la siguiente manera: Número de direcciones IP = Número de nodos de clúster + 1 (para Manager).

Parámetro	Descripción
Security Group	Un grupo de seguridad es un conjunto de reglas de acceso de ECS. Proporciona políticas de acceso para ECS que tienen los mismos requisitos de protección de seguridad y son de confianza mutua en una VPC. Al crear un clúster, puede seleccionar **Auto create** en la lista desplegable de **Security Group** para crear un grupo de seguridad o seleccionar un grupo de seguridad existente. **NOTA** Cuando seleccione un grupo de seguridad creado por usted mismo, asegúrese de que la regla de entrada contiene una regla en la que **Protocol** se establece en **All**, **Port** se establece en **All**, y **Source** se establece en un intervalo de direcciones IP accesible de confianza. No utilice **0.0.0.0/0** como dirección de origen. De lo contrario, pueden producirse riesgos de seguridad. Si no conoce el rango de direcciones IP accesibles de confianza, seleccione **Auto create**.
EIP	Después de vincular una EIP a un clúster MRS, puede utilizar la EIP para acceder a la interfaz de usuario web de Manager del clúster. Al crear un clúster, puede seleccionar una EIP disponible de la lista desplegable y vincularlo. Si no hay ninguna EIP disponible en la lista desplegable, haga clic en **Manage EIP** para acceder a la página de servicio de **EIPs** a uno. **NOTA** La EIP debe estar en la misma región que el clúster.

Tabla 2-3 Información del nodo de clúster

Parámetro	Descripción
CPU Architecture	Arquitectura de CPU soportada por MRS. Este parámetro no está disponible para MRS 3.1.0 y 3.1.5. ● **x86**: La arquitectura de CPU basada en x86 utiliza computación de conjuntos de instrucciones complejos (CISC). Cada instrucción se puede usar para ejecutar operaciones de hardware de bajo nivel. El número de instrucciones es grande, y la longitud de cada instrucción es diferente. Por lo tanto, ejecutar una instrucción de este tipo es compleja y requiere mucho tiempo. ● **Kunpeng**: La arquitectura de CPU basada en Kunpeng utiliza computación reducida de conjuntos de instrucciones (RISC). RISC es un microprocesador que ejecuta menos tipos de instrucciones de computadora pero a una velocidad más alta que CISC. RISC simplifica la arquitectura del ordenador y mejora la velocidad de funcionamiento. En comparación con la arquitectura de CPU basada en x86, la arquitectura de CPU basada en Kunpeng tiene una relación de rendimiento y consumo de energía más equilibrada. Kunpeng cuenta con la densidad alta, el consumo de energía bajo y la rentabilidad alta.
Common Node Configurations	Este parámetro solo está disponible cuando **Cluster Type** está establecido en **Custom**. Las opciones de valor incluyen **Compact**, **Full-size** y **OMS-separate**. Para obtener más información, consulte **Descripción de plantilla de clúster personalizado**.

Parámetro	Descripción
Node Group	Un clúster de MRS consta de varios nodos de ECS. Basado en diferentes especificaciones de nodo, el sistema gestiona los nodos en grupos de nodos. Los nodos de un clúster se clasifican en los siguientes tipos según los roles de los componentes desplegados en los nodos: ● Master: gestiona el clúster y asigna los archivos ejecutables del clúster a los nodos principales. rastrea el estado de ejecución de cada trabajo y monitorea el estado de ejecución del DataNode. ● Core: nodo de trabajo de clúster, que procesa y analiza datos y almacena datos de proceso. El sistema crea automáticamente un grupo de nodos de núcleo basado en los componentes contenidos en el clúster. Por ejemplo, si selecciona el componente de ClickHouse, el sistema agrega el grupo de nodos de ClickHouse y despliega el rol ClickHouseServer en el grupo de nodos de forma predeterminada. ● Tarea: proporciona recursos de cómputo, en los que Yarn y Storm (soportados solo por MRS 1.9.2) están instalados. Los nodos de tarea no almacenan datos persistentes. Cuando los recursos informáticos de un clúster son insuficientes, puede configurar políticas de escalado automático para aumentar automáticamente los nodos de tareas. Cuando el cambio de volumen de datos es pequeño en un clúster pero las capacidades de procesamiento de servicios del clúster necesitan mejorarse notablemente y temporalmente, agregue nodos de Task para abordar las siguientes situaciones: Para los clústeres cuyo **Cluster Type** sea **Analysis cluster**, **Streaming cluster** (soportado únicamente por MRS 1.9.2) o **Hybrid cluster**, el sistema agrega automáticamente el grupo de nodos de tarea correspondiente. Puede eliminar manualmente el grupo de nodos de tarea si no es necesario.
Payment Type	Modo de facturación de nodos en un clúster. ● El modo de facturación de los nodos principal y principal es el mismo que el del clúster. ● El modo de facturación de los nodos de Task se fija a Pago por uso, es decir, los nodos de Task en un clúster suscrito anual/mensual todavía se facturan en una base de pago por uso.

Parámetro	Descripción
Node Count	Configure la cantidad de nodos en cada grupo de nodos. ● Grupos de nodos de Master: El número de instancias de Master oscila entre 3 y 9. ● Debe existir al menos un nodo Core y el número total de nodos de Core y Task no puede superar los 10,000. Haga clic en  para agregar un grupo de nodos, haga clic en  para modificar las especificaciones de instancia de nodo y haga clic en  para eliminar el grupo de nodos agregado. **NOTA** Un pequeño número de nodos puede hacer que los clústeres se ejecuten lentamente, mientras que un gran número de nodos puede ser innecesariamente costoso. Establezca un valor apropiado basado en los datos que se van a procesar.

Parámetro	Descripción
Instance Specifications	Especificaciones de instancia de los nodos de Master o Core. MRS admite especificaciones de host determinadas por CPU, memoria y espacio en disco. Consulte **Especificaciones de ECS utilizadas por MRS** y para obtener las especificaciones de instancia permitidas. Haga clic en  para configurar las especificaciones de instancia, el disco del sistema y los parámetros del disco de datos del nodo del clúster. MRS admite especificaciones de BMS solo cuando el modo de facturación de un clúster es **Yearly/Monthly**. MRS admite el siguiente despliegue híbrido de **ECSs** y **BMSs**: ● Los nodos de Master, Core y Task se despliegan en los ECS. ● Los nodos de Master y Core se despliegan en los BMS, y los nodos de Task se despliegan en los ECS. ● Los nodos de Master se despliegan en ECS o BMS, los nodos de Core se despliegan en ECS o BMS y los nodos de Task se despliegan en ECS. Los tenants comparten recursos físicos de ECS, pero pueden usar exclusivamente recursos de BMS. Los BMS pueden satisfacer mejor sus requisitos para desplegar aplicaciones y servicios clave que requieren un alto rendimiento (como los clústeres de big data y los sistemas de middleware empresarial) y un entorno de ejecución seguro y confiable. Si se usan especificaciones de BMS, las especificaciones de nodo de Master no se pueden escalar. **NOTA** ● Las especificaciones de instancia más avanzadas proporcionan un mejor procesamiento de datos. Sin embargo, requieren un mayor costo de clúster. ● Si selecciona HDD para nodos de Core, no hay información de facturación para los discos de datos. Las tarifas se cobran con ECS. ● Si selecciona discos que no son HDD para los nodos de Core, **Data Disk** determina los tipos de disco de los nodos de Master y Core. ● Si **Sold out** aparece junto a una especificación de instancia de un nodo, el nodo de esta especificación no se puede . Solo puede nodos de otras especificaciones. ● La especificación del nodo de Master (4 vCPUs 8 GB) no está dentro del ámbito de posventa del SLA. Es aplicable solo al entorno de prueba y no se recomienda para el entorno de producción. ● Para MRS 3.*x* o posterior, la memoria del nodo de master debe ser mayor que 64 GB.

Parámetro	Descripción
System Disk	Tipo de almacenamiento y espacio de almacenamiento del disco del sistema en un nodo. El tipo de almacenamiento puede ser cualquiera de los siguientes: ● **SATA**: E/S común ● **SAS**: E/S alta ● **SSD**: E/S ultra alta ● **GPSSD**: SSD de uso general
Data Disk	Espacio de almacenamiento en disco de datos de un nodo. Para aumentar la capacidad de almacenamiento de datos, puede agregar discos al mismo tiempo al crear un clúster. Los siguientes dos escenarios de aplicación están involucrados. ● El almacenamiento de datos y la computación están separados. Los datos se almacenan en OBS, que cuenta con un bajo costo y capacidad de almacenamiento ilimitada. Los clústeres se pueden terminar en cualquier momento en OBS. El rendimiento informático está determinado por el rendimiento de acceso de OBS y es menor que el de HDFS. Esta configuración se recomienda si la computación de datos es poco frecuente. ● El almacenamiento de datos y la computación no están separados. Los datos se almacenan en HDFS, lo que ofrece un alto costo, un alto rendimiento informático y una capacidad de almacenamiento limitada. Antes de terminar los clústeres, debe exportar y almacenar los datos. Esta configuración se recomienda si la computación de datos es frecuente. El tipo de almacenamiento puede ser cualquiera de los siguientes: ● SATA: E/S común ● SAS: E/S alta ● SSD: E/S ultra alta ● GPSSD: SSD de uso general **NOTA** Más nodos de un clúster requieren una mayor capacidad de disco que los nodos de Master. Para garantizar un funcionamiento estable del clúster, establezca la capacidad de disco del nodo de Master en más de 600 GB si el número de nodos es 300 y aumente a más de 1 TB si el número de nodos alcanza 500.

Parámetro	Descripción
LVM	Este parámetro es válido solo cuando se crea un nodo de Core de streaming. Haga clic en este parámetro para habilitar o deshabilitar la función de gestión LVM de disco. Este parámetro no está disponible en MRS 3.*x* y versiones posteriores. Si LVM está habilitado, todos los discos de un nodo se montan como volúmenes lógicos. Esto proporciona una planificación más adecuada del disco para evitar el sesgo de datos, lo que mejora la estabilidad del sistema.
Topology Adjustment	Si el modo de despliegue en **Common Node** no cumple con los requisitos, establezca **Topology Adjustment** en **Enable** y ajuste el modo de despliegue de instancia según los requisitos de servicio. Para obtener más información, consulte **Ajuste de topología para un clúster personalizado**. Este parámetro solo es válido cuando **Cluster Type** está establecido en **Custom**.

Opciones avanzadas

Tabla 2-4 Topología de configuración avanzada de clúster MRS

Parámetro	Descripción
Kerberos Authentication	Si se debe habilitar la autenticación Kerberos al iniciar sesión en Manager. El estado del control deslizante no se puede cambiar una vez que el clúster se ha comprado. ●  : Si **Kerberos Authentication** está deshabilitado, los usuarios comunes pueden usar todas las funciones de un clúster de MRS. Se recomienda deshabilitar la autenticación de Kerberos en escenarios de un solo usuario. Si la autenticación de Kerberos está deshabilitada, puede seguir las instrucciones en **Sugerencias de configuración de seguridad para clústeres con autenticación de Kerberos deshabilitada** para realizar la configuración de seguridad. ●  : Si **Kerberos Authentication** está habilitado, los usuarios comunes no pueden usar las funciones de gestión de archivos y trabajos de un clúster MRS y no pueden ver el uso de recursos del clúster o los registros de trabajos de Hadoop y Spark. Para utilizar más funciones de clúster, los usuarios deben ponerse en contacto con el administrador de Manager para asignar más permisos. Se recomienda habilitar la autenticación de Kerberos en escenarios multiusuario. ● Actualmente, Presto no admite la autenticación de Kerberos.

Parámetro	Descripción
Username	Nombre del administrador de Manager. **admin** se utiliza de forma predeterminada.
Password	Contraseña del administrador de Manager Se deben cumplir los siguientes requisitos: ● Debe contener de 8 a 26 caracteres. ● Debe contener al menos cuatro de los siguientes: – Letras en minúscula – Letras en mayúscula – Dígitos – Tiene al menos uno de los siguientes caracteres especiales: !?,.: -_{} [ ]@ $% ^ + = / ● No puede ser el mismo que el nombre de usuario o el nombre de usuario escrito al revés. Fuerza de la contraseña: La barra de colores en rojo, naranja y verde indica una contraseña débil, mediana y fuerte, respectivamente.
Confirm Password	Ingrese de nuevo la contraseña del administrador del Manager.

Parámetro	Descripción
Login Mode	● Contraseña Inicie sesión en el ECS o BMS como usuario **root**. Introduzca la contraseña del usuario **root** y confirme la contraseña. Una contraseña debe cumplir con los siguientes requisitos: 1. Debe tener una cadena de 8 a 26 caracteres. 2. La contraseña debe contener al menos cuatro tipos de los siguientes caracteres: letras mayúsculas, minúsculas, dígitos y caracteres especiales (! ?,.: -_{} [ ]@ $% ^ + = /). 3. La contraseña no puede ser el nombre de usuario o el nombre de usuario inverso. ● Par de claves Los pares de claves se utilizan para iniciar sesión en los nodos ECS del clúster. Seleccione un par de claves en la lista desplegable. Seleccione "I acknowledge that I have obtained private key file *SSHkey-xxx* and that without this file I will not be able to log in to my ECS." Si nunca ha creado un par de claves, haga clic en **View Key Pair** para crear o importar un par de claves. Y luego, obtener un archivo de clave privada. Un par de claves, también llamado clave SSH, consiste en una clave pública y una clave privada. Puede crear una clave SSH y descargar la clave privada para autenticar el inicio de sesión remoto. Por seguridad, una clave privada solo se puede descargar una vez. Manténgalo seguro. Utilice una clave SSH en cualquiera de los dos métodos siguientes: 1. Creación de una clave SSH: Después de crear una clave SSH, se generan una clave pública y una clave privada. La clave pública se almacena en el sistema, y la clave privada se almacena en el ECS local. Cuando inicia sesión en un ECS, las claves públicas y privadas se utilizan para la autenticación. 2. Importación de una clave SSH: Si ha obtenido las claves públicas y privadas, importe la clave pública en el sistema. Cuando inicia sesión en un ECS, las claves públicas y privadas se utilizan para la autenticación.
Hostname Prefix	Introduzca el prefijo para el nombre de host del equipo de un ECS o BMS en el clúster.
Setting Advanced Options	Parámetros de función avanzados de un clúster de MRS. Seleccione **Configure**. Para obtener más información, consulte **Tabla 2-5**.

Tabla 2-5 (Opcional) Información de configuración avanzada del clúster de MRS

Parámetro	Descripción
Tag	Para obtener más información, consulte **Adición de una etiqueta a un clúster**.
Auto Scaling	El escalado automático solo se puede configurar después de especificar las especificaciones del nodo de tarea en el paso **Configure Hardware** haciendo referencia a **Configuración de reglas de escalado automático**.
Bootstrap Action	Para obtener más información, consulte **Adición de una acción de arranque**.
Agency	Al vincular una delegación, los ECS o BMS pueden gestionar algunos de sus recursos. Determine si se debe configurar una delegación en función del escenario de servicio real. Por ejemplo, puede configurar una delegación del tipo de ECS para obtener automáticamente el AK/SK para acceder a OBS. La delegación **MRS_ECS_DEFAULT_AGENCY** tiene el permiso OBSOperateAccess de OBS y los permisos CESFullAccess (para usuarios que han habilitado políticas detalladas), CES Administrator y KMS Administrator en la región donde se encuentra el clúster.
Metric Sharing	Se recopilan métricas de monitoreo de componentes de big data. Si se produce un error al usar un clúster, comparta las métricas de monitoreo con Huawei Cloud para la solución de problemas. Este parámetro no está disponible en MRS 3.*x*.
Data Disk Encryption	Si se deben cifrar datos en el disco de datos montado en el clúster. Esta función está deshabilitada por defecto. Para utilizar esta función, debe tener los permisos de Security Administrator y KMS Administrator. Este parámetro no está disponible para MRS 3.1.0 y MRS 3.1.2-LTS.3. Las claves utilizadas por los discos de datos cifrados son proporcionadas por el Key Management Service (KMS) del Data Encryption Workshop (DEW), seguro y conveniente. Por lo tanto, no es necesario establecer y mantener la infraestructura de gestión de claves. Haga clic en **Data Disk Encryption** para habilitar o deshabilitar la función de encriptación del disco de datos. Para obtener más información, consulte **Encriptación de disco de EVS**.
Data Disk Key ID	Este parámetro sólo se muestra cuando la función **Data Disk Encryption** está activada. Este parámetro indica el ID de clave correspondiente al nombre de clave seleccionado. Este parámetro no está disponible para MRS 3.1.0 y MRS 3.1.2-LTS.3.

Parámetro	Descripción
Data Disk Key Name	Este parámetro es obligatorio cuando la función **Data Disk Encryption** está activada. Seleccione el nombre de la clave utilizada para cifrar el disco de datos. De forma predeterminada, se selecciona la clave maestra predeterminada denominada **evs/default**. Puede seleccionar otra clave maestra de la lista desplegable. Este parámetro no está disponible para MRS 3.1.0 y MRS 3.1.2-LTS.3. Si los discos se cifran mediante un CMK, que luego se deshabilita o se programa para su eliminación, los discos ya no se pueden leer ni escribir en, y es posible que los datos de estos discos nunca se restablezcan. Tenga cuidado al realizar esta operación. Haga clic en **View Key List** para introducir una página en la que pueda crear y gestionar claves.
Alarm	Si la función de alarma está habilitada, se puede notificar al personal de mantenimiento del clúster de manera oportuna para localizar fallas cuando el clúster funciona de manera anormal o el sistema está defectuoso.
Rule Name	Nombre de la regla para enviar mensajes de alarma. El valor solo puede contener letras, dígitos, puntos (.), guiones (-) y guiones bajos (_).
Topic Name	Seleccione un tema existente o haga clic en **Create Topic** para crear un tema. Para enviar mensajes publicados en un tema, debe agregar un suscriptor al tema. Para obtener más información, consulte **Adición de suscripciones a un tema**. Un tema sirve como un canal de envío de mensajes, donde los editores y suscriptores pueden interactuar entre sí.
Logging	Si se recopilan registros cuando se produce un error en la creación de clústeres. Una vez habilitada la función de registro, los registros del sistema y los registros de ejecución de componentes se recopilan automáticamente y se guardan en el sistema de archivos de OBS en escenarios como fallas de creación de clústeres y fallas de escalamiento horizontal o de escalamiento horizontal para que el personal de O&M localice rápidamente las fallas. La información de registro se conserva durante un máximo de siete días.

Error al crear un clúster

Si no se crea un clúster, la tarea fallida se gestionará en la página **Manage Failed Tasks**. Elija **Clusters** > **Active Clusters**. Haga clic en  en **Figura 2-14** para ir a la página **Manage Failed Tasks**. En la columna **Task Status**, coloque el cursor sobre  para ver la causa del error. Consulte **Figura 2-15**. Puede eliminar las tareas fallidas haciendo referencia a **Consulta de tareas de MRS fallidas**.

Figura 2-14 Gestión de tarea fallida

Figura 2-15 Causa de la falla

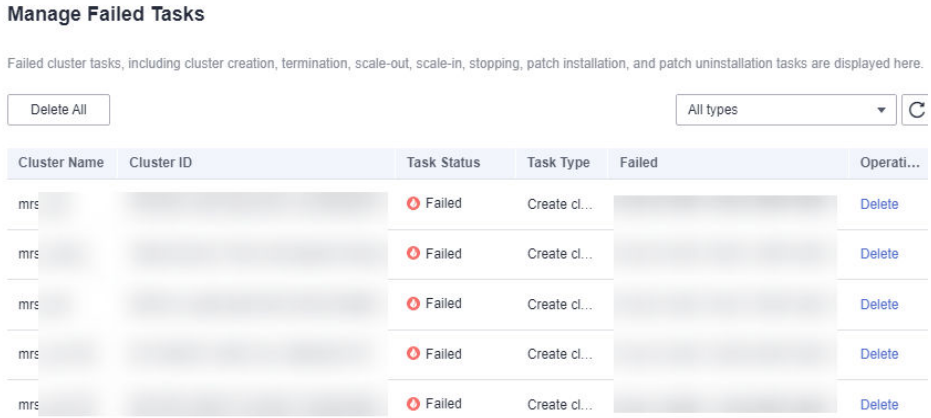


Tabla 2-6 enumera los códigos de error de los errores de creación de clústeres de MRS.

Tabla 2-6 Códigos de error

Código de error	Descripción
MRS.101	Cuota insuficiente para satisfacer su solicitud. Comuníquese con el servicio de atención al cliente para incrementar la cuota.
MRS.102	El token no puede ser nulo ni inválido. Vuelva a intentarlo más tarde o póngase en contacto con el servicio al cliente.
MRS.103	Solicitud no válida. Vuelva a intentarlo más tarde o póngase en contacto con el servicio al cliente.
MRS.104	Recursos insuficientes. Vuelva a intentarlo más tarde o póngase en contacto con el servicio al cliente.
MRS.105	Direcciones IP insuficientes en la subred existente. Vuelva a intentarlo más tarde o póngase en contacto con el servicio al cliente.
MRS.201	Error debido a un error de ECS. Vuelva a intentarlo más tarde o póngase en contacto con el servicio al cliente.
MRS.202	Error debido a un error de IAM. Vuelva a intentarlo más tarde o póngase en contacto con el servicio al cliente.
MRS.203	Error debido a un error de VPC. Vuelva a intentarlo más tarde o póngase en contacto con el servicio al cliente.
MRS.400	Error del sistema de MRS. Vuelva a intentarlo más tarde o póngase en contacto con el servicio al cliente.

2.4 Compra de un clúster de topología personalizado

El clúster de análisis, el clúster de streaming y el clúster híbrido proporcionados por MRS utilizan plantillas fijas para desplegar procesos de clúster. Por lo tanto, no puede personalizar los procesos de servicio en los nodos de gestión y los nodos de control. Si desea personalizar el despliegue del clúster, establezca **Cluster Type** en **Custom** al crear un clúster. De esta manera, puede personalizar el modo de despliegue de las instancias de proceso en los nodos de gestión y los nodos de control en el clúster. Solo MRS 3.x y versiones posteriores admiten la creación de clústeres en una topología personalizada.

Un clúster personalizado proporciona las siguientes funciones:

- Despliegue separado de los roles de gestión y control: El rol de gestión y el rol de control se despliegan en diferentes nodos de Master.
- Despliegue conjunto de los roles de gestión y control: Los roles de gestión y control se despliegan conjuntamente en el nodo de Master.
- ZooKeeper se despliega en un nodo independiente para mejorar la confiabilidad.
- Los componentes se despliegan por separado para evitar la contención de recursos.

Roles en un clúster MRS:

- Nodo de gestión (MN): es el nodo para instalar Manager (el sistema de gestión del clúster MRS). Proporciona una entrada de acceso unificada. El administrador gestiona de forma centralizada los nodos y los servicios desplegados en el clúster.
- Nodo de control (CN): controla y monitorea cómo los nodos de datos almacenan y reciben datos, y envían el estado del proceso, y proporciona otras funciones públicas. Los nodos de control de MRS incluyen HMaster, HiveServer, ResourceManager, NameNode, JournalNode y SlapdServer.
- Nodo de datos (DN): Un nodo de datos ejecuta las instrucciones enviadas por el nodo de gestión, informa del estado de la tarea, almacena datos y proporciona otras funciones públicas. Los nodos de datos de MRS incluyen DataNode, RegionServer y NodeManager.

Personalización de un clúster

Paso 1 Inicie sesión en la consola de MRS.

Paso 2 Haga clic en **Buy Cluster**. Se muestra la página para comprar un clúster.

Paso 3 En la página para comprar un clúster, haga clic en la pestaña **Custom Config**.

Paso 4 Configure la información básica del clúster. Para obtener más información sobre los parámetros, consulte **Configuraciones de software**.

- **Region**: Conserva el valor predeterminado.
- **Billing Mode**: Seleccione **Yearly/Monthly** o **Pay-per-use**.
- **Cluster Name**: Puede utilizar el nombre predeterminado. Sin embargo, se recomienda incluir una abreviatura de nombre de proyecto o fecha para la memoria consolidada y fácil de distinguir, por ejemplo, **mrs_20180321**.
- **Cluster Version**: Actualmente, solo MRS 3.*x* está disponible.
- **Cluster Type**: Seleccione **Custom** y seleccione los componentes según sea necesario.

Paso 5 Haga clic en **Next**. Configurar la información de hardware.

- **AZ**: Conservar el valor predeterminado.
- **Enterprise Project**: Conserve el valor predeterminado.
- **VPC**: Conservar el valor predeterminado. Si no hay una VPC disponible, haga clic en **View VPC** para acceder a la consola de VPC y crear una nueva VPC.
- **Subnet**: Conservar el valor predeterminado.
- **Security Group**: Seleccione **Auto create**.
- **EIP**: Seleccione **Bind later**.
- **CPU Architecture**: Conservar el valor predeterminado. Este parámetro no está disponible en MRS 3.x.
- **Common Node**: Para más información, véase **Descripción de plantilla de clúster personalizado**.
- **Node Count**: Ajustar el número de instancias de clúster según el volumen de servicio. Para obtener más información, consulte **Tabla 2-8**.
- **Instance Specifications**: Haga clic en  para configurar las especificaciones de instancia, los tipos de almacenamiento de disco de sistema y disco de datos y el espacio de almacenamiento.
- **Topology Adjustment**: si el modo de despliegue en **Common Node** no cumple los requisitos, debe instalar manualmente algunas instancias que no se despliegan de forma predeterminada, o debe instalar manualmente algunas instancias, establecer **Topology Adjustment** en **Enable** y ajustar el modo de despliegue de instancia en función de los requisitos de servicio. Para obtener más información, consulte **Ajuste de topología para un clúster personalizado**.

Paso 6 Haga clic en **Next** y configure las opciones avanzadas.

Para obtener más información sobre los parámetros, consulte **Opciones avanzadas**.

Paso 7 Haga clic en **Next**.

En la página **Confirm Configuration**, compruebe la información de configuración del clúster. Si necesita ajustar la configuración, haga clic en  para ir a la pestaña correspondiente y configurar los parámetros de nuevo.

Paso 8 Seleccione **Enable** para habilitar las comunicaciones seguras. Para obtener más información, consulte **Autorización de seguridad de comunicación**.

Paso 9 Haga clic en **Buy Now**.

Si la autenticación de Kerberos está habilitada para un clúster, compruebe si es necesaria la autenticación de Kerberos. En caso afirmativo, haga clic en **Continue**. Si no, haga clic en **Back** para deshabilitar la autenticación de Kerberos y, a continuación, cree un clúster.

Paso 10 Haga clic en **Back to Cluster List** para ver el estado del clúster.

Se necesita algún tiempo para crear un clúster. El estado inicial del clúster es **Starting**. Una vez que el clúster se ha creado correctamente, el estado del clúster pasa a ser **Running**.

----Fin

Descripción de plantilla de clúster personalizado

Tabla 2-7 Plantillas comunes para clústeres personalizados

Nodo común	Descripción	Rango de nodos
Compact	El rol de gestión y el rol de control se despliegan en el nodo de Master y las instancias de datos se despliegan en el mismo grupo de nodos. Este modo de despliegue se aplica a escenarios en los que el número de nodos de control es inferior a 100, lo que reduce los costos.	● El número de nodos de Master es mayor que o igual a 3 y menor que o igual a 11. ● El número total de grupos de nodos es menor o igual que 10, y el número total de nodos en grupos de nodos no Master es menor o igual que 10,000.
OMS-separate	El rol de gestión y el rol de control se despliegan en diferentes nodos de Master, y las instancias de datos se despliegan en el mismo grupo de nodos. Este modo de despliegue es aplicable a un clúster con 100 a 500 nodos y ofrece un mejor rendimiento en escenarios de carga de alta simultaneidad.	● El número de nodos de Master es mayor o igual que 5 y menor o igual que 11. ● El número total de grupos de nodos es menor o igual que 10, y el número total de nodos en grupos de nodos no Master es menor o igual que 10,000.
Full-size	El rol de gestión y el rol de control se despliegan en diferentes nodos de Master, y las instancias de datos se despliegan en diferentes grupos de nodos. Este modo de despliegue es aplicable a un clúster con más de 500 nodos. Los componentes se pueden desplegar por separado, lo que se puede utilizar para una escala de clúster más grande.	● El número de nodos de Master es mayor o igual que 9 y menor o igual que 11. ● El número total de grupos de nodos es menor o igual que 10, y el número total de nodos en grupos de nodos no Master es menor o igual que 10,000.

Tabla 2-8 Esquema de despliegue de nodos de un clúster MRS personalizado

Principio de despliegue de nodos		Escenario de aplicación	Regla de redes
Los nodos de gestión, los nodos de control y los nodos de datos se despliegan por separado. (Este esquema requiere al menos ocho nodos.)	MN × 2 + CN × 9 + DN × n	(Recomendado) Este esquema se utiliza cuando el número de nodos de datos es de 500 a 2000.	● Si el número de nodos en un grupo excede de 200, los nodos se distribuyen a diferentes subredes y las subredes se interconectan entre sí en la Capa 3 usando conmutadores de núcleo. Cada subred puede contener un máximo de 200 nodos y la asignación de nodos a diferentes subredes debe estar equilibrada. ● Si el número de nodos es inferior a 200, los nodos del clúster se despliegan en la misma subred y los nodos se interconectan entre sí en la capa 2 mediante conmutadores de agregación.
	MN × 2 + CN × 5 + DN × n	(Recomendado) Este esquema se usa cuando el número de nodos de datos es de 100 a 500.	
	MN × 2 + CN × 3 + DN × n	(Recomendado) Este esquema se usa cuando el número de nodos de datos es de 30 a 100.	
Los nodos de gestión y los nodos de control se despliegan juntos, y los nodos de datos se despliegan por separado.	(MN+CN) × 3 + DN × n	(Recomendado) Este esquema se usa cuando el número de nodos de datos es de 3 a 30.	Los nodos del clúster se despliegan en la misma subred y se interconectan entre sí en la capa 2 a través de conmutadores de agregación.

Principio de despliegue de nodos	Escenario de aplicación	Regla de redes
Los nodos de gestión, los nodos de control y los nodos de datos se despliegan juntos.	● Este esquema es aplicable a un clúster que tiene menos de 6 nodos. ● Este esquema requiere al menos tres nodos. **NOTA** Esta plantilla no se recomienda en el entorno de producción o comercial. ● Si los nodos de gestión, control y datos se implementan conjuntamente, el rendimiento y la confiabilidad del clúster se ven muy afectados. ● Si el número de nodos cumple con los requisitos, despliegue los nodos de datos por separado. ● Si el número de nodos es insuficiente para admitir nodos de datos desplegados por separado, utilice el modo de red de doble plano para este escenario. El tráfico de la red de gestión se aísla del de la red de servicio para evitar volúmenes de datos excesivos en el plano de servicio, asegurando la correcta entrega de las operaciones de gestión.	Los nodos del clúster se despliegan en la misma subred y se interconectan entre sí en la capa 2 a través de conmutadores de agregación.

Ajuste de topología para un clúster personalizado

Tabla 2-9 Ajuste de topología

Servicio	Dependencia	Rol	Sugerencias de despliegue de roles	Descripción
OMSServer	-	OMSServer	Este rol se puede desplegar en el nodo de Master y no se puede modificar.	-

Servicio	Dependencia	Rol	Sugerencias de despliegue de roles	Descripción
ClickHouse	Depende de ZooKeeper.	CHS (ClickHouseServer)	Este rol se puede desplegar en todos los nodos. Número de instancias de rol a desplegar: un número par comprendido entre 2 y 256	Un grupo de nodos que no sea Master con este rol asignado se considera como un nodo Core.
		CLB (ClickHouseBalancer)	Este rol se puede desplegar en todos los nodos. Número de instancias de rol que se desplegarán: 2 a 256	-
ZooKeeper	-	QP(quorumpeer)	Este rol solo se puede desplegar en el nodo de Master. Número de instancias de rol a desplegar: De 3 a 9, con un tamaño de paso de 2	-
Hadoop	Depende de ZooKeeper.	NN(NameNode)	Este rol solo se puede desplegar en el nodo de Master. Número de instancias de rol a desplegar: 2	-
		HFS (HttpFS)	Este rol solo se puede desplegar en el nodo de Master. Número de instancias de rol que se desplegarán: 0 a 10	-
		JN(JournalNode)	This role can be deployed on the Master node only. Number of role instances to be deployed: 3 to 60, with the step size of 2	-

Servicio	Dependencia	Rol	Sugerencias de despliegue de roles	Descripción
		DN(DataNode)	Este rol se puede desplegar en todos los nodos. Número de instancias de rol a desplegar: De 3 a 10,000	Un grupo de nodos que no sea Master con este rol asignado se considera como un nodo Core.
		RM(ResourceManager)	Este rol solo se puede desplegar en el nodo de Master. Número de instancias de rol a desplegar: 2	-
		NM(NodeManager)	Este rol se puede desplegar en todos los nodos. Número de instancias de rol a desplegar: De 3 a 10,000	-
		JHS(JobHistoryServer)	Este rol solo se puede desplegar en el nodo de Master. Número de instancias de rol a desplegar: 1 a 2	-
		TLS(TimelineServer)	Este rol solo se puede desplegar en el nodo de Master. Número de instancias de rol a desplegar: 0 a 1	-
Presto	Depende de Hive.	PCD(Coordinator)	Este rol solo se puede desplegar en el nodo de Master. Número de instancias de rol a desplegar: 2	-
		PWK(Worker)	Este rol se puede desplegar en todos los nodos. Número de instancias de rol a desplegar: 1 a 10,000	-

Servicio	Dependencia	Rol	Sugerencias de despliegue de roles	Descripción
Spark2x	● Depende de Hadoop. ● Depende de Hive. ● Depende de ZooKeeper.	JS2X(JDBCServer2x)	Este rol solo se puede desplegar en el nodo de Master. Número de instancias de rol que se desplegarán: 2 a 10	-
		JH2X(JobHistory2x)	Este rol solo se puede desplegar en el nodo de Master. Número de instancias de rol a desplegar: 2	-
		SR2X(SparkResource2x)	Este rol solo se puede desplegar en el nodo de Master. Número de instancias de rol que se desplegarán: 2 a 50	-
		IS2X(IndexServer2x)	(Opcional) Este rol solo se puede desplegar en el nodo de Master. Número de instancias de rol a desplegar: 0 a 2, con un tamaño de paso de 2	-
HBase	Depende de Hadoop.	HM(HMaster)	Este rol solo se puede desplegar en el nodo de Master. Número de instancias de rol a desplegar: 2	-
		TS(ThriftServer)	Este rol se puede desplegar en todos los nodos. Número de instancias de rol a desplegar: 0 a 10,000	-
		RT(RESTServer)	Este rol se puede desplegar en todos los nodos. Número de instancias de rol a desplegar: 0 a 10,000	-

Servicio	Dependencia	Rol	Sugerencias de despliegue de roles	Descripción
		RS(RegionServer)	Este rol se puede desplegar en todos los nodos. Número de instancias de rol a desplegar: De 3 a 10,000	-
		TS1(Thrift1Server)	Este rol se puede desplegar en todos los nodos. Número de instancias de rol a desplegar: 0 a 10,000	Si el servicio Hue está instalado en un clúster y HBase necesita usarse en la interfaz de usuario web Hue, instale esta instancia para el servicio HBase.
Hive	● Depende de Hadoop. ● Depende de DBService.	MS(MetaStore)	Este rol solo se puede desplegar en el nodo de Master. Número de instancias de rol que se desplegarán: 2 a 10	-
		WH(WebHCat)	Este rol solo se puede desplegar en el nodo de Master. Número de instancias de rol que se desplegarán: 1 a 10	-
		HS(HiveServer)	Este rol solo se puede desplegar en el nodo de Master. Número de instancias de rol que se desplegarán: 2 a 80	-
Hue	Depende de DBService.	H(Hue)	Este rol solo se puede desplegar en el nodo de Master. Número de instancias de rol a desplegar: 2	-
Sqoop	Depende de Hadoop.	SC(Sqoop Client)	Este rol se puede desplegar en todos los nodos. Número de instancias de rol a desplegar: 1 a 10,000	-

Servicio	Dependencia	Rol	Sugerencias de despliegue de roles	Descripción
Kafka	Depende de ZooKeeper.	B(Broker)	Este rol se puede desplegar en todos los nodos. Número de instancias de rol a desplegar: De 3 a 10,000	-
Flume	-	MS(MonitorServer)	Este rol solo se puede desplegar en el nodo de Master. Número de instancias de rol a desplegar: 1 a 2	-
		F(Flume)	Este rol se puede desplegar en todos los nodos. Número de instancias de rol a desplegar: 1 a 10,000	Un grupo de nodos que no sea Master con este rol asignado se considera como un nodo Core.
Tez	● Depende de Hadoop. ● Depende de DBService. ● Depende de ZooKeeper.	TUI(TezUI)	Este rol solo se puede desplegar en el nodo de Master. Número de instancias de rol a desplegar: 1 a 2	-
Flink	● Depende de ZooKeeper. ● KrbServer ● DBService ● Depende de Hadoop.	FR(FlinkResource)	Este rol se puede desplegar en todos los nodos. Número de instancias de rol a desplegar: 1 a 10,000	-
		FS(FlinkServer)	Este rol se puede desplegar en todos los nodos. Número de instancias de rol que se desplegarán: 0 a 2	-

Servicio	Dependencia	Rol	Sugerencias de despliegue de roles	Descripción
Oozie	● Depende de Hadoop. ● Depende de DBService. ● Depende de ZooKeeper.	O(oozie)	Este rol solo se puede desplegar en el nodo de Master. Número de instancias de rol a desplegar: 2	-
Impala	● Depende de Hadoop. ● Depende de Hive. ● Depende de DBService. ● Depende de ZooKeeper.	StateStore	Este rol solo se puede desplegar en el nodo de Master. Número de instancias de rol que se desplegarán: 1	-
		Catalog	Este rol solo se puede desplegar en el nodo de Master. Número de instancias de rol que se desplegarán: 1	-
		Impalad	Este rol se puede desplegar en todos los nodos. Número de instancias de rol a desplegar: 1 a 10,000	-
Kudu	-	KuduMaster	Este rol solo se puede desplegar en el nodo de Master. Número de instancias de rol que se desplegarán: 3 o 5	-
		KuduTserver	Este rol se puede desplegar en todos los nodos. Número de instancias de rol a desplegar: De 3 a 10,000	-

Servicio	Dependencia	Rol	Sugerencias de despliegue de roles	Descripción
Ranger	Depende de DBService.	RA(RangerAdmin)	Este rol solo se puede desplegar en el nodo de Master. Número de instancias de rol a desplegar: 1 a 2	-
		USC(UserSync)	Este rol solo se puede desplegar en el nodo de Master. Número de instancias de rol que se desplegarán: 1	-
		TSC (TagSync)	Este rol se puede desplegar en todos los nodos. Número de instancias de rol a desplegar: 0 a 1	-
HetuEngine (aplicable únicamente a MRS 3.1.2-LTS.3)	● Depende de Hadoop. ● Depende de DBService. ● Depende de Hive. ● Depende de ZooKeeper.	HSB(HSBroker)	Este rol se puede desplegar en todos los nodos. Número de instancias de rol que se desplegarán: 2 a 50	-
		HSC(HSConsole)	Este rol se puede desplegar en todos los nodos. Número de instancias de rol a desplegar: 2	-
		HSF(HSFabric)	Este rol se puede desplegar en todos los nodos. Número de instancias de rol que se desplegarán: 0 a 50	-

2.5 Adición de una etiqueta a un clúster

Las etiquetas se utilizan para identificar clústeres. Agregar etiquetas a los clústeres puede ayudarlo a identificar y gestionar los recursos del clúster.

Puede agregar un máximo de 10 etiquetas a un clúster al crear el clúster o agregarlas en la página de detalles del clúster creado.

Una etiqueta consiste en una clave de etiqueta y un valor de etiqueta. **Tabla 2-10** proporciona la clave de etiqueta y los requisitos de valor.

Tabla 2-10 Clave de etiquetas y requisitos de valor

Parámetro	Requerimiento	Ejemplo
Key	Una clave de etiqueta no se puede dejar en blanco. Una clave de etiqueta debe ser única en un clúster. Una clave de etiqueta contiene un máximo de 36 caracteres. Un valor de etiqueta no puede contener caracteres especiales (=*<>\,|/) ni empezar o terminar con espacios.	Organization
Value	Un valor de etiqueta contiene un máximo de 43 caracteres. Un valor de etiqueta no puede contener caracteres especiales (=*<>\,|/) ni empezar o terminar con espacios. Este parámetro se puede dejar en blanco.	Apache

Adición de etiquetas a un clúster

Puede realizar las siguientes operaciones para agregar etiquetas a un clúster al crear el clúster.

1. Inicie sesión en la consola de MRS.
2. Haga clic en Comprar **Cluster**. Se muestra la página correspondiente.
3. Haga clic en la pestaña **Custom Config**.
4. Para configurar el software y el hardware del clúster, consulte **Compra de un clúster personalizado**.
5. En la página de pestaña **Set Advanced Options**, agregue una etiqueta.

   Ingrese la clave y el valor de una etiqueta que se agregará.

   Puede agregar un máximo de 10 etiquetas a un clúster y usar intersecciones de etiquetas para buscar el clúster de destino.

   NOTA

   También puede agregar etiquetas a clústeres existentes. Para obtener más información, consulte **Gestión de etiquetas**.

Búsqueda del clúster de destino

En la página **Active Clusters**, busque el clúster de destino por clave de etiqueta o valor de etiqueta.

1. Inicie sesión en la consola de MRS.
2. En la esquina superior derecha de la página **Active Clusters**, haga clic en **Search by Tag** para acceder a la página de búsqueda.
3. Ingrese la etiqueta del clúster que se va a buscar.

   Puede seleccionar una clave de etiqueta o un valor de etiqueta de sus listas desplegables. Cuando la clave de etiqueta o el valor de etiqueta coinciden exactamente, el sistema puede localizar automáticamente el clúster de destino. Si introduce varias etiquetas, sus intersecciones se utilizan para buscar el clúster.
4. Haga clic en **Search**.

   El sistema busca el clúster de destino por clave o valor de etiqueta.

Gestión de etiquetas

Puede ver, agregar, modificar y eliminar etiquetas en la pestaña **Tags** del clúster.

1. Inicie sesión en la consola de MRS.
2. En la página **Active Clusters**, haga clic en el nombre del clúster para el que desea gestionar las etiquetas.

   Se muestra la página de detalles del clúster.
3. Haga clic en la pestaña **Tags** y vea, agregue, modifique y elimine etiquetas en la página de pestaña.
   - Ver

     En la página de la pestaña **Tags**, puede ver detalles sobre las etiquetas del clúster, incluido el número de etiquetas y la clave y el valor de cada etiqueta.
   - Agregar

     Haga clic en **Add Tag** en la esquina superior izquierda. En el cuadro de diálogo **Add Tag** que se muestra, escriba la clave y el valor de la etiqueta que se va a agregar y haga clic en **OK**.
   - Modificar

     En la columna **Operation** de la etiqueta, haga clic en **Edit**. En la página **Edit Tag** mostrada, introduzca la nueva clave y el valor de la etiqueta y haga clic en **OK**.
   - Eliminar

     En la columna **Operation** de la etiqueta, haga clic en **Delete**. Después de la confirmación, haga clic en **OK** en la página mostrada para eliminar una etiqueta.

     NOTA

     Las actualizaciones de etiquetas del clúster de MRS se sincronizarán con todos los ECS del clúster. Se aconseja no modificar las etiquetas del ECS en la consola del ECS para evitar diferencias entre las etiquetas del ECS y las del clúster de MRS. Si la cantidad de etiquetas de un ECS del clúster de MRS alcanza el límite máximo, no se podrá crear ninguna etiqueta para el clúster de MRS.

2.6 Autorización de seguridad de comunicación

Los clústeres MRS aprovisionan, gestionan y usan componentes de big data a través de la consola de gestión. Los componentes de big data se despliegan en la VPC de un usuario. Si la consola de gestión de MRS necesita acceder directamente a los componentes de big data desplegados en la VPC del usuario, debe habilitar las reglas de grupo de seguridad correspondientes después de haber obtenido la autorización del usuario. Este proceso de autorización se llama comunicaciones seguras.

Si la función de comunicaciones seguras no está habilitada, no se pueden crear clústeres MRS. Si deshabilita la comunicación después de crear un clúster, el estado del clúster será **Network channel is not authorized** y las siguientes funciones se verán afectadas:

- Las funciones, como la instalación de componentes de big data, la expansión horizontal y reducción horizontal del clúster y la actualización de la especificación del nodo Master, no están disponibles.
- El estado de ejecución del clúster, las alarmas y los eventos no se pueden monitorear.
- Las funciones de gestión de nodos, gestión de componentes, gestión de alarmas, gestión de archivos, gestión de trabajos, gestión de parches, y gestión de tenant de la página de detalles del clúster no están disponibles.
- No se puede acceder a la página de Manager y al sitio web de cada componente.

Después de que la función de comunicaciones seguras se habilita de nuevo, el estado del clúster se restaura a **Running** y las funciones anteriores quedan disponibles. Para obtener más información, consulte **Habilitación de comunicaciones seguras para clústeres con esta función deshabilitada**.

Si las reglas de grupo de seguridad autorizadas en el clúster no son suficientes para aprovisionar, gestionar y usar componentes de big data, aparece a la derecha de **Secure Communications**. En este caso, haga clic en **Update** para actualizar las reglas del grupo de seguridad. Para obtener más información, consulte **Actualizar**.

Habilitación de comunicaciones seguras durante la creación de clústeres

Paso 1 Inicie sesión en la consola de MRS.

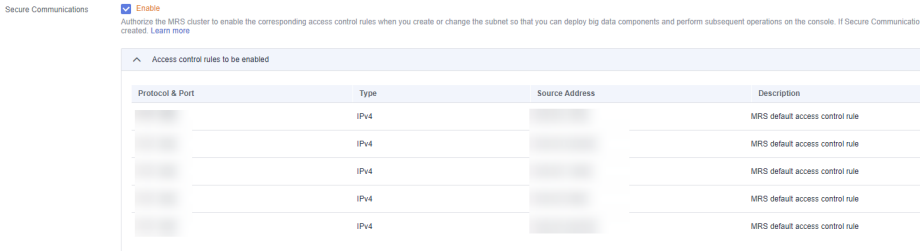
Paso 2 Haga clic en Comprar **Cluster**. Se muestra la página correspondiente.

Paso 3 Haga clic en **Quick Config** o **Custom Config**.

Paso 4 Configure la información del clúster haciendo referencia a **Comprar rápidamente un clúster MRS** o **Compra de un clúster personalizado**.

Paso 5 Seleccione **Enable** para **Secure Communications**.

Figura 2-16 Enable



Paso 6 Haga clic en **Buy Now**.

Si la autenticación de Kerberos está habilitada para un clúster, compruebe si es necesaria la autenticación de Kerberos. En caso afirmativo, haga clic en **Continue**. Si no, haga clic en **Back** para deshabilitar la autenticación de Kerberos y, a continuación, cree un clúster.

----Fin

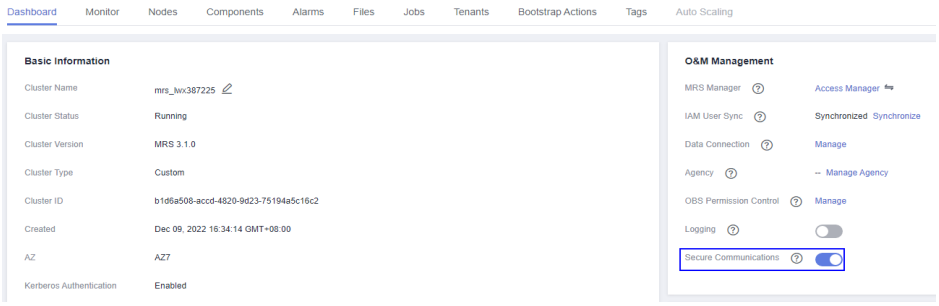
Desactivación de comunicaciones seguras después de crear un clúster

Paso 1 Inicie sesión en la consola de MRS.

Paso 2 En la lista de clústeres activos, haga clic en el nombre del clúster para el que desea deshabilitar las comunicaciones seguras.

Se muestra la página de detalles del clúster.

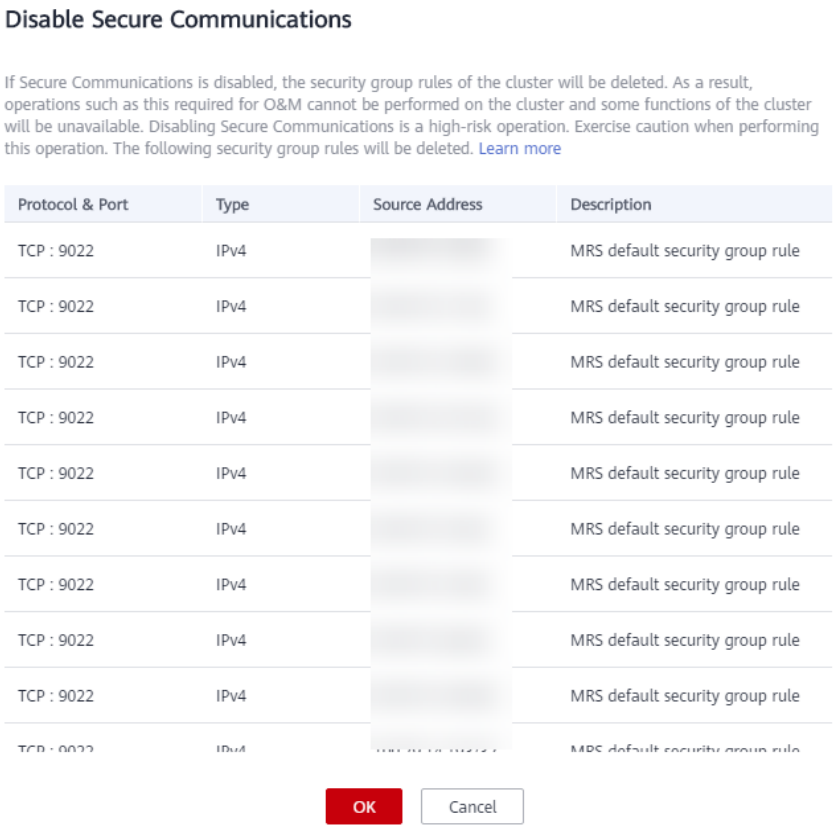
Figura 2-17 Comunicaciones seguras



Paso 3 Haga clic en el interruptor a la derecha de **Secure Communications** para desactivar la autorización. En el cuadro de diálogo que se muestra, haga clic en **OK**.

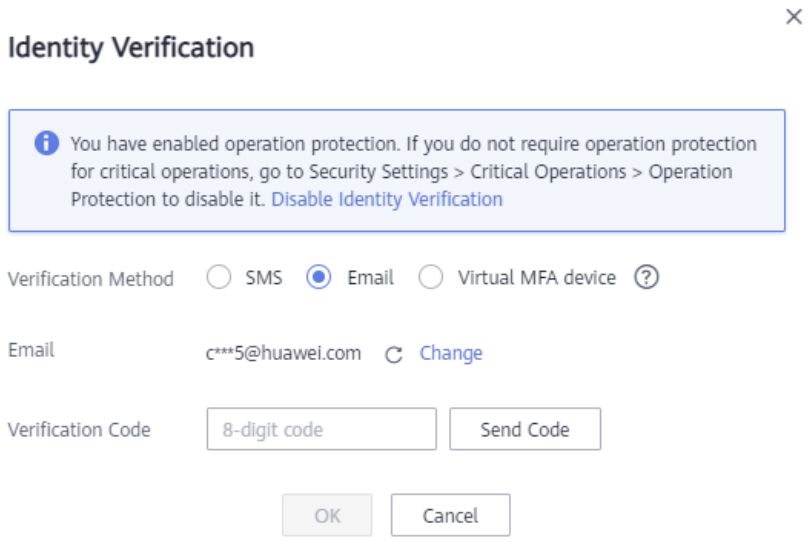
Una vez deshabilitada la autorización, el estado del clúster cambia a **Network channel unauthorized** y algunas funciones del clúster no están disponibles. Tenga cuidado al realizar esta operación.

Figura 2-18 Desactivación de comunicaciones seguras



Paso 4 Si ha habilitado la función de protección de operación crítica (para obtener más información, consulte **Protección de operación crítica** en IAM), introducir el código de verificación obtenido en el modo de verificación correspondiente para evitar riesgos y pérdidas causadas por mal funcionamiento.

Figura 2-19 Verificación de identidad



----Fin

Habilitación de comunicaciones seguras para clústeres con esta función deshabilitada

Paso 1 Inicie sesión en la consola de MRS.

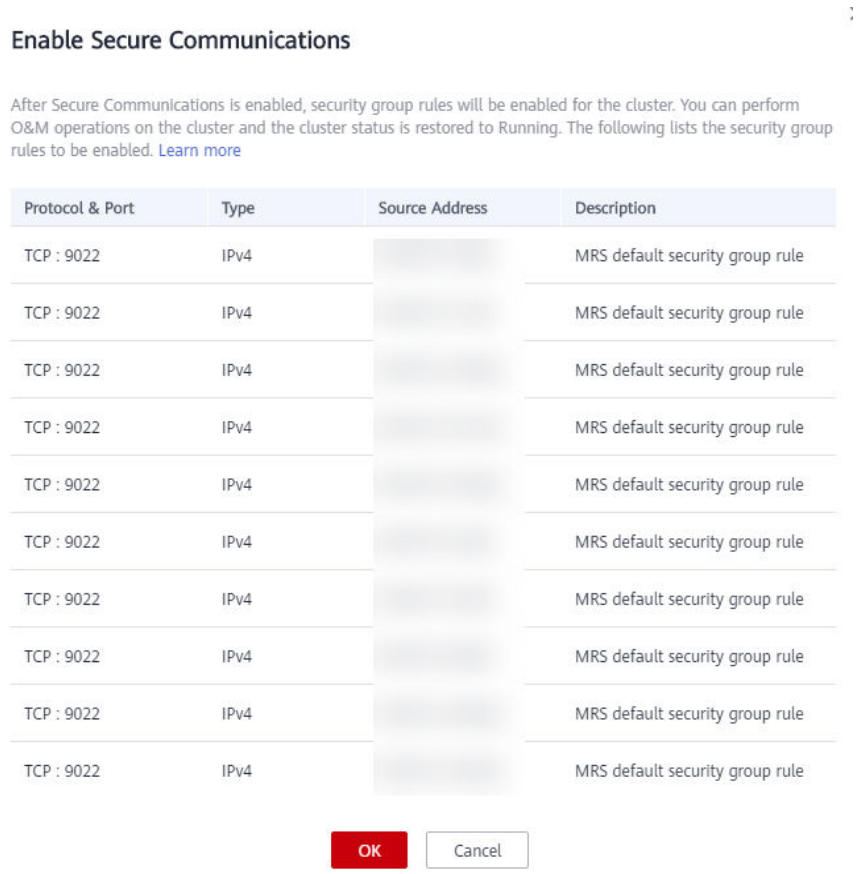
Paso 2 En la lista de clústeres activos, haga clic en el nombre del clúster para el que desea habilitar las comunicaciones seguras.

Se muestra la página de detalles del clúster.

Paso 3 Haga clic en el interruptor a la derecha de **Secure Communications** para activar la función.

Una vez activada la función, el estado del clúster cambia a **Running**.

Figura 2-20 Habilitación de comunicaciones seguras



----Fin

Actualizar

Si las reglas de grupo de seguridad autorizadas en el clúster no son suficientes para aprovisionar, gestionar y usar componentes de big data, se muestra a la derecha de **Secure Communications**. En este caso, haga clic en **Update** para actualizar las reglas del grupo de seguridad. Para obtener más información, consulte **Actualizar**.

Paso 1 Inicie sesión en la consola de MRS.

Paso 2 En la lista de clústeres activos, haga clic en el nombre del clúster para el que desea actualizar las comunicaciones seguras.

Se muestra la página de detalles del clúster.

Paso 3 Haga clic en **Update** a la derecha de **Secure Communications**.

Figura 2-21 Update

Paso 4 Haga clic en **OK**.

----Fin

2.7 Configuración de reglas de escalado automático

2.7.1 Descripción

En escenarios de aplicaciones de big data, especialmente análisis y procesamiento de datos en tiempo real, el número de nodos de clúster debe ajustarse dinámicamente de acuerdo con los cambios en el volumen de datos para proporcionar el número requerido de recursos. La función de escalado automático de MRS permite escalar automáticamente los nodos de tarea de un clúster para que coincidan con las cargas del clúster. Si el volumen de datos cambia periódicamente, puede configurar una regla de escalado automático para que el número de nodos de tarea se pueda ajustar automáticamente en un período de tiempo fijo antes de que cambie el volumen de datos.

- Reglas de escalado automático: puede aumentar o disminuir los nodos de tarea en función de las cargas de clúster en tiempo real. El escalado automático se activará con un cierto retraso cuando cambie el volumen de datos.
- Planes de recursos: Establezca la cantidad de nodo de tarea en función del intervalo de tiempo. Si el volumen de datos cambia periódicamente, puede crear planes de recursos para cambiar el tamaño del clúster antes de que cambie el volumen de datos, evitando así retrasos en el aumento o la disminución de recursos.

Puede configurar reglas de escalado automático o planes de recursos o ambos para activar el escalado automático. La configuración de planes de recursos y reglas de escalado automático mejora la escalabilidad del nodo del clúster para hacer frente a picos de volumen de datos ocasionalmente inesperados.

En algunos escenarios de servicio, los recursos deben reasignarse o la lógica de servicio debe modificarse después de escalar o reducir el clúster. Si se escala o reduce manualmente un clúster, puede iniciar sesión en los nodos del clúster para reasignar recursos o modificar la lógica del servicio. Si utiliza escalado automático, MRS le permite personalizar secuencias de comandos de automatización para la reasignación de recursos y la modificación de la lógica de servicio. Los scripts de automatización pueden ejecutarse antes y después del escalado automático y adaptarse automáticamente a los cambios de carga de servicio, todo lo cual elimina las operaciones manuales. Además, los scripts de automatización se pueden personalizar y ejecutar completamente en varios momentos, cumpliendo con sus requisitos personalizados y mejorando la flexibilidad de escalado automático.

- Reglas de escalado automático:
  - Puede establecer un máximo de cinco reglas para escalar hacia fuera o en un clúster, respectivamente.
  - El sistema determina el escalado horizontal y, a continuación, el escalado en función de la secuencia de configuración. Las políticas importantes tienen prioridad sobre otras políticas para evitar la activación repetida cuando el efecto esperado no se puede lograr después de una escalabilidad horizontal o vertical.
  - Los factores de comparación incluyen mayor que, mayor que o igual a, menor que, y menor que o igual a.
  - El escalado horizontal o el escalado horizontal del clúster solo se pueden activar después de que se alcance el umbral métrico configurado durante 5*n* consecutivos (el valor predeterminado de *n* es 1) minutos.
  - Después de cada escalado horizontal o vertical, hay una duración de enfriamiento que es mayor que 0 y dura 20 minutos de forma predeterminada.
  - En cada escalado horizontal o escalado vertical de clúster, se pueden añadir o reducir al menos un nodo y como máximo 100 nodos.
  - El número de nodos de tarea en un clúster se limita al número predeterminado de nodos configurados por los usuarios o al intervalo de cantidades de nodos en el plan de recursos que tiene efecto en el período de tiempo actual. El intervalo de cantidades de nodo en el plan de recursos que surte efecto en el período de tiempo actual tiene una prioridad más alta.
- Planes de recursos (definiendo el número de nodos Task por intervalo de tiempo):
  - Puede especificar un intervalo de nodos de Task (número mínimo a número máximo) en un intervalo de tiempo. Si el número de nodos de Task está más allá del rango de nodos de Task en un plan de recursos, el sistema activa la escalabilidad horizontal o vertical del clúster.
  - Puede establecer un máximo de cinco planes de recursos para un clúster.
  - Un ciclo de plan de recursos es por día. La hora de inicio y la hora de finalización se pueden establecer en cualquier punto de tiempo entre las 00:00 y las 23:59. La hora de inicio debe ser al menos 30 minutos antes que la hora de finalización. Los intervalos de tiempo configurados para diferentes planes de recursos no pueden superponerse.
  - Después de que un plan de recursos active la escalabilidad horizontal o vertical del clúster, hay una duración de enfriamiento de 10 minutos. El escalado automático no se activará de nuevo durante el tiempo de enfriamiento.
  - Cuando se habilita un plan de recursos, el número de nodos de Task del clúster se limita al intervalo de nodos predeterminado configurado por usted en otros períodos de tiempo, excepto el período de tiempo configurado en el plan de recursos.
- Scripts de automatización:
  - Puede establecer un script de automatización para que pueda ejecutarse automáticamente en los nodos del clúster cuando se active el escalado automático.
  - Puede establecer un número máximo de 10 scripts de automatización para un clúster.
  - Puede especificar un script de automatización que se ejecutará en uno o más tipos de nodos.
  - Los scripts de automatización se pueden ejecutar antes o después de escalar horizontalmente o verticalmente.

– Antes de usar scripts de automatización, cárguelos en un sistema de archivos VM o OBS de clúster en la misma región que el clúster. Los scripts de automatización cargados en la máquina virtual del clúster solo se pueden ejecutar en los nodos existentes. Si desea hacer que los scripts de automatización se ejecuten en los nuevos nodos, súbalos al sistema de archivos OBS.

2.7.2 Configuración del escalado automático durante la creación de clústeres

Al crear un clúster, puede configurar la función de escalado automático en parámetros de configuración avanzada.

NOTA

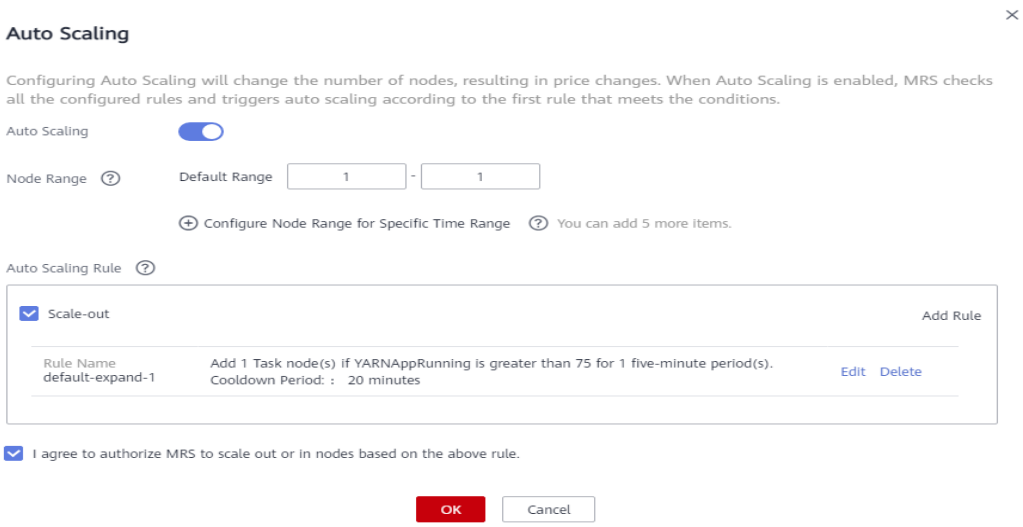
Las políticas de escalado automático solo se pueden configurar durante la creación de clústeres para análisis, streaming y clústeres híbridos.

Procedimiento

Paso 1 Inicie sesión en la consola de gestión de MRS.

Paso 2 Cuando un clúster que contiene nodos de tarea, configure la información de hardware y software del clúster haciendo referencia a **Compra de un clúster personalizado**. A continuación, en la página **Set Advanced Options**, habilite **Analysis Task** y configure o modifique reglas de escalado automático y planes de recursos.

Figura 2-22 Configuración de reglas de escalado automático al crear un clúster



NOTA

Puede configurar las reglas de escalado automático haciendo referencia a los siguientes escenarios:

- **Escenario 1: Uso exclusivo de reglas de escalamiento automático**
- **Escenario 2: Utilización exclusiva de planes de recursos**
- **Escenario 3: Uso de reglas de escalado automático y planes de recursos**

----Fin

2.7.3 Creación de una política de escalado automático para un clúster existente

Después de crear un clúster, puede configurar reglas para el grupo de nodos de tareas en un clúster por grupo de nodos o por grupo de recursos.

La política de grupo de nodos y la política de grupo de recursos se excluyen mutuamente. Puede configurar cualquiera de ellos según sea necesario.

MRS 3.1.5 o posterior admite la política de grupo de recursos especificada.

Concepto	Por grupo de nodos	Por grupo de recursos
Objeto de escalado automático	Todos los nodos del grupo de nodos de task	Nodos de task en el grupo de recursos especificado por una política de escalado automático
Propiedad del grupo de recursos de los nodos añadidos	Grupo de recursos predeterminado	Grupo de recursos especificado por la política de escalado automático
Objeto de escalado vertical	Reducción aleatoria de los nodos del grupo de nodos de task	Reducción aleatoria de nodos en un grupo de recursos especificado por una política de escalado automático

Prerrequisitos

- Los nodos de task se han configurado haciendo referencia a **Adición de un nodo de Task**.
- Se ha agregado un grupo de recursos haciendo referencia a **Creación de un grupo de recursos** si planea configurar políticas de escalado automático por grupo de recursos.

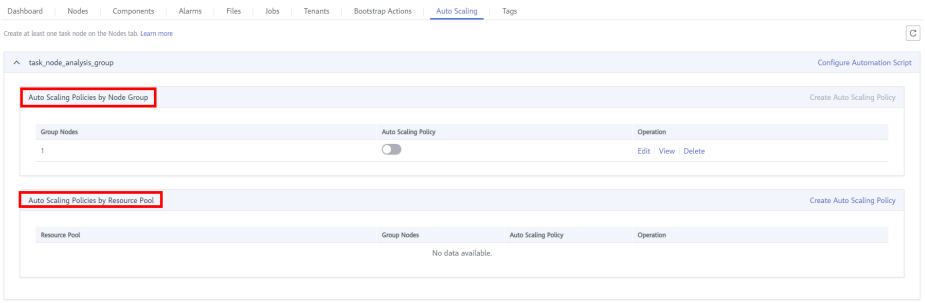
Procedimiento

Paso 1 Inicie sesión en la consola de gestión de MRS.

Paso 2 Elija **Clusters** > **Active Clusters**. En la lista de clústeres, seleccione un clúster en ejecución para acceder a su página de detalles.

Paso 3 En la página que se muestra, haga clic en la pestaña **Auto Scaling**.

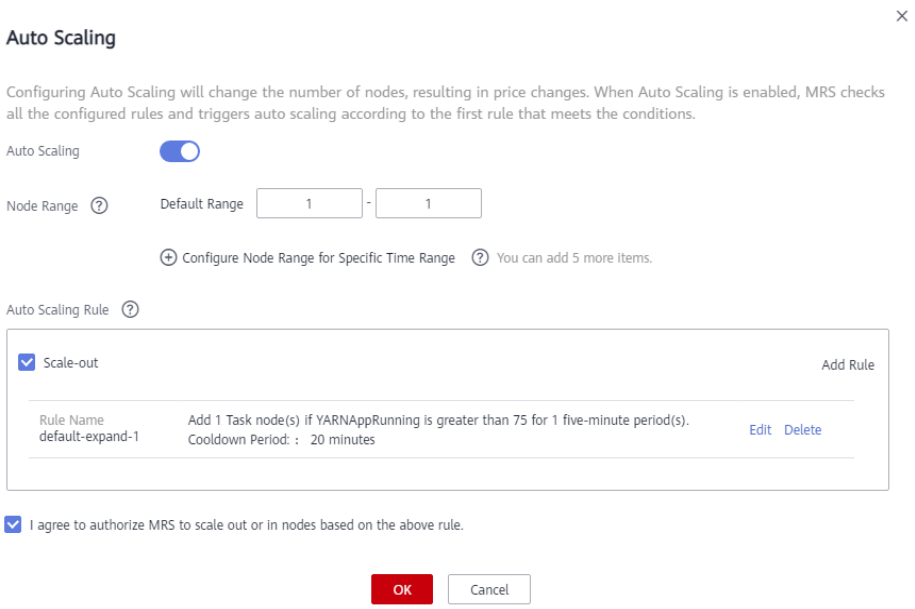
Puede configurar políticas por grupo de recursos o grupo de nodos según sea necesario.



NOTA

- Las políticas de escalado automático de diferentes grupos de nodos se excluyen mutuamente. Es decir, solo puede habilitar políticas de escalado automático para un grupo de nodos.
- Una regla de escalado automático ajusta el número de nodos, pero también afecta al precio real. Tenga cuidado al agregar una regla de escalado automático.

Paso 4 Haga clic en **Create Auto Scaling Policy** para crear una política de escalado automático.



NOTA

Puede configurar las reglas de escalado automático haciendo referencia a los siguientes escenarios:

- **Escenario 1: Uso exclusivo de reglas de escalamiento automático**
- **Escenario 2: Utilización exclusiva de planes de recursos**
- **Escenario 3: Uso de reglas de escalado automático y planes de recursos**

----Fin

2.7.4 Escenario 1: Uso exclusivo de reglas de escalamiento automático

Escenario donde solo se configuran las reglas de escalado automático: El número de nodos debe ajustarse dinámicamente en función del uso de recursos de YARN. Cuando la memoria YARN disponible es inferior al 20%, es necesario añadir cinco nodos. Cuando la memoria YARN disponible es superior al 70%, es necesario reducir cinco nodos. El número de nodos de un grupo de nodos de tarea oscila entre 1 y 10.

Procedimiento

Paso 1 Vaya a la página **Auto Scaling** para configurar reglas de escalado automático.

- Configure el parámetro **Default Range**.

Introduzca un rango de nodos de task en el que se realiza el escalado automático. Esta restricción se aplica a todas las reglas de escalado vertical y escalado horizontal. El rango de valores máximo permitido es de 0 a 500.

El intervalo de valores en este ejemplo es de 1 a 10.

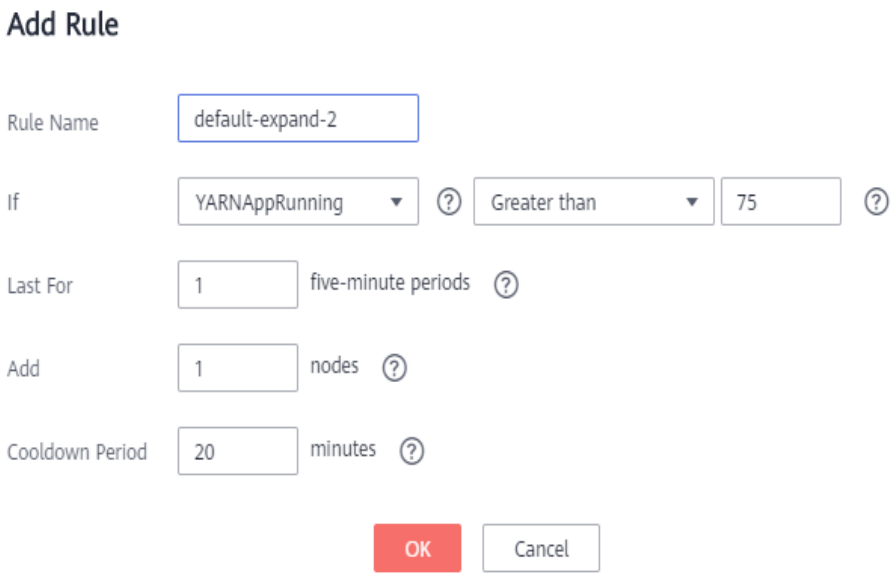
- Configure una regla de escalado automático.

  Para habilitar **Auto Scaling**, debe configurar una regla de escalamiento horizontal o de escalamiento vertical.

  a. Seleccione **Scale-Out** o **Scale-In**.

  b. Haga clic en **Add Rule**.

  Figura 2-23 Cuadro de diálogo de Add Rule

  c. Configure **Rule Name**, **If**, **Last For**, **Add** y **Cooldown Period**. Para obtener más información sobre las métricas de escalado automático, consulte **Configuración de métricas de escalado automático**.

  d. Haga clic en **OK**.

  Puede ver, editar o eliminar las reglas configuradas en el área **Scale-out** o **Scale-in** de la página **Auto Scaling**. Puede hacer clic en **Add Rule** para configurar varias reglas.

Paso 2 Haga clic en **OK**.

NOTA

Si desea configurar una regla de escalado automático para un clúster existente, seleccione **I agree to authorize MRS to scale out or in nodes based on the above rule**.

----Fin

2.7.5 Escenario 2: Utilización exclusiva de planes de recursos

Si el volumen de datos cambia regularmente todos los días y desea escalar o escalar en un clúster antes de que cambie el volumen de datos, puede crear planes de recursos para ajustar el número de nodos de tarea según lo planeado en el intervalo de tiempo especificado.

Antecedentes

Un servicio de procesamiento en tiempo real ve un fuerte aumento en el volumen de datos de 7:00 a 13:00 los lunes, martes y sábados. Supongamos que se utiliza un clúster de flujo continuo MRS para procesar los datos de servicio. Se requieren cinco nodos de tarea de 7:00 a 13:00 los lunes, martes y sábados, mientras que solo se requieren dos en otro momento.

Procedimiento

Paso 1 Vaya a la página **Auto Scaling** para configurar un plan de recursos.

NOTA

Se puede configurar un plan de recursos para ajustar el número de nodos, lo que afecta al precio real. Tenga cuidado al realizar esta operación.

Paso 2 Por ejemplo, el **Default Range** de la cantidad de nodos se establece en **2-2** indicando que el número de nodos de tarea se fija en 2 excepto el intervalo de tiempo especificado en el plan de recursos.

Paso 3 Haga clic en **Configure Node Range for Specific Time Range** en **Default Range** o **Add Resource Plan**.

Paso 4 Configure **Effective On**, **Time Range** y **Node Range**.

Por ejemplo, establezca **Effective On** en **Monday**, **Tuesday** y **Saturday**, **Time Range** en **07:00-13:00** y **Node Range** en **5-5**. Esto indica que el número de nodos de tarea se fija en 5 de 07:00 a 13:00.

Puede hacer clic en **Configure Node Range for Specific Time Range** para configurar varios planes de recursos.

NOTA

- **Effective On** está establecido en **Daily** de forma predeterminada. También puede seleccionar uno o varios días de lunes a domingo.
- Si no establece **Node Range**, se usará su valor predeterminado.
- Si establece **Node Range** y **Time Range**, el rango de nodos que establezca se usará durante el rango de tiempo que establezca, y el rango de nodos predeterminado se usará más allá del rango de tiempo que establezca. Si el tiempo no está dentro del intervalo de tiempo configurado, se utiliza el intervalo predeterminado.

----Fin

2.7.6 Escenario 3: Uso de reglas de escalado automático y planes de recursos

Si el volumen de datos no es estable y puede producirse la fluctuación esperada, el intervalo de nodos de Task fijo no puede garantizar que se cumplan los requisitos en algunos escenarios de servicio. En este caso, es necesario ajustar el número de nodos de Task basándose en las cargas en tiempo real y los planes de recursos.

Antecedentes

Un servicio de procesamiento en tiempo real observa un aumento inestable en el volumen de datos de 7:00 a 13:00 los lunes, martes y sábados. Por ejemplo, se requieren de 5 a 8 nodos de

tarea de 7:00 a 13:00 los lunes, martes y sábado, y de 2 a 4 más allá de este período. Por lo tanto, puede establecer una regla de escalado automático basada en un plan de recursos. Cuando el volumen de datos excede el valor esperado, se puede ajustar el número de nodos Task si cambian las cargas de recursos, sin exceder el rango de nodos especificado en el plan de recursos. Cuando se activa un plan de recursos, el número de nodos se ajusta dentro del rango de nodos especificado con un efecto mínimo. Es decir, aumentar los nodos hasta el límite superior y disminuir los nodos hasta el límite inferior.

Procedimiento

Paso 1 Vaya a la página **Auto Scaling** para configurar reglas de escalado automático.

Una regla de escalado automático ajusta el número de nodos, pero también afecta al precio real. Tenga cuidado al agregar una regla de escalado automático.

- **Default Range**

  Introduzca un rango de nodos de task en el que se realiza el escalado automático. Esta restricción se aplica a todas las reglas de escalado vertical y escalado horizontal.

  Por ejemplo, este parámetro se establece en **2-4** en este escenario.

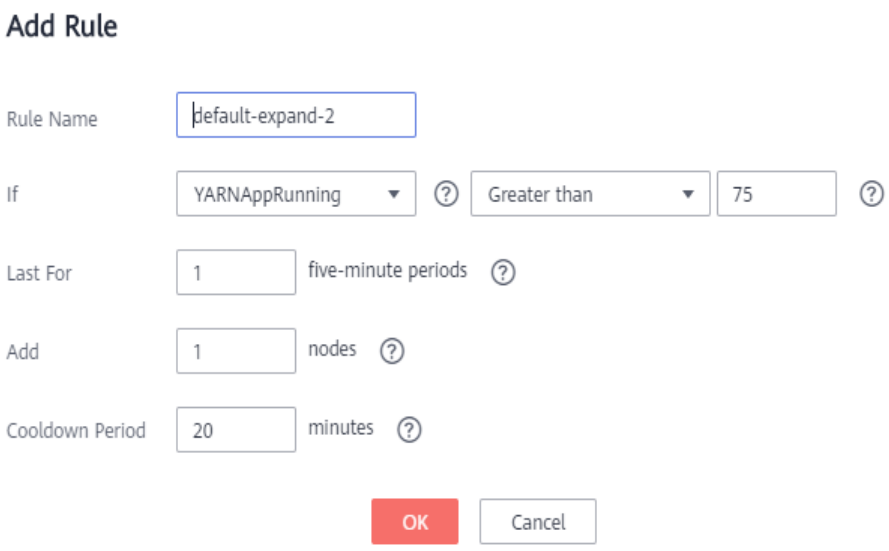
- **Auto Scaling**

  Para habilitar **Auto Scaling**, debe configurar una regla de escalamiento horizontal o de escalamiento vertical.

  a. Seleccione **Scale-Out** o **Scale-In**.

  b. Haga clic en **Add Rule**. Se muestra la página **Add Rule**.

  Figura 2-24 Adición de una regla

  c. Configure los parámetros **Rule Name**, **If**, **Last for**, **Add** y **Cooldown Period**.

  d. Haga clic en **OK**.

  Puede ver, editar o eliminar las reglas configuradas en el área **Scale-out** o **Scale-in** de la página **Auto Scaling**.

Paso 2 Configurar un plan de recursos.

1. Haga clic en **Configure Node Range for Specific Time Range** en **Default Range** o **Add Resource Plan**.
2. Configure **Effective On**, **Time Range** y **Node Range**.

   Por ejemplo, establezca **Effective On** en **Monday**, **Tuesday** y **Saturday**, **Time Range** en **07:00-13:00** y **Node Range** en **5-8**.

   Puede hacer clic en **Configure Node Range for Specific Time Range** o **Add Resource Plan** para configurar varios planes de recursos.

   NOTA

   - **Effective On** está establecido en **Daily** de forma predeterminada. También puede seleccionar uno o varios días de lunes a domingo.
   - Si no establece **Node Range**, se usará su valor predeterminado.
   - Si establece **Node Range** y **Time Range**, el rango de nodos que establezca se usará durante el rango de tiempo que establezca, y el rango de nodos predeterminado se usará más allá del rango de tiempo que establezca. Si el tiempo no está dentro del intervalo de tiempo configurado, se utiliza el intervalo predeterminado.

----Fin

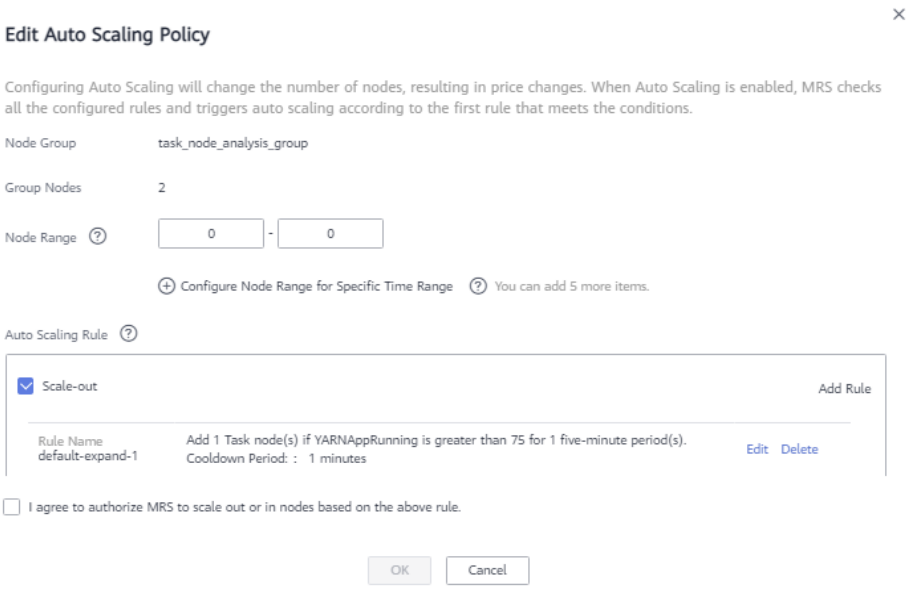
2.7.7 Modificación de una política de escalado automático

Paso 1 Inicie sesión en la consola de gestión de MRS.

Paso 2 Elija **Clusters** > **Active Clusters**. En la lista de clústeres, seleccione un clúster en ejecución para acceder a su página de detalles.

Paso 3 Haga clic en la pestaña **Auto Scaling**.

Paso 4 Haga clic en **Edit** a la derecha de la política de escalado automático de destino.



----Fin

2.7.8 Eliminación de una política de escalado automático

Paso 1 Inicie sesión en la consola de gestión de MRS.

Paso 2 Elija **Clusters** > **Active Clusters**. En la lista de clústeres, seleccione un clúster en ejecución para acceder a su página de detalles.

Paso 3 Haga clic en la pestaña **Auto Scaling**.

Paso 4 Haga clic en **Delete** a la derecha de la política de escalado automático de destino.

----Fin

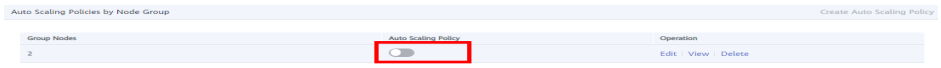
2.7.9 Activar o desactivar una política de escalado automático

Paso 1 Inicie sesión en la consola de gestión de MRS.

Paso 2 Elija **Clusters** > **Active Clusters**. En la lista de clústeres, seleccione un clúster en ejecución para acceder a su página de detalles.

Paso 3 Haga clic en la pestaña **Auto Scaling**.

Paso 4 Active o desactive **Auto Scaling Policy** para activar o desactivar una política de escalado automático.



----Fin

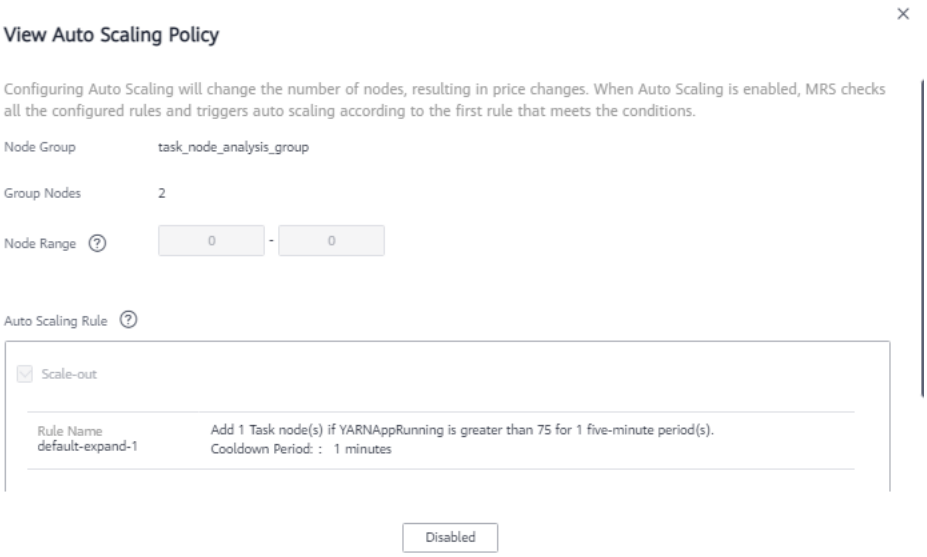
2.7.10 Consulta de una política de escalado automático

Paso 1 Inicie sesión en la consola de gestión de MRS.

Paso 2 Elija **Clusters** > **Active Clusters**. En la lista de clústeres, seleccione un clúster en ejecución para acceder a su página de detalles.

Paso 3 Haga clic en la pestaña **Auto Scaling**.

Paso 4 Haga clic en **View** a la derecha de la política de escalado automático de destino para verlo.



----Fin

2.7.11 Configuración scripts de automatización

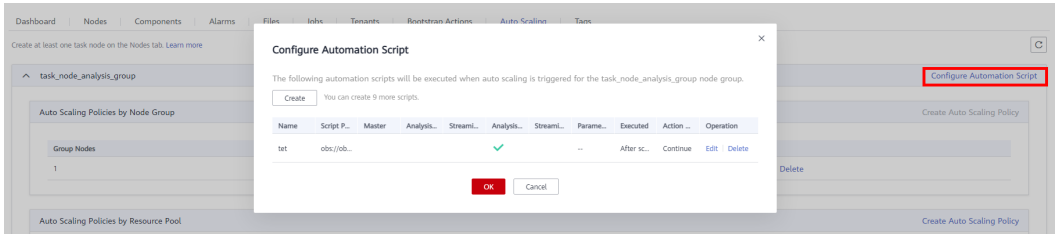
Paso 1 Inicie sesión en la consola de gestión de MRS.

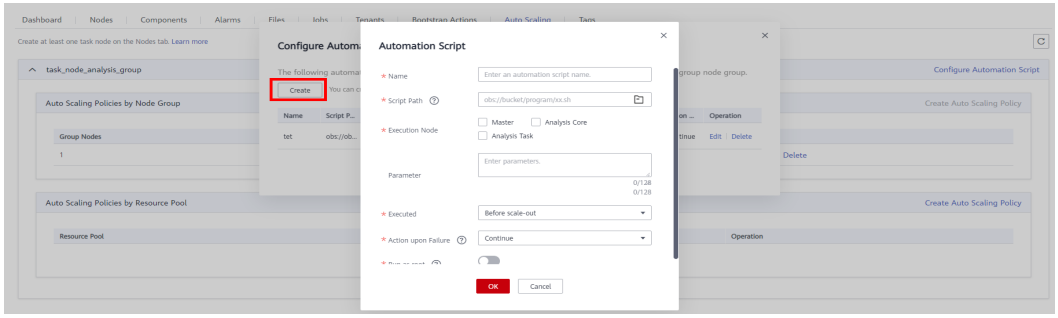
Paso 2 Elija **Clusters** > **Active Clusters**. En la lista de clústeres, seleccione un clúster en ejecución para acceder a su página de detalles.

Paso 3 Haga clic en la pestaña **Auto Scaling**.

Paso 4 Haga clic en **Configure Automation Script**.

Paso 5 Haga clic en **Add**.





Paso 6 Configure **Name**, **Script Path**, **Execution Node**, **Parameter**, **Executed** y **Action upon Failure**. Para obtener más información sobre los parámetros, consulte **Tabla 2-14**.

Paso 7 Haga clic en **OK** para guardar las configuraciones del script de automatización.

----Fin

2.7.12 Configuración de métricas de escalado automático

Políticas de escalado automático por grupo de nodos

Cuando agrega una regla, puede consultar **Tabla 2-11** para configurar las métricas correspondientes.

Tabla 2-11 Métricas de escalado automático

Tipo de clúster	Métrica	Tipo de valor	Descripción
Clúster de streaming	StormSlotAvailable	Integer	Número de slot disponible de Storm Rango de valores: 0 a 2147483646
	StormSlotAvailable-Percentage	Percentage	Porcentaje de slot disponible de Storm, es decir, la proporción de slot disponible respecto al total de slots Rango de valores: 0 a 100
	StormSlotUsed	Integer	Número de slots de Storm utilizados Rango de valores: 0 a 2147483646
	StormSlotUsedPer-centage	Percentage	Porcentaje de slots usados de Storm, es decir, la proporción de slots usados con respecto al total de slots Rango de valores: 0 a 100
	StormSupervisor-MemAverageUsage	Integer	Uso promedio de memoria del proceso Supervisor de Storm Rango de valores: 0 a 2147483646
	StormSupervisor-MemAverageUsage Percentage	Percentage	Porcentaje medio de la memoria utilizada del proceso Supervisor de Storm con respecto a la memoria total del sistema Rango de valores: 0 a 100
	StormSupervisorC-PUAverageUsagePe rcentage	Percentage	Porcentaje promedio de las CPUs usadas del proceso Supervisor de Storm con respecto al total de CPUs Rango de valores: 0 a 6000
Clúster de análisis	YARNAppPending	Integer	Número de tareas pendientes en YARN Rango de valores: 0 a 2147483646

Tipo de clúster	Métrica	Tipo de valor	Descripción
	YARNAppPendingRatio	Ratio	Relación entre tareas pendientes en YARN, es decir, la relación entre tareas pendientes y tareas en ejecución en YARN Rango de valores: 0 a 2147483646
	YARNAppRunning	Integer	Número de tareas en ejecución en YARN Rango de valores: 0 a 2147483646
	YARNContainerAllocated	Integer	Número de contenedores asignados a YARN Rango de valores: 0 a 2147483646
	YARNContainerPending	Integer	Número de contenedores pendientes en YARN Rango de valores: 0 a 2147483646
	YARNContainerPendingRatio	Ratio	Relación entre contenedores pendientes en Yarn, es decir, la relación entre contenedores pendientes y contenedores en funcionamiento en YARN Rango de valores: 0 a 2147483646
	YARNCPUAllocated	Integer	Número de CPU virtuales (vCPUs) asignadas a YARN Rango de valores: 0 a 2147483646
	YARNCPUAvailable	Integer	Número de vCPUs disponibles en YARN Rango de valores: 0 a 2147483646
	YARNCPUAvailablePercentage	Percentage	Porcentaje de vCPUs disponibles en YARN, es decir, la proporción de vCPUs disponibles respecto al total de vCPUs Rango de valores: 0 a 100
	YARNCPUPending	Integer	Número de vCPU pendientes en YARN Rango de valores: 0 a 2147483646
	YARNMemoryAllocated	Integer	Memoria asignada a YARN, en MB Rango de valores: 0 a 2147483646
	YARNMemoryAvailable	Integer	Memoria disponible en YARN en MB Rango de valores: 0 a 2147483646

Tipo de clúster	Métrica	Tipo de valor	Descripción
	YARNMemoryAvailablePercentage	Percentage	Porcentaje de memoria disponible en YARN es decir, la proporción de memoria disponible a memoria total en YARN Rango de valores: 0 a 100
	YARNMemoryPending	Integer	Memoria pendiente en YARN Rango de valores: 0 a 2147483646

NOTA

- Cuando el tipo de valor es porcentaje o relación en **Tabla 2-11**, el valor válido puede ser exacto a percentil. El valor de la métrica porcentual es un valor decimal con un signo de porcentaje (%) eliminado. Por ejemplo, 16.80 representa 16.80%.
- Los clústeres híbridos admiten todas las métricas de los clústeres de análisis y streaming.

Políticas de escalado automático por grupo de recursos

Al agregar una regla, puede consultar **Tabla 2-12** para configurar las métricas correspondientes.

NOTA

Las políticas de escalado automático se pueden configurar para un clúster por grupo de recursos en MRS 3.1.5 o posterior.

Tabla 2-12 Descripción de configuración de regla

Tipo de clúster	Métrica	Tipo de valor	Descripción
Clúster de análisis/ personalizado	ResourcePoolMemoryAvailable	Integer	Memoria disponible en YARN en el grupo de recursos, en MB Rango de valores: 0 a 2147483646

Tipo de clúster	Métrica	Tipo de valor	Descripción
	ResourcePoolMemoryAvailablePercentage	Percentage	Porcentaje de memoria disponible en YARN en el grupo de recursos, es decir, la proporción de memoria disponible a memoria total en YARN Rango de valores: 0 a 100
	ResourcePoolCPUAvailable	Integer	Número de vCPUs disponibles en YARN en el grupo de recursos Rango de valores: 0 a 2147483646
	ResourcePoolCPUAvailablePercentage	Percentage	Porcentaje de vCPUs disponibles en YARN en el grupo de recursos. es decir, la proporción de vCPUs disponibles con respecto al total de vCPUs Rango de valores: 0 a 100

Al agregar un plan de recursos, puede configurar los parámetros haciendo referencia a **Tabla 2-13**.

Tabla 2-13 Conceptos de configuración del plan de recursos

Parámetro	Descripción
Effective On	La fecha de entrada en vigor de un plan de recursos. **Daily** está seleccionado de forma predeterminada. También puede seleccionar uno o varios días de lunes a domingo.
Time Range	La hora de inicio y la hora de finalización de un plan de recursos son exactas a los minutos, con un valor que oscila entre **00:00** y **23:59**. Por ejemplo, si un plan de recursos comienza a las 8:00 y termina a las 10:00, establezca este parámetro en **8:00-10:00**. La hora de finalización debe ser al menos 30 minutos más tarde que la hora de inicio.

Parámetro	Descripción
Node Range	El número de nodos de un plan de recursos varía entre **0** y **500**. En el intervalo de tiempo especificado en el plan de recursos, si el número de nodos de tarea es menor que el número mínimo especificado de nodos, se incrementará al valor mínimo especificado del intervalo de nodos a la vez. Si el número de nodos de tarea es mayor que el número máximo de nodos especificado en el plan de recursos, la función de escalado automático reduce el número de nodos de tarea al valor máximo del intervalo de nodos a la vez. La cantidad mínima de nodos debe ser inferior o igual a la cantidad máxima de estos.

NOTA

- Cuando se habilita un plan de recursos, el valor **Default Range** de la página de escalado automático tiene efecto por la fuerza más allá del intervalo de tiempo especificado en el plan de recursos. Por ejemplo, si **Default Range** se establece en **1-2**, **Time Range** está entre **08:00-10:00** y **Node Range** es **4-5** en un plan de recursos, el número de nodos Task en otros períodos (0:00-8:00 y 10:00-23:59) de un día está limitado forzosamente al rango de nodos predeterminado (1 a 2). Si el número de nodos es mayor que 2, se activa el escalado automático; si el número de nodos es menor que 1, se activa el escalado automático.
- Cuando un plan de recursos no está habilitado, el **Default Range** tiene efecto en todos los intervalos de tiempo. Si el número de nodos no está dentro del rango de nodos predeterminado, el número de nodos de Task se incrementa o disminuye automáticamente al rango de nodos predeterminado.
- Los rangos de tiempo de los planes de recursos no pueden superponerse. El intervalo de tiempo superpuesto indica que existen dos planes de recursos efectivos en un punto de tiempo. Por ejemplo, si el plan de recursos 1 tiene efecto de **08:00** a **10:00** y el plan de recursos 2 tiene efecto de **09:00** a **11:00**, se superpone el intervalo de tiempo entre **09:00** y **10:00**.
- El intervalo de tiempo de un plan de recursos debe ser el mismo día. Por ejemplo, si desea configurar un plan de recursos de **23:00** a **01:00** al día siguiente, configure dos planes de recursos cuyos intervalos de tiempo son **23:00-00:00** y **00:00-01:00** respectivamente.

Script de automatización

Al agregar una secuencia de comandos de automatización, puede configurar parámetros relacionados haciendo referencia a **Tabla 2-14**.

Tabla 2-14 Descripción de configuración del script de automatización

Parámetro	Descripción
Name	Nombre de un script de automatización El valor solo puede contener números, letras, espacios, guiones (-) y guiones bajos (_) y no debe comenzar con un espacio. El valor puede contener de 1 a 64 caracteres. **NOTA** Un nombre debe ser único en el mismo clúster. Puede configurar el mismo nombre para diferentes clústeres.

Parámetro	Descripción
Script Path	Ruta del script. El valor puede ser una ruta de sistema de archivos OBS o una ruta de VM local. ● Una ruta de sistema de archivos de OBS debe comenzar por **s3a://** y terminar por **.sh**, por ejemplo, **s3a://mrs-samples/***xxx***.sh**. ● Una ruta de VM local debe comenzar con una barra diagonal (/) y terminar con **.sh**. Por ejemplo, la ruta del script de ejemplo para instalar el Zepelin es **/opt/bootstrap/zepelin/zepelin_install.sh**.
Execution Node	Seleccione un tipo del nodo donde se ejecuta un script de automatización. **NOTA** ● Si selecciona nodos **Master**, puede elegir si desea ejecutar el script sólo en los nodos de Master activos mediante activación o desactivación el interruptor **Active Master**. ● Si lo habilita, el script solo se ejecuta en los nodos Master activos. Si lo deshabilita, el script se ejecuta en todos los nodos Master. Esta función está deshabilitada por defecto.
Parameter	Parámetro de script de automatización. Se pueden importar las siguientes variables predefinidas para obtener información de escalado automático: ● **${mrs_scale_node_num}**: Número de nodos de escalado automático. El valor es siempre positivo. ● **${mrs_scale_type}**: Tipo de escalar horizontalmente/verticalmente. El valor puede ser **scale_out** o **scale_in**. ● **${mrs_scale_node_hostnames}**: Nombres de host de los nodos de escalado automático. Utilice comas (,) para separar varios nombres de host. ● **${mrs_scale_node_ips}**: dirección IP de los nodos de escalado automático. Utilice comas (,) para separar varias direcciones IP. ● **${mrs_scale_rule_name}**: Nombre de la regla de escalado automático activada. Para un plan de recursos, este parámetro se establece en **resource_plan**.
Executed	Tiempo para ejecutar un script de automatización. Se admiten las siguientes cuatro opciones: **Before scale-out**, **After scale-out**, **Before scale-in** y **After scale-in**. **NOTA** Supongamos que los nodos de ejecución incluyen nodos Task. ● El script de automatización ejecutada antes de escalar horizontalmente no puede ejecutarse en los nodos Task que se van a agregar. ● El script de automatización ejecutado después de escalar hacia fuera puede ejecutarse en los nodos Task agregados. ● El script de automatización ejecutado antes de escalar puede ejecutarse en los nodos Task que se van a eliminar. ● El script de automatización ejecutada después de escalar no puede ejecutarse en los nodos Task eliminados.

Parámetro	Descripción
Action upon Failure	Si se deben continuar ejecutando scripts posteriores y escalar horizontalmente/verticalmente después de que el script no se ejecute. **NOTA** ● Se recomienda establecer este parámetro en **Continue** en la fase de puesta en marcha para que el clúster pueda continuar con la operación de escalado horizontal o vertical sin importar si se ejecuta el script. ● Si el script no se ejecuta, vea el registro **/var/log/Bootstrap** en la máquina virtual del clúster. ● La operación de escalado de entrada no se puede revertir. Por lo tanto, el **Action upon Failure** solo se puede establecer en **Continue** después de escalar verticalmente.

NOTA

El script de automatización solo se activa durante el escalado automático. No se activa cuando el nodo del clúster se escalar horizontal o verticalmente de forma manual.

2.8 Gestión de conexiones de datos

2.8.1 Configuración de conexiones de datos

Las conexiones de datos de MRS se utilizan para gestionar las conexiones de origen externas utilizadas por los componentes de un clúster. Por ejemplo, si los metadatos de Hive utilizan una base de datos relacional externa, se puede utilizar una conexión de datos para asociar la base de datos relacional externa con el componente Hive.

- **Local**: Los metadatos se almacenan en la GaussDB local de un clúster. Cuando se elimina el clúster, también se eliminan los metadatos. Para conservar los metadatos, realice una copia de respaldo manual de los metadatos en la base de datos con antelación.
- **Conexión de datos externa**: Puede seleccionar **RDS PostgreSQL database** o **RDS MySQL database** asociado a la misma VPC y subred que el clúster actual. Los metadatos se almacenan en la base de datos y no se eliminan cuando se elimina el clúster actual. Varios clústeres de MRS pueden compartir los mismos metadatos.

NOTA

Cuando los metadatos de Hive se cambian entre diferentes clústeres, MRS sincroniza solo los permisos en la base de datos de metadatos del componente Hive. El modelo de permiso en MRS se mantiene en MRS Manager. Por lo tanto, cuando los metadatos de Hive se cambian entre clústeres, los permisos de los usuarios o grupos de usuarios no se pueden sincronizar automáticamente con MRS Manager de otro clúster.

Creación de una conexión de datos

Paso 1 Inicie sesión en la consola de gestión de MRS y elija **Data Connections** en el panel de navegación izquierdo.

Paso 2 Haga clic en **Create Data Connection**.

Para obtener más información acerca de cómo configurar una conexión de datos RDS, consulte **Creación de una conexión de datos de RDS**.

Paso 3 Haga clic en **OK**.

----Fin

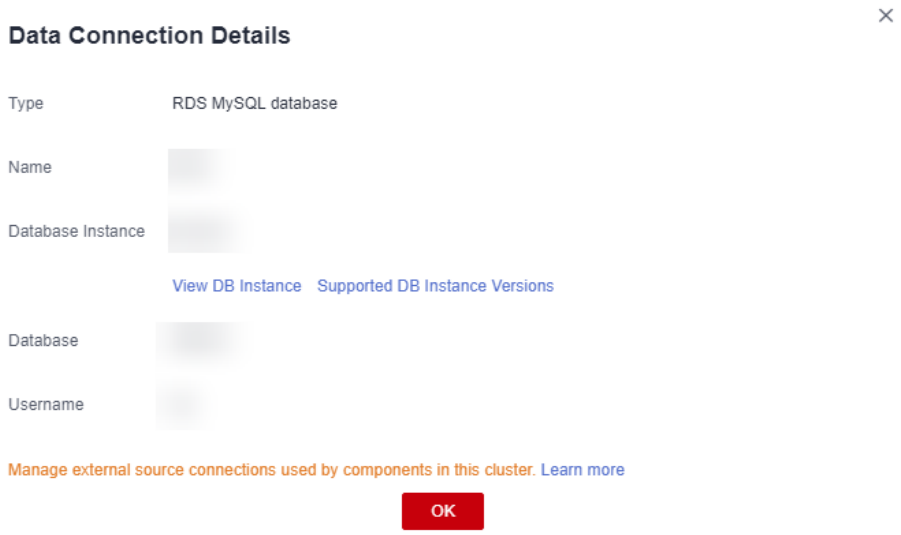
Consulta de detalles de conexión de datos

Paso 1 Inicie sesión en la consola de gestión de MRS y elija **Data Connections** en el panel de navegación izquierdo.

Paso 2 En la lista de conexiones de datos, haga clic en la conexión de datos deseada. En la página que se muestra, vea sus detalles.

Por ejemplo, la información de conexión de datos de la base de datos de RDS for MySQL es la siguiente:

Figura 2-25 Consulta de la información de conexión de datos de la base de datos de RDS for MySQL



----Fin

Eliminación de una conexión de datos

Paso 1 Inicie sesión en la consola de gestión de MRS y elija **Data Connections** en el panel de navegación izquierdo.

Paso 2 En la columna **Operation** de la lista de conexiones de datos, haga clic en **Delete** en la fila donde se encuentra la conexión de datos que se va a eliminar.

Si la conexión de datos seleccionada se ha asociado a un clúster, la eliminación no afecta al clúster.

----Fin

Configuración de una conexión de datos durante la creación del clúster

Paso 1 Inicie sesión en la consola de MRS.

Paso 2 Haga clic en **Buy Cluster**. Se muestra la página para comprar un clúster.

Paso 3 Haga clic en la pestaña **Custom Config**.

Paso 4 Realice configuraciones relacionadas basadas en los siguientes escenarios de conexión de datos externos. Para obtener más información sobre cómo configurar otros parámetros, consulte **Compra de un clúster personalizado**.

Para obtener más información acerca de cómo configurar una conexión de datos RDS, consulte **Configuración de una conexión de datos de RDS durante la creación de clústeres**.

----Fin

2.8.2 Configuración de una conexión de datos de RDS

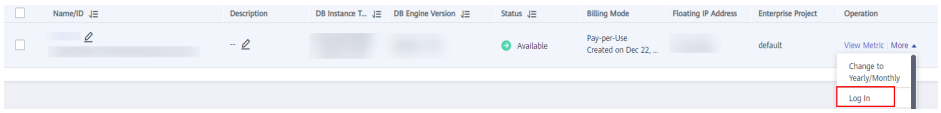
2.8.2.1 Configuración de una conexión de datos de RDS

Preparaciones

Paso 1 Inicie sesión en la consola de gestión de RDS.

Paso 2 Compre una instancia de base de datos de RDS. Para obtener más información, consulte **Comprar una instancia de base de datos**.

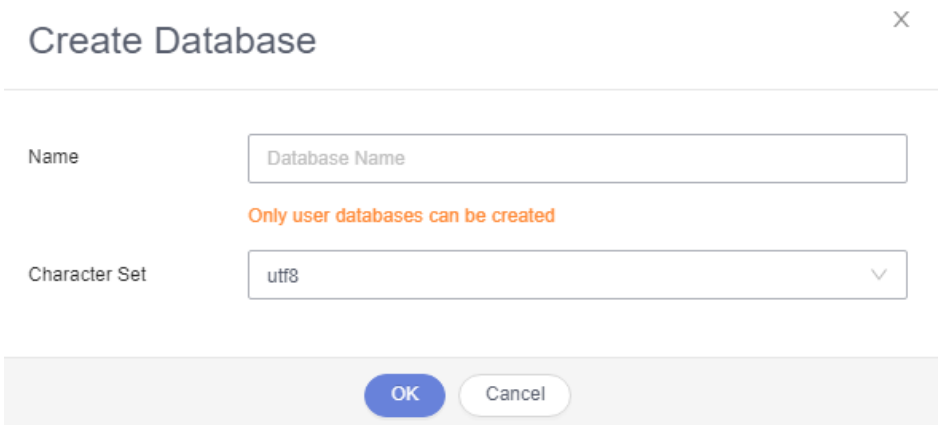
Paso 3 En el panel de navegación izquierdo de la consola de gestión de RDS, seleccione **Instances**. Busque la fila que contiene la instancia de base de datos de RDS utilizada por las conexiones de datos de MRS, haga clic en **More** en la columna **Operation** y seleccione **Log In** para iniciar sesión en la instancia de base de datos como usuario **root**.



Paso 4 En la página principal de la instancia, haga clic en **Create Database** para crear una base de datos.

NOTA

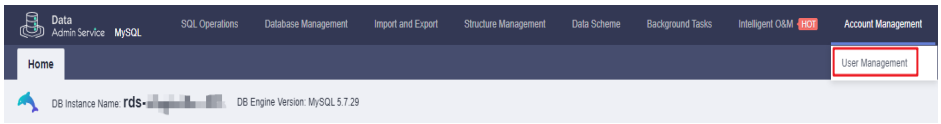
Si no se crea ninguna base de datos nueva, las conexiones de datos MRS no se configurarán.



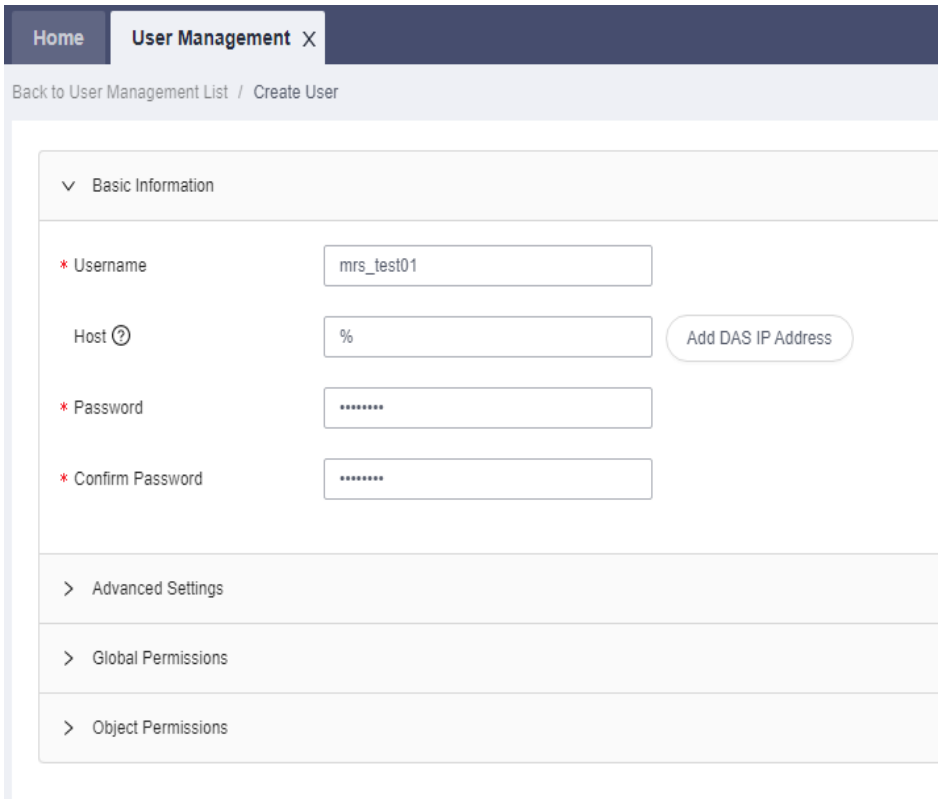
Paso 5 En la parte superior de la página, seleccione **Account Management** > **User Management**.

NOTA

Si la conexión de datos seleccionada es **RDS MySQL database**, asegúrese de que el usuario de la base de datos es el usuario **root**. Si el usuario no es **root**, realice **Paso 5** a **Paso 7**.



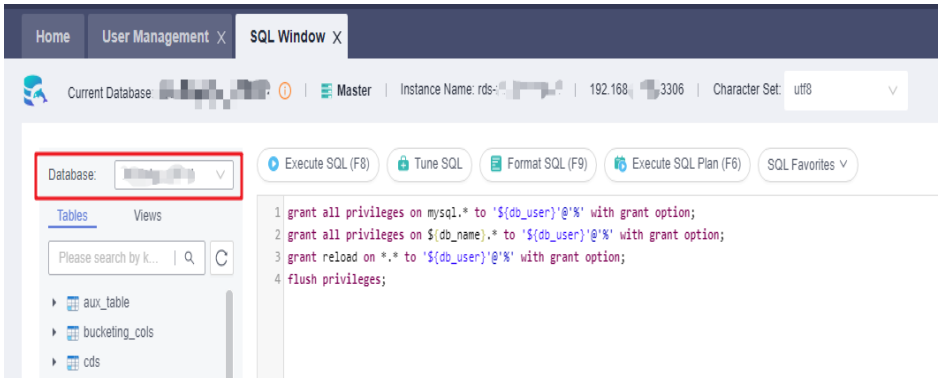
Paso 6 Haga clic en **Create User** para crear un usuario que no sea root.



Paso 7 En la parte superior de la página, elija **SQL Operations** > **SQL Query** y cambie a la base de datos de destino por nombre de base de datos y ejecute las siguientes sentencias SQL para conceder permisos al usuario de la base de datos. En las siguientes sentencias, *${db_name}* y

${db_user} indican el nombre de la base de datos que se va a conectar a MRS y el nombre del nuevo usuario, respectivamente.

```
grant SELECT, INSERT on mysql.* to '${db_user}'@'%' with grant option;
grant all privileges on ${db_name}.* to '${db_user}'@'%' with grant option;
grant reload on *.* to '${db_user}'@'%' with grant option;
flush privileges;
```



Paso 8 Cree una conexión de datos haciendo referencia a **Creación de una conexión de datos de RDS**.

----Fin

Creación de una conexión de datos de RDS

Cree una conexión de datos RDS para un clúster MRS existente.

Paso 1 Inicie sesión en la consola de gestión de MRS y elija **Data Connections** en el panel de navegación izquierdo.

Paso 2 Haga clic en **Create Data Connection**.

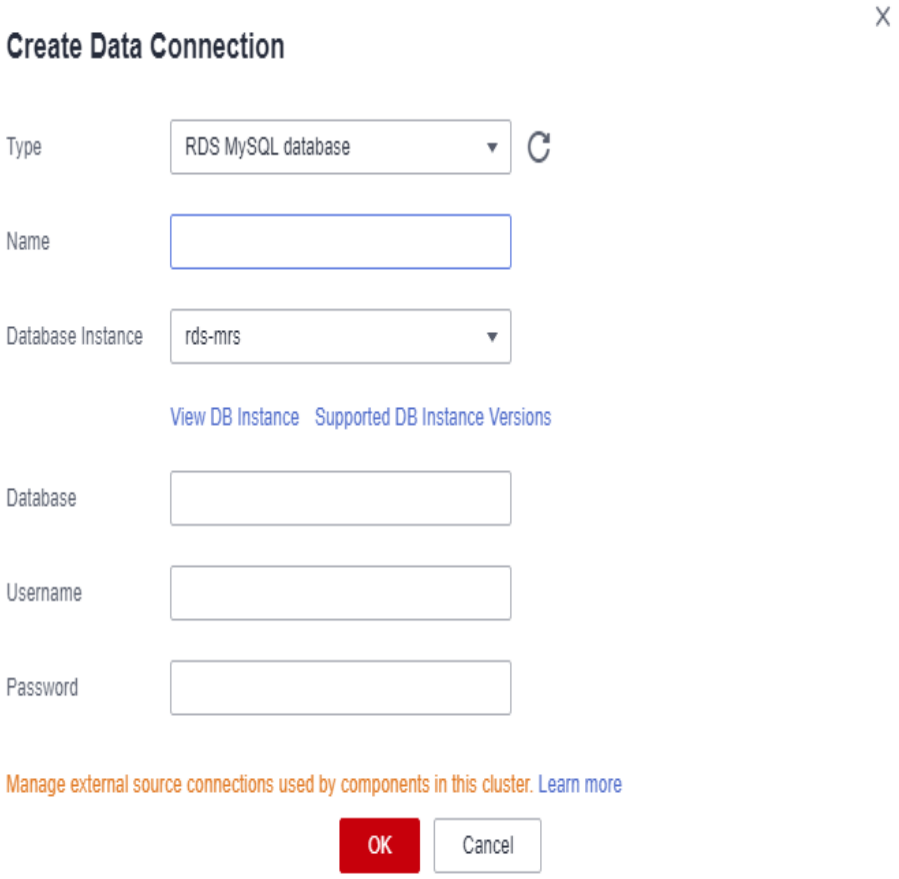
Paso 3 Configure los parámetros de acuerdo con **Tabla 2-15**.

Tabla 2-15 Parámetros para crear una conexión de datos

Parámetro	Descripción
Type	Tipo de conexión de origen externa. Las opciones de valor son las siguientes: ● **RDS PostgreSQL database**. Los clústeres que admiten Hive pueden conectarse a este tipo de base de datos. ● **RDS MySQL database**. Clústeres que soportan Hive o Ranger pueden conectarse a este tipo de base de datos.
Name	El nombre de una conexión de datos.

Parámetro	Descripción
Database Instance	La instancia de base de datos de RDS. Esta instancia debe crearse en RDS antes de que se haga referencia aquí y la base de datos debe haber sido creada. Para obtener más información, consulte **Preparaciones**. Haga clic en **View DB Instance** para ver las instancias de base de datos creadas. **NOTA** ● Para garantizar las comunicaciones de red entre el clúster y la base de datos de PostgreSQL, cree la instancia en la misma VPC y subred que el clúster. ● La regla de entrada del grupo de seguridad de la instancia de base de datos de RDS debe permitir el acceso de la instancia al puerto 3306. Para configurarlo, haga clic en el nombre de la instancia en la consola de RDS para ir a la página de gestión de instancias. En el área **Connection Information**, haga clic en el nombre junto a **Security Group**. En la página que se muestra, haga clic en la pestaña **Inbound Rules** y, a continuación, haga clic en **Add Rule**. En el cuadro de diálogo **Add Inbound Rule** mostrado, en el área **Protocol & Port** seleccione **TCP** e introduzca el número de puerto **3306**. En el área **Source**, seleccione **IP address** e introduzca las direcciones IP de todos los nodos donde se encuentran las instancias MetaStore de Hive. ● Actualmente, MRS es compatible con **PostgreSQL9.5/ PostgreSQL9.6** en RDS. ● Actualmente, MRS solo admite **MySQL 5.7.*x*** en RDS.
Database	El nombre de la base de datos a la que se va a conectar.
Username	El nombre de usuario para iniciar sesión en la base de datos que se va a conectar.
Password	La contraseña para iniciar sesión en la base de datos que se va a conectar.

Figura 2-26 Parámetros para crear una conexión a base de datos de RDS



NOTA

Cuando **Type** se establece en **RDS MySQL database** o **GaussDB(for MySQL)**, **Username** debe ser **root**. Si el usuario no es **root**, realice operaciones haciendo referencia a **Preparaciones**.

Paso 4 Haga clic en **OK**.

----Fin

Configuración de una conexión de datos de RDS durante la creación de clústeres

Configure una conexión de datos de RDS al crear un clúster MRS.

Paso 1 Inicie sesión en la consola de gestión de MRS.

Paso 2 Haga clic en **Buy Cluster**. Se muestra la página para comprar un clúster.

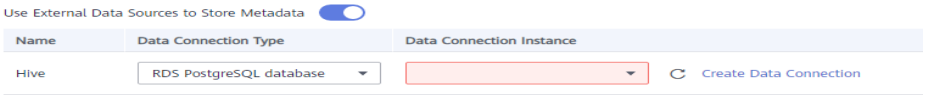
Paso 3 Haga clic en la pestaña **Custom Config**.

Paso 4 En el área de configuración del software, ajuste **Metadata** según **Tabla 2-16**. Para otros parámetros, consulte **Compra de un clúster personalizado** para la configuración y la creación de clústeres.

Tabla 2-16 Parámetros de conexión de datos

Parámetro	Descripción
Metadata	Seleccione **External data connection**. Se utilizan metadatos de fuentes de datos externas. Si el clúster es anormal o se elimina, los metadatos no se verán afectados. Este modo se aplica a escenarios en los que el almacenamiento y la computación están desacoplados. Los clústeres que admiten Hive o Ranger admiten esta función.
Name	Este parámetro sólo está disponible cuando se selecciona **External data connection** para **Metadata**. Indica el nombre del componente para el que se puede configurar una fuente de datos externa. ● Hive ● Ranger
Data Connection Type	Este parámetro sólo está disponible cuando se selecciona **External data connection** para **Metadata**. Indica el tipo de origen de datos externo. ● Hive admite los siguientes tipos de conexión de datos: – **RDS PostgreSQL database** – **RDS MySQL database** – **Local database** ● Ranger admite los siguientes tipos de conexión de datos: – **RDS PostgreSQL database** – **RDS MySQL database** – Local database
Data Connection Instance	Este parámetro no es necesario cuando **Data Connection Type** se establece en **Local database**. Indica el nombre de la conexión entre el clúster MRS y la base de datos de RDS. Esta instancia debe ser creada antes de ser referenciada aquí. Puede hacer clic en **Create Data Connection** para crear una conexión de datos. Para más detalles, véase **Preparaciones** y **Creación de una conexión de datos de RDS**.

Figura 2-27 Configuración de una conexión de datos durante la creación del clúster



----Fin

2.8.2.2 Configuración de conexiones de datos de Ranger

Cambie los metadatos del Ranger del clúster existente a los metadatos almacenados en la base de datos de RDS. Esta operación permite que varios clústeres MRS compartan los mismos

metadatos y los metadatos no se eliminarán cuando se eliminen los clústeres. De esta manera, la migración de metadatos de Ranger no es necesaria durante la migración del clúster.

Prerrequisitos

Ha creado una instancia de base de datos MySQL de RDS haciendo referencia a **Creación de una conexión de datos de RDS**.

NOTA

- Para las versiones anteriores a MRS 3.*x*, si **Type** está establecido en **RDS MySQL database**, **Username** debe ser **root**. Si el usuario no es **root**, cree un usuario y conceda permisos al usuario haciendo referencia a **Preparaciones**.
- Para los clústeres de MRS 3.*x* o posteriores, cuando **Type** está establecido en **RDS MySQL database**, **Username** no debe ser **root**. En este caso, cree un usuario y conceda permisos al usuario haciendo referencia a **Preparaciones**.

Preparación para la configuración de metadatos de Ranger de base de datos de MySQL

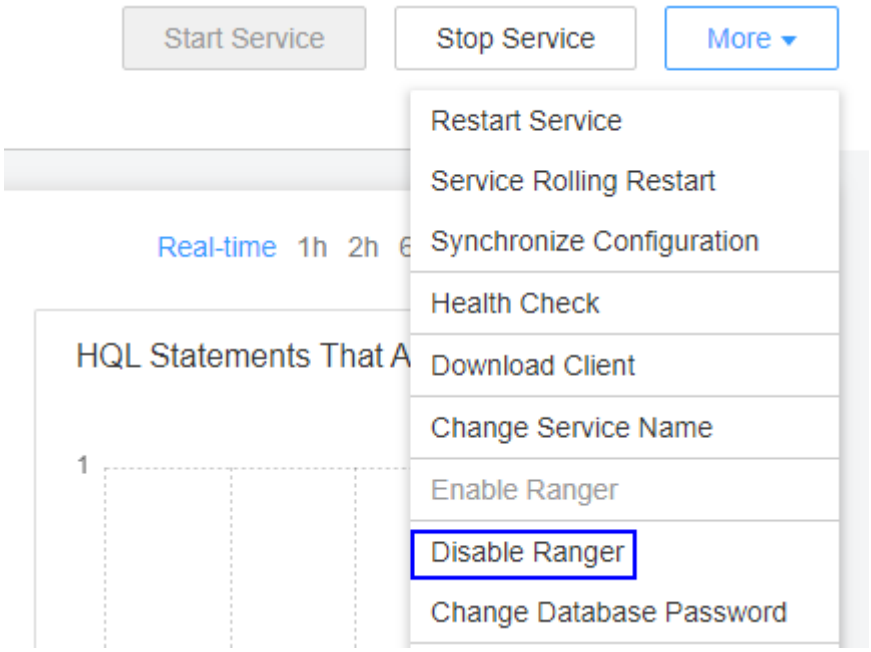
Esta operación solo es necesaria para **MRS 3.1.0 o posterior**.

Paso 1 Inicie sesión en FusionInsight Manager. Para más detalles, consulte **Acceder a FusionInsight Manager (MRS 3.x o posterior)**. Elija **Clusters** > **Services** > *Service name*.

Actualmente, los siguientes componentes en un clúster MRS 3.1.*x* admiten la autenticación de Ranger: HDFS, HBase, Hive, Spark, Impala, Storm, y Kafka.

Paso 2 En la esquina superior derecha de la página **Dashboard**, haga clic en **More** y seleccione **Disable Ranger**. Si **Disable Ranger** está atenuado, la autenticación de Ranger está deshabilitada, como se muestra en el documento **Figura 2-28**.

Figura 2-28 Desactivación de la autenticación de Ranger



Paso 3 (Opcional) Para utilizar una política de autenticación existente, realice este paso para exportar la política de autenticación en la página web de Ranger. Después de cambiar los metadatos del Ranger, puede importar de nuevo la política de autenticación existente. A continuación se utiliza Hive como ejemplo. Después de la exportación, se genera un archivo de política en formato JSON en un directorio local.

1. Inicie sesión en FusionInsight Manager.
2. Seleccione **Cluster** > **Services** > **Ranger** para ir a la página de descripción general del servicio Ranger.
3. Haga clic en **RangerAdmin** en el área **Basic Information** para ir a la interfaz de usuario web de Ranger.

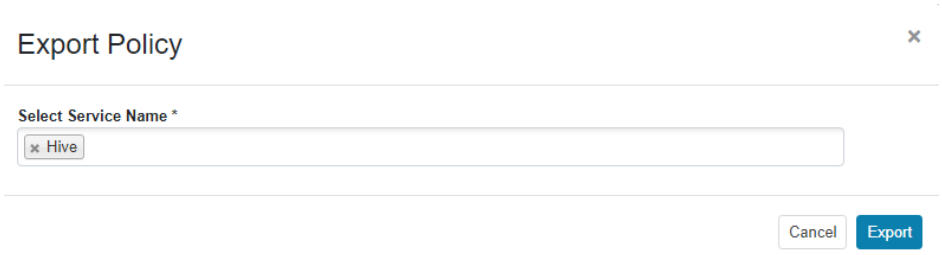
   El usuario **admin** de Ranger pertenece al tipo **User**. Para ver todas las páginas de gestión, haga clic en el nombre de usuario en la esquina superior derecha y seleccione **Log Out** para salir del sistema.
4. Inicie sesión en el sistema como usuario **rangeradmin** (contraseña predeterminada: **Rangeradmin@123**) u otro usuario que tenga los permisos de administrador de Ranger. Para obtener más información sobre los usuarios y sus contraseñas predeterminadas, consulte Lista de cuenta de usuario.
5. Haga clic en el botón de exportación en la fila donde se encuentra el componente Hive para exportar la política de autenticación.

   Figura 2-29 Exportación de políticas de autenticación

6. Haga clic en **Export**. Una vez finalizada la exportación, se genera un archivo de política en formato JSON en un directorio local.

   Figura 2-30 Exportación de políticas de autenticación de Hive

----Fin

Configuración de una conexión de datos para un clúster MRS

Paso 1 Inicie sesión en la consola de MRS.

Paso 2 Haga clic en el nombre del clúster para ver sus detalles.

Paso 3 Haga clic en **Manage** a la derecha de **Data Connection** para ir a la página de configuración de la conexión de datos.

Paso 4 Haga clic en **Configure Data Connection** y defina los parámetros relacionados.

- **Component Name**: Ranger
- **Module Type**: Metadatos de Ranger
- **Connection Type**: Base de datos de MySQL de RDS
- **Connection Instance**: Seleccione una instancia de base de datos de MySQL de RDS creada. Para obtener más información acerca de cómo crear una conexión de datos, consulte **Creación de una conexión de datos de RDS**.

Paso 5 Seleccione **I understand the consequences of performing the scale-in operation** y haga clic en **Test**.

Paso 6 Después de que la prueba se realice correctamente, haga clic en **OK** para completar la configuración de la conexión de datos.

Paso 7 Inicie sesión en FusionInsight Manager.

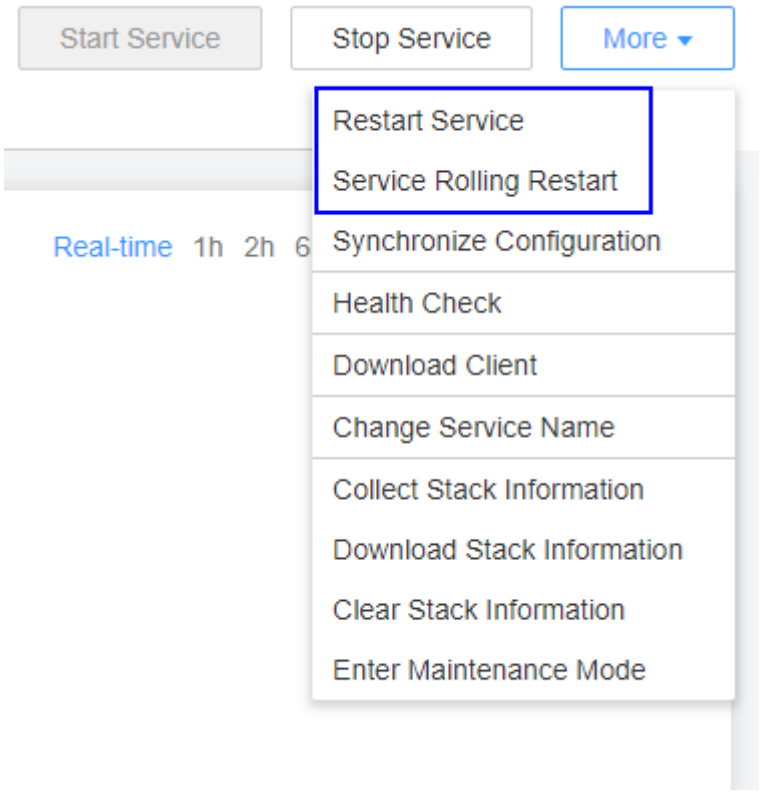
Paso 8 Seleccione **Cluster** > **Services** > **Ranger** para ir a la página de descripción general del servicio Ranger.

Paso 9 Elija **More** > **Restart Service** or **More** > **Service Rolling Restart**.

Si elige **Restart Service**, los servicios se interrumpirán durante el reinicio. Si selecciona **Service Rolling Restart**, el reinicio rodante puede minimizar el impacto o no afectar a la ejecución del servicio.

Reiniciar Ranger afectará a los permisos de todos los componentes controlados por Ranger y puede afectar al funcionamiento normal de los servicios. Por lo tanto, reinicie Ranger cuando el clúster esté inactivo o durante las horas no pico. Antes de reiniciar el componente Ranger, las políticas del componente Ranger siguen surtiendo efecto.

Figura 2-31 Reinicio de un servicio

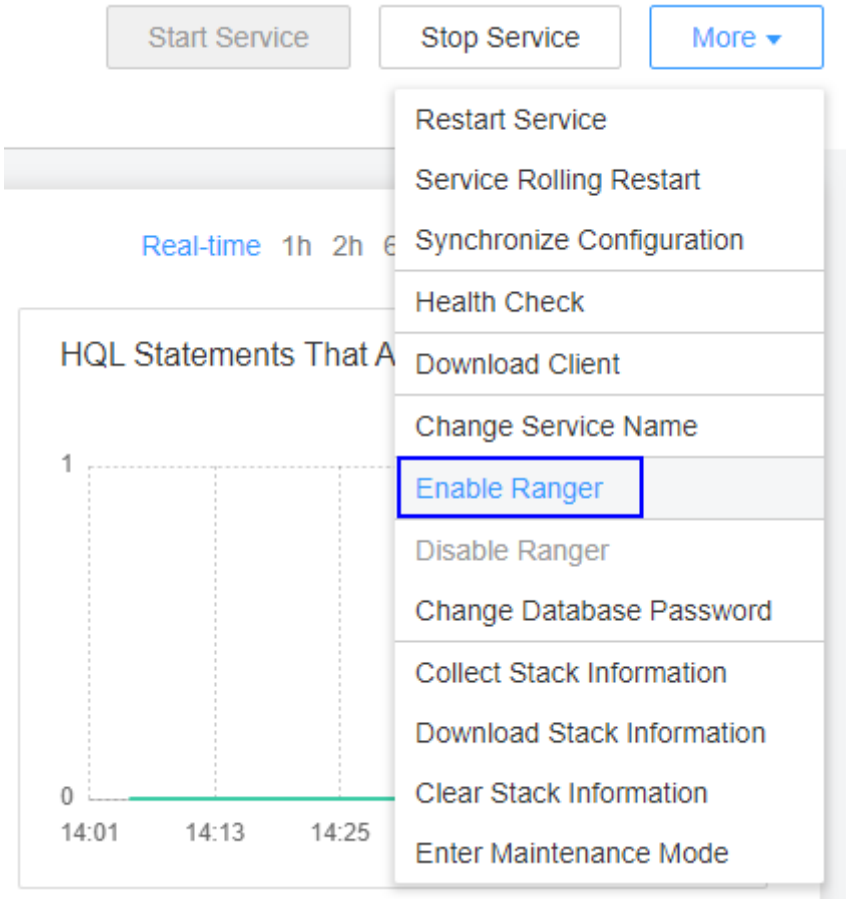


Paso 10 Habilitar la autenticación de Ranger para el componente que se va a autenticar. El componente Hive se utiliza como ejemplo.

Actualmente, los siguientes componentes en un clúster MRS 3.1.*x* admiten la autenticación de Ranger: HDFS, HBase, Hive, Spark, Impala, Storm, y Kafka.

1. Inicie sesión en FusionInsight Manager y elija **Cluster** > **Services** > *Service Name*.
2. En la esquina superior derecha de la página **Dashboard**, haga clic en **More** y seleccione **Enable Ranger**.

Figura 2-32 Habilitación de la autenticación de Ranger

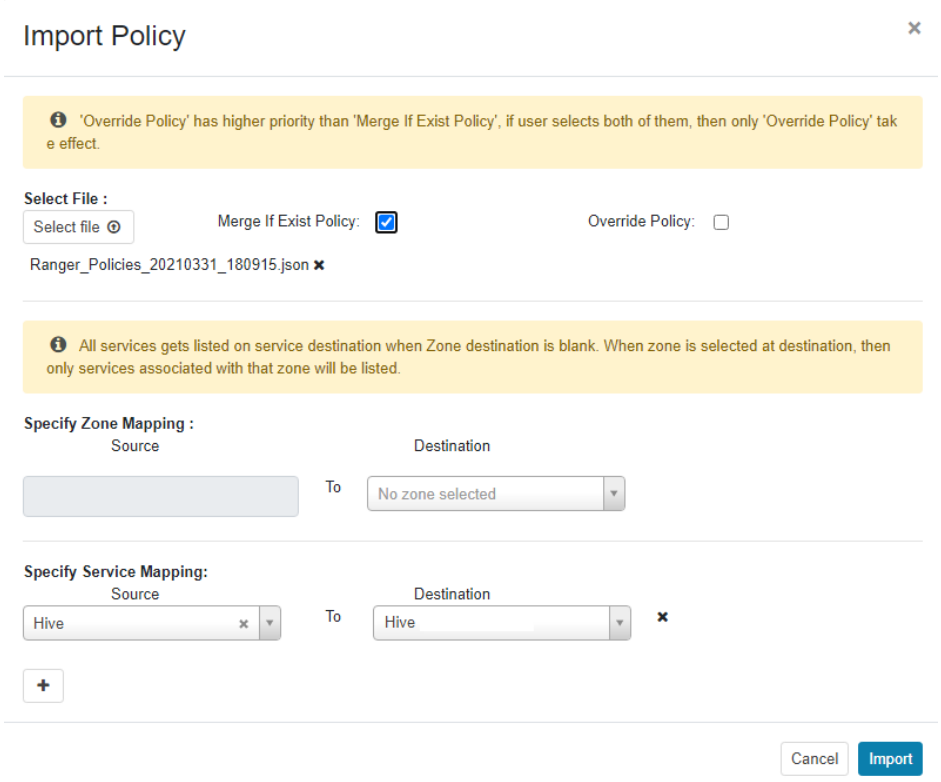


Paso 11 Inicie sesión en la interfaz de usuario web de Ranger y haga clic en el botón de importación en la fila del componente Hive.

Paso 12 Importar parámetros.

- Haga clic en **Select file** y seleccione el archivo de política de autenticación descargado en **Paso 3.6**.
- Seleccione **Merge If Exist Policy**.

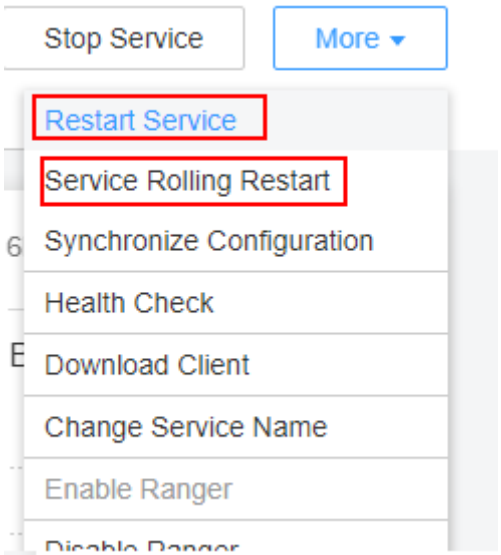
Figura 2-33 Importación de políticas de autenticación



Paso 13 Reinicie el componente para el que está habilitada la autenticación de Ranger.

1. Inicie sesión en FusionInsight Manager.
2. Elija **Cluster** > **Services** > **Hive** to para ir a la página de descripción del servicio Hive.
3. Elija **More** > **Restart Service** or **More** > **Service Rolling Restart**.

Figura 2-34 Reinicio de un servicio



Si elige **Restart Service**, los servicios se interrumpirán durante el reinicio. Si selecciona **Service Rolling Restart**, el reinicio rodante puede minimizar el impacto o no afectar a la ejecución del servicio.

----Fin

2.8.2.3 Configuración de una conexión de datos de Hive

Esta sección describe cómo cambiar los metadatos de Hive de un clúster activo a los metadatos almacenados en una base de datos local o base de datos de RDS después de comprar un clúster. Esta operación permite que varios clústeres MRS compartan los mismos metadatos y los metadatos no se eliminarán cuando se eliminen los clústeres. De esta manera, la migración de metadatos de Hive no es necesaria durante la migración del clúster.

NOTA

- Cuando los metadatos de Hive se cambian entre diferentes clústeres, MRS sincroniza solo los permisos en la base de datos de metadatos del componente Hive. El modelo de permiso en MRS se mantiene en MRS Manager. Por lo tanto, cuando los metadatos de Hive se cambian entre clústeres, los permisos de los usuarios o grupos de usuarios no se pueden sincronizar automáticamente con MRS Manager de otro clúster.
- Para los clústeres cuya versión es anterior a MRS 3.*x*, si la conexión de datos seleccionada es **RDS MySQL database**, asegúrese de que el usuario de la base de datos es **root**. Si el usuario no es **root**, cree un usuario y conceda permisos al usuario haciendo referencia a **Preparaciones**.
- Para los clústeres de MRS 3.*x* o posteriores, cuando **Type** está establecido en **RDS MySQL database**, **Username** no debe ser **root**. En este caso, cree un usuario y conceda permisos al usuario haciendo referencia a **Preparaciones**.

Configuración de una conexión de datos de Hive

Esta función no es compatible con MRS 3.0.5.

Paso 1 Inicie sesión en la consola de MRS. En el panel de navegación de la izquierda, elija **Clusters** >**Active Clusters**.

Paso 2 Haga clic en el nombre de un clúster para ir a la página de detalles del clúster.

Paso 3 En la página de la pestaña **Dashboard**, haga clic en **Manage** junto a **Data Connection**.

Paso 4 En el cuadro de diálogo **Data Connection**, se muestran las conexiones de datos asociadas con el clúster. Puede hacer clic en **Edit** o **Delete** para editar o eliminar las conexiones de datos.

Paso 5 Si no hay ninguna conexión de datos asociada en el cuadro de diálogo **Data Connection**, haga clic en **Configure Data Connection** para agregar una conexión.

NOTA

Solo se puede configurar una conexión de datos para un tipo de módulo. Por ejemplo, después de configurar una conexión de datos para los metadatos de Hive, no se puede configurar ninguna otra conexión de datos para ella. Si no hay ningún tipo de módulo disponible, el botón **Configure Data Connection** no estará disponible.

Tabla 2-17 Configuración de una conexión de datos de Hive

Parámetro	Descripción
Component	Hive

Parámetro	Descripción
Module Type	Metadatos de Hive
Data Connection Type	● Base de datos de RDS PostgreSQL (compatible con clústeres de MRS 1.9.*x*) ● Base de datos de RDS MySQL ● Base de datos local
Instance	Este parámetro solo es válido cuando **Data Connection Type** está establecido en **RDS PostgreSQL database** o **RDS MySQL database**. Seleccione el nombre de la conexión entre el clúster MRS y la base de datos de RDS. Esta instancia debe ser creada antes de ser referenciada aquí. Puede hacer clic en **Create Data Connection** para crear una conexión de datos. Para obtener más información, consulte **Creación de una conexión de datos de RDS**.

Paso 6 Haga clic en **Test** para probar la conectividad de la conexión de datos.

Paso 7 Una vez que la conexión de datos se haya realizado correctamente, haga clic en **OK**.

NOTA

- Después de configurar los metadatos de Hive, reinicie Hive. Hive creará las tablas de base de datos necesarias en la base de datos especificada. (Si ya existen tablas, no se crearán.)
- Antes de reiniciar el servicio Hive, asegúrese de que el paquete de controlador se ha instalado en todos los nodos donde se encuentran las instancias de Metastore.
  - Postgres: Utilice el paquete de controlador Postgres de código abierto para reemplazar el existente del clúster. Sube el paquete de controladores PostgreSQL **postgresql-42.2.5.jar** al directorio *${BIGDATA_HOME}*/**third_lib/Hive** en todos los nodos de MetaStore. Para descargar el paquete de controladores de código abierto, visite **https://repo1.maven.org/maven2/org/postgresql/postgresql/42.2.5/**.
  - MySQL: Vaya al sitio web oficial de MySQL (https://www.mysql.com/). Elija **DOWNLOADS** y haga clic en **MySQL Community (GPL) Downloads**. En la página mostrada, haga clic en **Connector/J** para descargar el paquete de controlador de la versión correspondiente y cargar el paquete de controlador en el directorio **/opt/Bigdata/FusionInsight_HD_*/install/FusionInsight-Hive-*/hive-*/lib/** en todos los nodos de RDSMetastore.

----Fin

2.9 Instalación de software de terceros mediante acciones de arranque

Prerrequisitos

El script de acción de arranque se ha preparado haciendo referencia a **Preparación del script de acción de arranque**.

Adición de una acción de arranque al crear un clúster

Paso 1 Inicie sesión en la consola de gestión de MRS.

Paso 2 Haga clic en **Buy Cluster**. Se muestra la página para comprar un clúster.

Paso 3 Haga clic en la pestaña **Custom Config**.

Paso 4 Para configurar el software y el hardware del clúster, consulte **Compra de un clúster personalizado**.

Paso 5 En la página de la pestaña **Set Advanced Options**, haga clic en **Add** en el área **Bootstrap Action**.

Tabla 2-18 Parámetros

Parámetro	Descripción
Name	Nombre de una secuencia de comandos de acción de arranque El valor solo puede contener dígitos, letras, espacios, guiones (-) y guiones bajos (_) y no debe comenzar con un espacio. El valor puede contener de 1 a 64 caracteres. **NOTA** Un nombre debe ser único en el mismo clúster. Puede establecer el mismo nombre para diferentes clústeres.
Script Path	Ruta del script. El valor puede ser una ruta de sistema de archivos OBS o una ruta de VM local. ● Una ruta de sistema de archivos de OBS debe comenzar por **s3a://** y terminar por **.sh**, por ejemplo, **s3a://mrs-samples/** *xxx***.sh**. ● Una ruta de VM local debe comenzar con una barra diagonal (/) y terminar con **.sh**. **NOTA** Una ruta de acceso debe ser única en el mismo clúster, pero puede ser la misma para diferentes clústeres.
Parameter	Parámetros de script de acción de arranque
Execution Node	Seleccione un tipo del nodo donde se ejecuta el script de acción de arranque.
Executed	Seleccione la hora a la que se ejecuta el script de acción de arranque. ● Antes del inicio del componente inicial ● Después del inicio del componente inicial **NOTA** Solo puede ejecutar manualmente el script de instalación de componentes de terceros en el nodo para instalar un componente de clúster en ejecución.

Parámetro	Descripción
Action upon Failure	Si se deben continuar ejecutando secuencias de comandos posteriores y crear un clúster después de que la secuencia de comandos no se ejecute. **NOTA** Se recomienda establecer este parámetro en **Continue** en la fase de depuración para que el clúster pueda seguir siendo instalado e iniciado sin importar si la acción de arranque es correcta.
Run as root	Si se debe escalar el permiso al usuario **root** Si la acción de arranque requiere operaciones de usuario root, habilite esta función, o la acción de arranque puede no ejecutarse. **NOTA** Esta operación se aplica a los clústeres MRS 3.1.5 o posteriores.

Paso 6 Haga clic en **OK**.

Después de agregar la acción de arranque, puede editarla, clonarla o eliminarla en la columna **Operation**.

----Fin

Adición de una secuencia de comandos de automatización en la página Auto Scaling

Paso 1 Inicie sesión en la consola de gestión de MRS.

Paso 2 Elija **Clusters** > **Active Clusters**, seleccione un clúster en ejecución y haga clic en su nombre para ir a su página de detalles.

Paso 3 Haga clic en la pestaña **Nodes**. En esta página de fichas, haga clic en **Auto Scaling** en la columna **Operation** del grupo de nodos de tareas. Se muestra la página **Auto Scaling**.

Si no hay ningún nodo de tarea disponible, haga clic en **Configure Task Node** para agregar un nodo de tarea y, a continuación, realice este paso.

NOTA

Configure Task Node solo está disponible para el análisis de MRS 3.*x* o posterior, streaming y clústeres híbridos.

Paso 4 Configurar un plan de recursos.

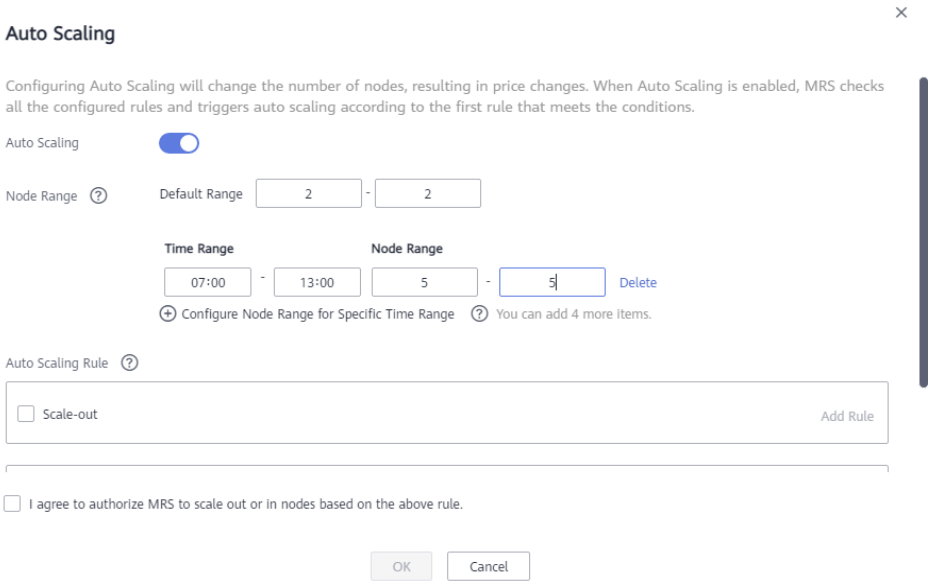
Se puede configurar un plan de recursos para ajustar el número de nodos, lo que afecta al precio real. Tenga cuidado al realizar esta operación.

Procedimiento de configuración:

1. En la página **Auto Scaling**, habilite **Auto Scaling**.
2. Por ejemplo, el **Default Range** de la cantidad de nodos se establece en **2-2** indicando que el número de nodos de tarea se fija en 2 excepto el intervalo de tiempo especificado en el plan de recursos.
3. Haga clic en **Configure Node Range for Specific Time Range** en **Default Range**.

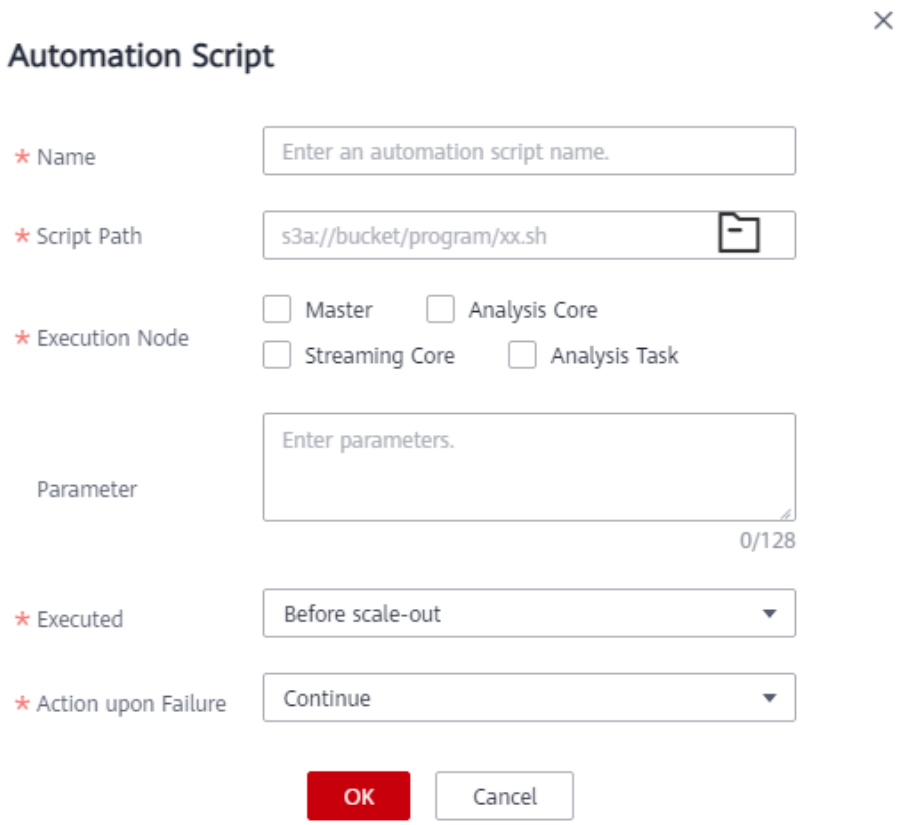
4. Configure **Time Range** y **Node Range**. Por ejemplo, establezca **Time Range** en **07:00-13:00** y **Node Range** en **5-5**. Esto indica que el número de nodos de tarea se fija en 5 en el intervalo de tiempo especificado en el plan de recursos.

   Puede hacer clic en **Configure Node Range for Specific Time Range** para configurar varios planes de recursos.



Paso 5 (Opcional) Configurar scripts de automatización.

1. Ajuste **Advanced Settings** a **Configure**.
2. Haga clic en **Create**. Se muestra la página **Automation Script**.
3. Establezca **Name**, **Script Path**, **Execution Node**, **Parameter**, **Executed**, y **Action upon Failure**. Para obtener más información sobre los parámetros, consulte **Tabla 2-14**.
4. Haga clic en **OK** para guardar las configuraciones del script de automatización.



Paso 6 Seleccione **I agree to authorize MRS to scale out or scale in nodes based on the above rule**.

Paso 7 Haga clic en **OK**.

----Fin

2.10 Consulta de tareas de MRS fallidas

En esta sección se describe cómo ver y eliminar una tarea de MRS fallida.

Antecedentes

Si un clúster no se puede crear, finalizar, escalar o escalar, se muestra la página **Manage Failed Tasks**. En la página **Cluster History** sólo se muestran las tareas que no se pueden eliminar. Puede eliminar una tarea fallida que no sea necesaria.

Procedimiento

Paso 1 Inicie sesión en la consola de MRS.

Paso 2 En el panel de navegación izquierdo, elija **Clusters** >**Active Clusters**.

Paso 3 Haga clic en o en el número situado a la derecha de **Failed Tasks**. Se muestra la página **Manage Failed Tasks**.

Paso 4 En la columna **Operation** del clúster que desea iniciar, haga clic en **Delete**.

En este paso, solo se puede eliminar un trabajo.

Paso 5 Puede hacer clic en **Delete All** en la esquina superior izquierda de la lista de tareas para eliminar todas las tareas fallidas.

----Fin

2.11 Consulta de información de un clúster histórico

Elija **Clusters > Cluster History** y haga clic en el nombre de un clúster de destino. Puede ver la información de configuración del clúster, los nodos, la información de escalamiento automático, la información de componentes, la información del trabajo, la acción de arranque y las etiquetas.

En la siguiente tabla se describen los parámetros de la información histórica del clúster.

Tabla 2-19 Información básica del clúster

Parámetro	Descripción
Cluster Name	Nombre de un clúster. El nombre del clúster se establece cuando se crea el clúster.
Cluster Status	Estado de un clúster.
Billing Mode	Modo de facturación de un clúster. Actualmente, son compatibles con **Pay-per-use** y **Yearly/Monthly**.
Cluster Version	Versión del clúster
Cluster Type	Tipo del clúster que se va a crear.
Obtaining a cluster ID	Identificador único de un clúster, que se asigna automáticamente cuando se crea un clúster
Created	Hora en la que se crea un clúster.
Order ID	ID de pedido para crear el clúster. Este parámetro sólo está disponible cuando **Billing Mode** está establecido en **Yearly/Monthly**.
AZ	Zona de disponibilidad (AZ) en la región de un clúster, que se establece cuando se crea un clúster.
Default Subnet	Subred seleccionada durante la creación del clúster. Una subred proporciona recursos de red dedicados que están aislados de otras redes, lo cual mejora la seguridad de la red.
VPC	VPC seleccionada durante la creación del clúster. Una VPC es un entorno de red seguro, aislado y lógico.
OBS Permission Control	Haga clic en **Manage** y modifique la asignación entre los usuarios de MRS y los permisos de OBS.

Parámetro	Descripción
Creating a data connection	Haga clic en **Manage** para ver el tipo de conexión de datos asociado al clúster. Para obtener más información, consulte **Configuración de conexiones de datos**.
Agency	Haga clic en **Manage Agency** para enlazar o modificar una agencia para el clúster. Una delegación permite al ECS o al BMS gestionar recursos del MRS. Puede configurar una agencia del tipo ECS para obtener automáticamente el AK/SK para acceder a OBS. La agencia **MRS_ECS_DEFAULT_AGENCY** tiene el permiso OBSOperateAccess de OBS y los permisos CESFullAccess (para usuarios que han habilitado políticas detalladas), CES Administrator y KMS Administrator en la región donde se encuentra el clúster.
Key Pair	Nombre de un par de claves. Establezca este parámetro al crear un clúster. Si el modo de inicio de sesión se establece en contraseña durante la creación del clúster, este parámetro no se muestra.
Kerberos Authentication	Si se debe habilitar la autenticación de Kerberos al iniciar sesión en Manager. **NOTA** La autenticación de Kerberos no se puede habilitar o deshabilitar manualmente después de crear el clúster. Establezca este parámetro con precaución al crear un clúster. Si necesita cambiar el estado de autenticación, se recomienda crear un nuevo clúster.
Enterprise Project	Proyecto de empresa al que pertenece un clúster. Sólo en la página **Active Clusters** puede hacer clic en el nombre de un proyecto de empresa para ir a su página **Proyecto empresarial Management**.
Security Group	Nombre del grupo de seguridad del clúster.
Streaming Core Node LVM	Indica si se habilita la función LVM (Logical Volume Manager) de los nodos de Core de streaming.
Data Disk Key Name	Nombre de la clave utilizada para cifrar los discos de datos. Para gestionar las claves usadas, inicie sesión en la consola de gestión de claves.
Data Disk Key ID	ID de la clave utilizada para cifrar los discos de datos.
Component Version	Versión de cada componente instalado en el clúster.
Agency	Delega ECS o BMSs para gestionar algunos de sus recursos.

Vuelve a la página de clústeres históricos. Puede utilizar los siguientes botones para realizar operaciones. Para obtener más información sobre los botones, consulte la tabla siguiente.

Tabla 2-20 Descripción de íconos

Ícono	Descripción
	Haga clic en  para actualizar manualmente la información del nodo.
	Escriba un nombre de clúster en la barra de búsqueda y haga clic en  para buscar un clúster.

3 Gestión de clústeres

3.1 Inicio de sesión en un clúster

3.1.1 Descripción del nodo de clúster de MRS

Un clúster MRS consta de múltiples ECS. El sistema gestiona los nodos en los grupos de nodos basándose en las especificaciones. Los nodos del mismo grupo de nodos utilizan las mismas especificaciones de ECS. Los nodos de un clúster se pueden clasificar en nodos de Master, nodos de Core y nodos de task según los roles de los componentes desplegados en los nodos. Para obtener más información acerca de los tipos de nodo, consulte **Tabla 3-1**.

Tabla 3-1 Tipos de nodos de clúster

Tipo de nodo	Funciones
Nodo principal	Nodo de gestión de un clúster de MRS. Gestiona y monitorea el clúster. En el árbol de navegación de la consola de gestión de MRS, elija **Clusters** > **Active Clusters**, seleccione un clúster en ejecución y haga clic en su nombre para cambiar a la página de detalles del clúster. En la página de la pestaña **Nodes**, vea el **Name**. El nodo que contiene **master1** en su nombre es el nodo Master1. El nodo que contiene **master2** en su nombre es el nodo Master2. Puede iniciar sesión en un nodo de Master mediante VNC en la consola de gestión de ECS o mediante SSH. Después de iniciar sesión en el nodo de Master, puede acceder a los nodos de Core sin introducir contraseñas. El sistema implementa automáticamente los nodos de Master en modo activo/en espera y admite la función de alta disponibilidad (HA) para la gestión de clústeres de MRS. Si el nodo de gestión activo falla, el nodo de gestión en espera cambia al estado activo y se hace cargo de los servicios. Para determinar si el nodo Master1 es el nodo de gestión activo, consulte **Determinación de nodos de gestión activos y en espera**.
Core node	Nodo de trabajo de un clúster de MRS. Procesa y analiza datos y almacena datos de proceso. En la pestaña **Nodes** de la página de detalles del clúster, los nodos del grupo de nodos cuyo **Node Type** es **Core** son nodos centrales.
Task node	Nodo de cómputo. Cuando los recursos de procesamiento de un clúster son insuficientes, puede configurar políticas de escalado elástico para aumentar los nodos automáticamente. En la pestaña **Nodes** de la página de detalles del clúster, los nodos del grupo de nodos cuyo **Node Type** es **Task** son nodos de tarea. Si solo se despliega el rol **NodeManager (Yarn)** o **Supervisor (Storm)** en un grupo de nodos además de los roles obligatorios básicos, este grupo de nodos es un grupo de nodos de Task.

Los nodos de clúster de MRS admiten el inicio de sesión remoto. Los siguientes métodos de inicio de sesión remoto están disponibles:

- GUI login: Utilice la función de inicio de sesión remoto proporcionada por la consola de gestión de ECS para iniciar sesión en la interfaz de Linux del nodo de Master en el clúster.
- Inicio de sesión de SSH: Solo se aplica a los ECS de Linux. Puede utilizar una herramienta de inicio de sesión remoto (como PuTTY) para iniciar sesión en un ECS. El ECS debe tener una EIP enlazada.

Para obtener detalles sobre cómo solicitar y vincular EIP para el nodo de Master, consulte **Asignación de un EIP**.

Puede iniciar sesión en un ECS de Linux utilizando un par de claves o una contraseña.

AVISO

Si necesita usar un par de claves para acceder a un nodo de clúster, debe iniciar sesión en el nodo como usuario **root**. Para obtener más información, consulte **Inicio de sesión en un ECS mediante un par de claves (SSH)**.

Para obtener más información acerca de cómo acceder a un nodo de clúster mediante una contraseña, consulte **Inicio de sesión en un ECS mediante una contraseña (SSH)**.

3.1.2 Inicio de sesión en un ECS

Esta sección describe cómo iniciar sesión remotamente en un ECS en un clúster MRS mediante la función de inicio de sesión remoto (modo VNC) proporcionada en la consola de gestión de ECS o una clave o contraseña (modo SSH). El inicio de sesión remoto (modo VNC) se utiliza principalmente para operaciones y mantenimiento de emergencia. En otros escenarios, se recomienda iniciar sesión en ECS mediante SSH.

NOTA

Para iniciar sesión en un nodo de clúster mediante SSH, debe agregar una regla de entrada al grupo de seguridad del clúster. Establezca **Source** en *IPv4 address of the client*/**32** o *IPv6 address of the client*/**128** y establezca el número de puerto en **22**. Para obtener más información, consulte **Adición de una regla de grupo de seguridad**.

Inicio de sesión en un ECS con VNC

Paso 1 Inicie sesión en la consola de gestión de MRS.

Paso 2 Elija **Clusters > Active Clusters** y seleccione un clúster en ejecución y haga clic en su nombre para cambiar a la página de detalles del clúster.

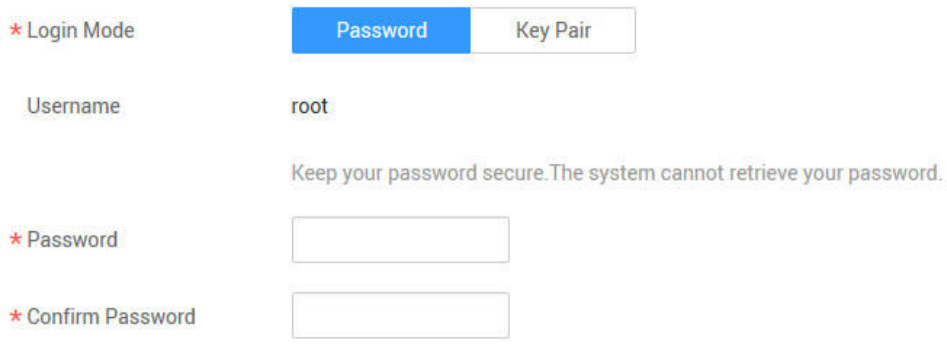
Paso 3 En la página de pestaña **Nodes**, haga clic en el nombre de un nodo de Master en el grupo de nodos de Master para iniciar sesión en la consola de gestión de ECS.

Paso 4 En la esquina superior derecha, haga clic en **Remote Login**.

Paso 5 Introduzca el nombre de usuario y la contraseña para iniciar sesión en el nodo de Master según se le solicite.

1. Si selecciona **Password** para **Login Mode**, debe ingresar **root** en **Username** y la contraseña que estableció durante la creación del clúster en **Password**.

Figura 3-1 Selección de contraseña como modo de inicio de sesión



2. Si selecciona **Key Pair** para **Login Mode** al crear un clúster, realice las siguientes operaciones para iniciar sesión en el clúster:
   a. Una vez creado el clúster, asigne una EIP y envíelo al nodo de Master del clúster. Para obtener más información, consulte **Asignación de un EIP**.
   b. Inicie sesión remotamente en el nodo de Master en modo SSH como usuario **root** usando el archivo de clave.
   c. Ejecute el comando **passwd root** para establecer una contraseña para usuario **root**.
   d. Vuelva a la interfaz de inicio de sesión e ingrese **root** y la contraseña establecida en **Paso 5.2.c** para iniciar sesión en el nodo.

----Fin

Inicio de sesión en un ECS mediante un par de claves (SSH)

Inicio de sesión en el ECS desde Windows local

Para iniciar sesión en Linux ECS desde Windows local, realice las operaciones descritas en esta sección. En el siguiente procedimiento se utiliza PuTTY como ejemplo para iniciar sesión en ECS.

1. Inicie sesión en la consola de gestión de MRS.
2. Seleccione **Clusters** > **Active Clusters**, seleccione un clúster en ejecución y haga clic en su nombre para cambiar a la página de detalles del clúster.
3. En la página de pestaña **Nodes**, haga clic en el nombre de un nodo de Master en el grupo de nodos de Master para iniciar sesión en la consola de gestión de ECS.
4. Haga clic en la pestaña **EIPs**, haga clic en **Bind EIP** para enlazar una EIP al ECS y registrar la EIP. Si una EIP ha sido vinculado al ECS, omita este paso.
5. Compruebe si el archivo de clave privada se ha convertido al formato **.ppk**.
   – En caso afirmativo, vaya a **10**.
   – Si no, vaya a **6**.
6. Ejecute PuTTY.
7. En el área **Actions**, haga clic en **Load** e importe el archivo de clave privada que utilizó durante la creación de ECS.

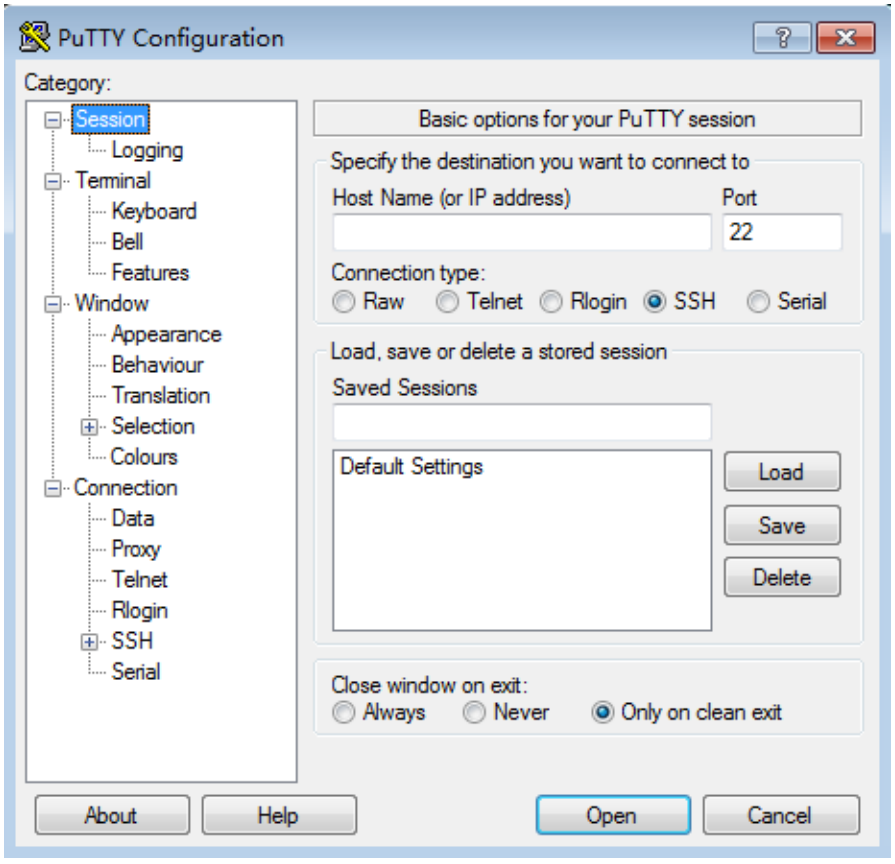
   Asegúrese de que el archivo de clave privada tenga el formato **All files (*.*)**.
8. Haga clic en **Save private key**.

9. Guarde la clave privada convertida, por ejemplo **kp-123.ppk** en un directorio local.
10. Ejecute PuTTY.
11. Elija **Connection** > **Data**. Ingrese el nombre de usuario de la imagen en **Auto-login username**.

    NOTA

    El nombre de usuario de la imagen para los nodos del clúster es **root**.
12. Elija **Connection** > **SSH** > **Auth**. En el último elemento de configuración **Private key file for authentication**, haga clic en **Browse** y seleccione la clave privada convertida en 9.
13. Haga clic en **Session**.
    a. **Host Name (or IP address)**: Introduzca la EIP enlazado al ECS.
    b. **Port**: Ingrese **22**.
    c. **Connection Type**: Seleccione **SSH**.
    d. **Saved Sessions**: Nombre de la tarea, que se puede hacer clic para la conexión remota cuando utilice PuTTY la próxima vez

    Figura 3-2 Hacer clic en **Session**



14. Haga clic en **Open** para iniciar sesión en el ECS.

    Si inicia sesión en ECS por primera vez, PuTTY muestra un cuadro de diálogo de advertencia de seguridad que le pregunta si desea aceptar el certificado de seguridad ECS. Haga clic en **Yes** para guardar el certificado en el registro local.

Inicio de sesión en ECS desde Linux local

Para iniciar sesión en Linux ECS desde Linux local, realice las operaciones descritas en esta sección. El siguiente procedimiento utiliza el archivo de clave privada **kp-123.pem** como ejemplo para iniciar sesión en ECS. El nombre de su archivo de clave privada puede diferir.

1. En la CLI de Linux, ejecute el siguiente comando para cambiar los permisos de operación:

   chmod 400 /*path*/kp-123.pem

   NOTA

   En el comando anterior, *path* se refiere a la ruta donde se guarda el archivo de clave.

2. Ejecute el siguiente comando para iniciar sesión en ECS:

   ssh -i /*path*/kp-123.pem*Default username@EIP*

   Por ejemplo, si el nombre de usuario predeterminado es **root** y la EIP es **123.123.123.123**, ejecute el siguiente comando:

   ssh -i /*path*/kp-123.pem root@123.123.123.123

   NOTA

   - *path* indica la ruta donde se guarda el archivo de clave.
   - *EIP* indica la EIP vinculada al ECS.
   - El nombre de usuario de la imagen es **root** para los nodos del clúster.

Inicio de sesión en un ECS mediante una contraseña (SSH)

Inicio de sesión en el ECS desde Windows local

Para iniciar sesión en Linux ECS desde Windows local, realice las operaciones descritas en esta sección. En el siguiente procedimiento se utiliza PuTTY como ejemplo para iniciar sesión en ECS.

Paso 1 Inicie sesión en la consola de gestión de MRS.

Paso 2 Elija **Clusters > Active Clusters** y seleccione un clúster en ejecución y haga clic en su nombre para cambiar a la página de detalles del clúster.

Paso 3 En la página de pestaña **Nodes**, haga clic en el nombre de un nodo de Master en el grupo de nodos de Master para iniciar sesión en la consola de gestión de ECS.

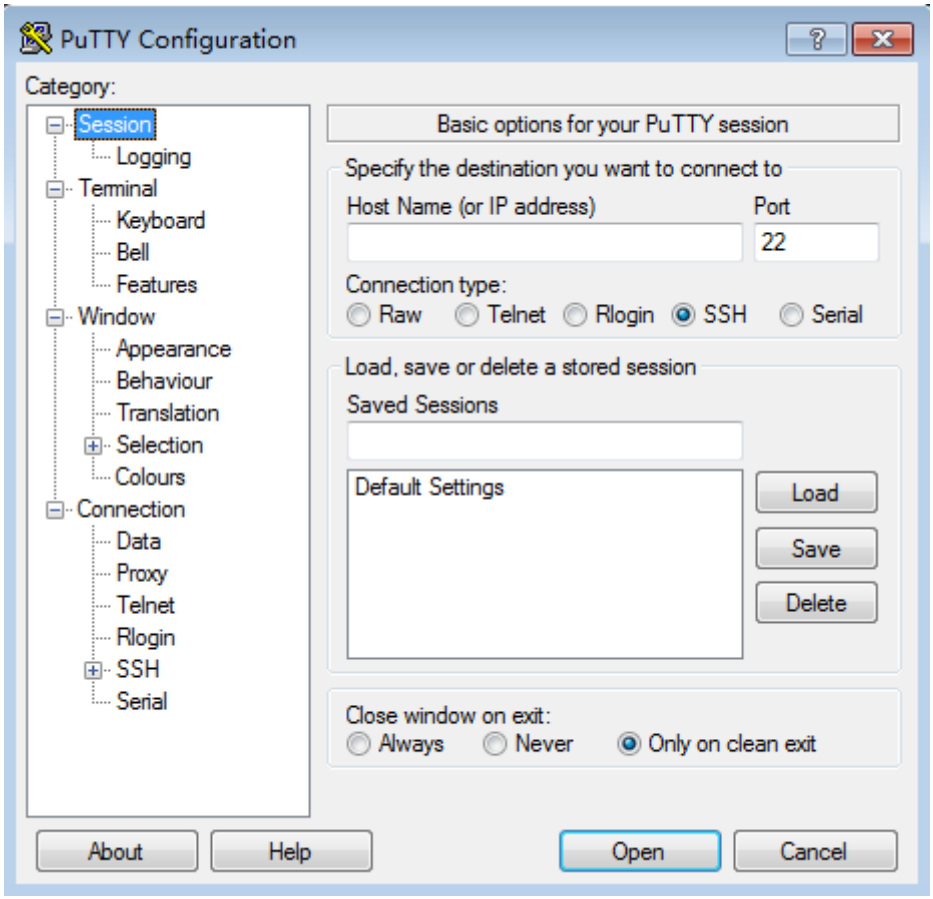
Paso 4 Haga clic en la pestaña **EIPs**, haga clic en **Bind EIP** para enlazar una EIP al ECS y registrar la EIP. Si una EIP ha sido vinculado al ECS, omita este paso.

Paso 5 Ejecute PuTTY.

Paso 6 Haga clic en **Session**.

1. **Host Name (or IP address)**: Introduzca la EIP enlazado al ECS.
2. **Port**: Ingrese **22**.
3. **Connection Type**: Seleccione **SSH**.
4. **Saved Sessions**: Nombre de la tarea, que se puede hacer clic para la conexión remota cuando utilice PuTTY la próxima vez

Figura 3-3 Hacer clic en **Session**



Paso 7 Haga clic en **Window** y seleccione **UTF-8** para **Remote character set:** en **Translation**.

Paso 8 Haga clic en **Open** para iniciar sesión en el ECS.

Si inicia sesión en ECS por primera vez, PuTTY muestra un cuadro de diálogo de advertencia de seguridad que le pregunta si desea aceptar el certificado de seguridad ECS. Haga clic en **Yes** para guardar el certificado en el registro local.

Paso 9 Después de configurar la conexión SSH al ECS, ingrese el nombre de usuario y la contraseña según se le solicite para iniciar sesión en el ECS.

NOTA

El nombre de usuario es **root** y la contraseña es la que configuraste durante la creación del clúster.

----Fin

Inicio de sesión en ECS desde Linux local

Si el host local ejecuta Linux, realice los pasos **Paso 1** a **Paso 4** para vincular una EIP al ECS, y ejecute el siguiente comando en la CLI para iniciar sesión en el ECS: **ssh *EIP bound by the ECS***

3.1.3 Determinación de nodos de gestión activos y en espera

Escenario

Algunos scripts y comandos de operación O&M deben ejecutarse o solo pueden ejecutarse en el nodo de gestión activo. Puede iniciar sesión en un nodo de Master o en el Manager (MRS 3.x o posterior) para determinar los nodos de gestión activos y en espera (nodos OMS activos y en espera).

En el modo activo/en espera, se puede implementar una conmutación entre el Master1 y Master2. Por esta razón, Master1 puede no ser el nodo de gestión activo para Manager.

Ejecución del script para determinar nodos activos y en espera

Paso 1 Encuentre los nodos de Master de un clúster MRS.

1. Inicie sesión en la consola de MRS, elija **Clusters** > **Active Clusters** y haga clic en el nombre del clúster de destino para acceder a su página de detalles.
2. En la página de pestaña **Nodes**, vea los nombres de nodo principal. El nodo que contiene **master1** en su nombre es el nodo Master1. El nodo que contiene **master2** en su nombre es el nodo Master2.

Paso 2 Determine los nodos de gestión activos y en espera del Manager.

1. Inicie sesión de forma remota en el nodo Master1. Para obtener más información, consulte **Inicio de sesión en un ECS**.

   Los nodos de Master admiten Cloud-Init. El nombre de usuario preestablecido para Cloud-Init es **root** y la contraseña es la que configuró durante la creación del clúster.
2. Ejecute los siguientes comandos para cambiar el usuario:

   sudo su - root

   su - omm
3. Ejecute el siguiente comando para identificar los nodos de gestión activo y en espera:

   Para versiones anteriores a MRS 3.*x*, ejecute el comando **sh ${BIGDATA_HOME}/om-0.0.1/sbin/status-oms.sh**.

   Para MRS 3.*x* o posterior: Ejecute el comando **sh ${BIGDATA_HOME}/om-server/om/sbin/status-oms.sh**.

   En la salida del comando, el nodo cuyo **HAActive** es **active** es el nodo de gestión activo (mgtomsdat-sh-3-01-1 en el siguiente ejemplo), y el nodo cuyo **HAActive** es **standby** es el nodo de gestión en espera (mgtomsdat-sh-3-01-2 en el siguiente ejemplo).

```
Ha mode
double
NodeName              HostName                    HAVersion
StartTime                HAActive              HAAllResOK           HARunPhase
192-168-0-30          mgtomsdat-sh-3-01-1         V100R001C01
20xx-11-18 23:43:02      active                 normal               Actived
192-168-0-24          mgtomsdat-sh-3-01-2         V100R001C01
20xx-11-21 07:14:02      standby                normal               Deactived
```

   NOTA

   Si el nodo Master1 al que ha iniciado sesión es el nodo de gestión en espera y necesita iniciar sesión en el nodo de gestión activo, ejecute el siguiente comando:

   ssh *IP address of Master2 node*

----Fin

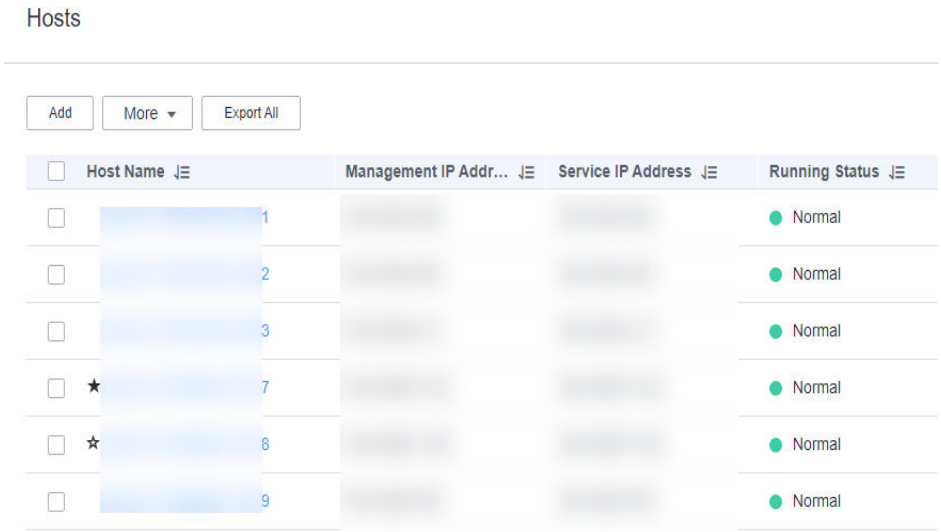
Iniciar sesión en Manager para determinar nodos activos y en espera

Esta sección solo se aplica a MRS 3.*x* o posterior.

Paso 1 Inicie sesión en Manager. Para obtener más información, consulte **Acceder a Manager**.

Paso 2 Haga clic en **Hosts**. Se muestra la página **Hosts**.

Paso 3 Vea y registre las direcciones IP de los nodos de gestión activos y en espera.



- Si un nombre de host comienza por ★ es el nodo de gestión activo (nodo OMS activo). Vea y registre el valor de **Management IP Address** en la fila que contiene el nodo activo.
- Si un nombre de host comienza por ☆ el host es un nodo de gestión en espera (nodo OMS en espera). Vea y registre el valor de **Management IP Address** en la fila que contiene el nodo en espera.

----Fin

3.2 Descripción del clúster

3.2.1 Lista de clústeres

Puede ver rápidamente el estado de todos los clústeres y trabajos al ver la información del panel y obtener documentos MRS relevantes de **Help** en el panel de navegación izquierdo de la consola de MRS.

MRS se utiliza para gestionar y analizar datos masivos. Es fácil de usar. Puede crear un clúster y agregar trabajos de MapReduce, Spark y Hive al clúster para analizar y procesar datos de usuario. Después de ser procesados, puede transmitir los datos en modo de encriptación SSL a OBS para garantizar la integridad y confidencialidad de los datos.

Estado del clúster

Tabla 3-2 muestra los estados de todos los clústeres de MRS después de iniciar sesión en la consola de gestión de MRS.

Tabla 3-2 Estado del clúster

Estado	Descripción
Starting	Si se está creando un clúster, el clúster se encuentra en el estado **Starting**.
Running	Si se crea un clúster correctamente y todos los componentes del clúster son normales, el clúster se encuentra en estado **Running**.
Scaling out	Si se agrega el nodo de Core o Task a un clúster, el clúster se encuentra en estado **Scaling out**. **NOTA** Si se produce un error en el escalado horizontal del clúster, puede volver a agregar un nodo al clúster.
Scaling in	Si detiene, elimina, cambia o reinstala los sistemas operativos de los nodos de clúster y modifica las especificaciones del nodo de clúster, se terminarán los nodos de clúster. Entonces, el clúster está en el estado **Scaling in**.
Abnormal	Si algunos componentes de un clúster son anormales, el clúster es de **Abnormal**.
Terminating	Si se está terminando un nodo de clúster de pago por uso, el clúster se encuentra en el estado de **Terminating**. **NOTA** No se puede terminar un clúster anual/mensual.
Frozen	Si el período de gracia de un recurso anual/mensual expira pero el recurso no se renueva, o si la tarifa de un recurso de pago por uso no se deduce y no ha recargado su cuenta antes de que expire el período de gracia, el sistema congela el recurso en el estado **Frozen**. **NOTA** Un clúster congelado no está disponible y todos sus ECS están cerrados. Después de ser descongelado, el clúster vuelve al estado **Running**. Si no se paga ninguna cuota de renovación, el clúster se eliminará después de un período especificado (denominado período de congelación) y el estado del clúster se cambiará a **Terminated**.
Terminated	Se ha terminado el clúster. Este parámetro sólo se muestra en **Cluster History**.
Scaling up Master node	Si se están actualizando las especificaciones de un nodo maestro, el estado del clúster es **Scaling up Master node**.

Estado del trabajo

Tabla 3-3 describe el estado de los trabajos que se ejecutan después de iniciar sesión en la consola de gestión de MRS.

Tabla 3-3 Estado del trabajo

Estado	Descripción
Accepted	Estado inicial de un trabajo después de que se haya enviado correctamente.
Running	Se está ejecutando un trabajo.
Completed	Un trabajo ha sido ejecutado y completado con éxito.
Terminated	Un trabajo se detiene durante la ejecución.
Abnormal	Se produce un error durante la ejecución del trabajo o la ejecución del trabajo falla.

3.2.2 Comprobación del estado del clúster

La lista de clústeres contiene todos los clústeres en MRS. Puede ver clústeres en varios estados. Si hay un gran número de clústeres involucrados, navegue por varias páginas para ver todos los clústeres.

MRS, como plataforma de gestión y análisis de datos masivos, proporciona una capacidad de procesamiento de datos a nivel PB. MRS le permite múltiples clústeres. La cantidad de clústeres está sujeta a la de los ECS.

Los clústeres se enumeran en orden cronológico de forma predeterminada en la lista de clústeres, con el clúster más reciente mostrado en la parte superior. **Tabla 3-4** describe los parámetros de la lista de clústeres.

- **Active Clusters**: contiene todos los clústeres excepto los de los estados **Failed** y **Terminated** .
- **Cluster History**: contiene las tareas en los estados **Terminated**. Solo se muestran los clústeres terminados en los últimos seis meses. Si desea ver los clústeres finalizados hace seis meses, póngase en contacto con el soporte técnico de Huawei Cloud.
- **Failed Tasks**: solo contiene las tareas en el estado **Failed**. Los errores de tareas incluyen:
  - Error de creación de clúster
  - Falla de terminación del clúster
  - Falla de escalamiento horizontal de clústeres
  - Falla de escalamiento vertical de clústeres
  - Error en la instalación de parches de clúster (soportado solo por versiones anteriores a MRS 3.x)
  - Error de desinstalación de parches de clúster (soportado solo por versiones anteriores a MRS 3.x)
  - Error en la actualización de las especificaciones del clúster
  - Falla de aislamiento de nodos
  - Falla de desolación del nodo
  - Falla de desmantelamiento de nodos
  - Falla en la puesta en marcha del nodo

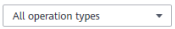
Tabla 3-4 Parámetros en la lista de clústeres activos

Parámetro	Descripción
Name/ID	Nombre del clúster, que se establece cuando se crea un clúster. Identificador único de un clúster, que se asigna automáticamente cuando se crea un clúster. ● : Cambiar el nombre del clúster. ● : Copiar el ID del clúster.
Cluster Version	Versión del clúster.
Cluster Type	El tipo del clúster que se va a crear.
Nodes	Número de nodos que se pueden desplegar en un clúster. Este parámetro se establece cuando se crea un clúster.
Status	Descripción del estado y el progreso de la operación de un clúster. El progreso de creación de clústeres incluye: ● Verificación de los parámetros del clúster ● Aplicación de recursos de clúster ● Creación de máquinas virtuales ● Inicialización de máquinas virtuales ● Instalación de MRS Manager ● Despliegue del clúster ● Error en la instalación del clúster El progreso de ampliación de los grupos incluye: ● Preparación para el escalado horizontal ● Creación de máquinas virtuales ● Inicialización de máquinas virtuales ● Adición de nodos al clúster ● Error de escalamiento horizontal El progreso de la reducción del clúster incluye: ● Preparación para el escalamiento vertical ● Instancia de desmantelamiento ● Eliminación de máquinas virtuales ● Eliminación de nodos del clúster ● Error de escalamiento vertical El sistema mostrará las causas de las fallas de instalación, expansión horizontal y reducción horizontal en clústeres. Para obtener más información, consulte **Tabla 2-6**.

Parámetro	Descripción
Modo de facturación	Actualmente, la versión comercial de MRS se cobra en función de los ECS en un clúster. ● **Yearly/Monthly**: La duración varía de un mes a un año. La duración mínima del clúster es de 1 mes y la duración máxima disponible del clúster es de 1 año. ● **Pay-per-use**: Los nodos se cobran por la duración real del uso, con un ciclo de facturación de una hora. La hora en la que el nodo del clúster se ha creado correctamente, es decir, la hora de inicio de facturación, se muestra en **Billing Mode**.
Created	La hora en que se crea correctamente un nodo de clúster.
Terminated	Hora en que se detiene la facturación de un nodo de clúster y comienza a finalizar el nodo de clúster. Este parámetro sólo es válido para clústeres históricos mostrados en la página **Cluster History**.
AZ	Zona de disponibilidad (AZ) en la región de un clúster, que se establece cuando se crea un clúster.
Enterprise Project	Proyecto de empresa al que pertenece un clúster.
Operation	**Terminate**: Si desea terminar un clúster después de que se completen los trabajos, haga clic en **Terminate**. El estado del clúster cambia de **Running** a **Terminating**. Una vez finalizado el clúster, el estado del clúster cambiará a **Terminated** y se mostrará en el archivo **Cluster History**. Si el clúster MRS no se despliega, el clúster se termina automáticamente. Este parámetro solo se muestra en **Active Clusters**. **NOTA** Por lo general, después de analizar y almacenar los datos, o cuando el clúster encuentra una excepción y no puede funcionar, puede terminar un clúster. Si se termina un clúster antes de que se complete el procesamiento y el análisis de datos, puede producirse una pérdida de datos. Por lo tanto, tenga cuidado al terminar un clúster.

Tabla 3-5 Descripción de botones

Botón	Descripción
	Seleccione un proyecto de empresa en la lista desplegable para filtrar el clúster correspondiente.

Botón	Descripción
	En la lista desplegable, seleccione un estado para filtrar los clústeres: ● Clústeres activos – Todos los tipos de operación: muestra todos los clústeres existentes. – Starting: muestra los clústeres existentes en el estado **Starting**. – Running: muestra los clústeres existentes en el estado **Running**. – Scaling out: muestra los clústeres existentes en el estado **Scaling out**. – Scaling in: muestra los clústeres existentes en el estado **Scaling in**. – Abnormal: muestra los clústeres existentes en el estado **Abnormal**. – Terminating: muestra los clústeres existentes en el estado **Terminating**. – Frozen: muestra los clústeres existentes en el estado **Frozen**.
	Elija **Clusters > Active Clusters** y haga clic en  para ir a la página de gestión de tareas fallidas.  *Num*: muestra las tareas fallidas en el estado **failed**.
	Escriba un nombre de clúster en la barra de búsqueda y haga clic en  para buscar un clúster.
Search by Tag	Haga clic en **Search by Tag**, introduzca la etiqueta del clúster que desea consultar y haga clic en **Search**. Puede seleccionar una clave de etiqueta o un valor de etiqueta de sus listas desplegables. Cuando la clave de etiqueta o el valor de etiqueta coinciden exactamente, el sistema puede localizar automáticamente el clúster de destino. Si introduce varias etiquetas, sus intersecciones se utilizan para buscar el clúster.
	Haga clic en  para actualizar manualmente la lista de clústeres.

3.2.3 Consulta de información básica del clúster

Puede monitorear y gestionar los clústeres que ha creado. Elija **Clusters > Active Clusters**. Seleccione un clúster y haga clic en su nombre para ir a la página de detalles del clúster. En la página mostrada, vea la configuración básica y la información de nodo del clúster.

NOTA

En la consola de MRS, las operaciones realizadas en un clúster de ECS son básicamente las mismas que las realizadas en un clúster de BMS. Este documento describe las operaciones en un clúster de ECS. Si las operaciones en los dos grupos difieren, las operaciones se describirán por separado.

En la página de detalles del clúster, haga clic en **Dashboard**. **Tabla 3-6**, **Tabla 3-7**, **Tabla 3-8** y **Tabla 3-9** describen los parámetros en la página de pestaña **Dashboard**.

Tabla 3-6 Información básica

Parámetro	Descripción
Cluster Name	El nombre de un clúster. Configure este parámetro al crear un clúster. Haga clic en para cambiar el nombre del clúster. Para las versiones anteriores a MRS 3.x, solo se cambia el nombre del clúster que se muestra en la consola de gestión de MRS, mientras que el nombre del clúster en MRS Manager no se cambia de forma sincrónica.
Cluster Status	El estado del clúster. Para obtener más información, consulte **Tabla 3-2**.
Cluster Version	Información sobre la versión de MRS.
Cluster Type	Hay tres tipos de clústeres: ● **Analysis cluster**: se utiliza para el análisis de datos fuera de línea y proporciona componentes de Hadoop. ● **Streaming cluster**: se utiliza para tareas de streaming y proporciona componentes de procesamiento de stream. ● **Hybrid cluster** se utiliza tanto para el análisis de datos fuera de línea como para el procesamiento de streaming y proporciona componentes Hadoop y componentes de procesamiento de streaming. ● **Custom**: Un clúster de MRS con todos los componentes personalizados. MRS 3.*x* o posterior soporta este tipo.
Cluster ID	Identificador único de un clúster, que se asigna automáticamente cuando se crea un clúster.
Created	Hora en la que se crea un clúster.
AZ	Zona de disponibilidad (AZ) en la región de un clúster, que se establece cuando se crea un clúster.
Kerberos Authentication	Si se debe habilitar la autenticación Kerberos al iniciar sesión en Manager.
Enterprise Project	El proyecto de empresa al que pertenece un clúster. Sólo en la página **Active Clusters** puede hacer clic en el nombre de un proyecto de empresa para ir a su página **Proyecto empresarial Management**.

Tabla 3-7 Información de la red

Parámetro	Descripción
Default Subnet	Subred seleccionada durante la creación del clúster. Si las direcciones IP de la subred son insuficientes, haga clic en **Change Subnet** para cambiar a otra subred en la misma VPC del clúster actual para obtener más direcciones IP de la subred disponibles. El cambio de una subred no afecta a las direcciones IP y subredes de los nodos existentes. Una subred proporciona recursos de red dedicados que están aislados de otras redes, lo cual mejora la seguridad de la red.
VPC	VPC seleccionada durante la creación del clúster. Una VPC es un entorno de red seguro, aislado y lógico.
EIP	Después de vincular una EIP a un clúster MRS, puede utilizar la EIP para acceder a la interfaz de usuario web de Manager del clúster.
Security Group	Nombre del grupo de seguridad del clúster.

Tabla 3-8 Gestión de O&M

Parámetro	Descripción
MRS Manager	Portal para la página de Manager. ● Para MRS 3.*x* o posterior, consulte **Acceder a FusionInsight Manager (MRS 3.x o posterior)**. ● Para las versiones anterior a MRS 3.x, debe vincular una EIP y agregar una regla de grupo de seguridad como se le solicite antes de acceder a la página MRS Manager. Para obtener más información, consulte **Acceso a MRS Manager (MRS 2.x o anterior)**.
IAM User Sync	La información del usuario de IAM se puede sincronizar con un clúster de MRS para la gestión del clúster. Para más detalles, consulte **Sincronización de usuarios de IAM a MRS**. **NOTA** Las páginas de pestaña **Components**, **Tenants** y **Backups & Restorations** de la página de detalles del clúster sólo se pueden utilizar después de sincronizar a los usuarios. Una vez sincronizados los clústeres de MRS 3.x, puede utilizar la función **Component Management**.
Data Connection	Haga clic en **Manage** para ver el tipo de conexión de datos asociado al clúster. Para obtener más información, consulte **Configuración de conexiones de datos**.

Parámetro	Descripción
Agency	Haga clic en **Manage Agency** para enlazar o modificar una delegación para el clúster. Una delegación permite al ECS o al BMS gestionar recursos del MRS. Puede configurar una delegación del tipo ECS para obtener automáticamente el AK/SK para acceder a OBS. La delegación **MRS_ECS_DEFAULT_AGENCY** tiene el permiso OBS OperateAccess de OBS y el FullAccess de CES (para usuarios que han habilitado políticas detalladas), permisos de administrador de CES y de administrador de KMS en la región donde se encuentra el clúster.
OBS Permission Control	Haga clic en **Manage** y modifique la asignación entre los usuarios MRS y los permisos OBS.
Logging	Se utiliza para recopilar registros sobre la creación de clústeres y los errores de escalamiento.
Secure Communications	Se utiliza para mostrar el estado de autorización de seguridad. Puede hacer clic en  para habilitar o deshabilitar la autorización de seguridad. La desactivación de la autorización de seguridad conlleva un alto riesgo. Tenga cuidado al realizar esta operación. Para obtener más información, consulte **Autorización de seguridad de comunicación**.

Tabla 3-9 Información de facturación

Parámetro	Descripción
Billing Mode	Modo de facturación de un clúster. Actualmente, son compatibles con **Pay-per-use** y **Yearly/Monthly**.
Auto-renewal	Si se debe habilitar la función de renovación automática para un clúster anual/mensual.
Order ID	ID de pedido para comprar el clúster. Este parámetro sólo está disponible cuando **Billing Mode** está establecido en **Yearly/Monthly**.

En la página de detalles del clúster, haga clic en **Nodes**. Para obtener más información sobre los parámetros del nodo, consulte **Tabla 3-10**.

Tabla 3-10 Información del nodo

Parámetro	Descripción
Configure Task Node	Se utiliza para agregar un nodo de Task. Para obtener más información, consulte **Adición de un nodo de Task**. Para las versiones 3.x y posteriores, esta operación solo se aplica al clúster de análisis, al clúster de streaming y al clúster híbrido.
Add Node Group	Este parámetro solo se aplica a las versiones 3.x y posteriores. Solo se aplica a clústeres personalizados y se utiliza para agregar grupos de nodos. Para obtener más información, consulte **Adición de un grupo de nodos**.
Node Group	Nombre del grupo de nodos.
Node Type	Tipo de nodo: ● **Master**: Un nodo de Master de un clúster de MRS gestiona el clúster, asigna archivos ejecutables de MapReduce a los nodos de Core, rastrea el estado de ejecución de cada trabajo y monitorea el estado de ejecución del DataNode. ● Un grupo de nodos de tarea es un grupo de nodos en el que solo se despliegan funciones de datos que no almacenan datos. Las funciones incluyen NodeManager, ThriftServer, Thrift1Server, RESTServer, Supervisor, LogViewer, HBaseIndexer, and TagSync. ● Si se despliegan otros roles en el grupo de nodos además de los roles anteriores, el grupo de nodos es el grupo de nodos de Core. En la página de pestaña **Nodes**, haga clic en ⌄ junto al nombre de un grupo de nodos para desplegar los nodos contenidos en el grupo de nodos. Haga clic en un nombre de nodo para iniciar sesión de forma remota en el ECS mediante la contraseña o el par de claves configurado durante la creación del clúster. Para obtener más información sobre los parámetros, consulte **Gestión de componentes y monitoreo de hosts**.
Node Count	Número de nodos en un grupo de nodos.
Operation	● **Scale Up Specifications**: Para más información, consulte **Scaling Up Master Node Specifications**. ● **Scale Out**: Para más información, consulte **Escalamiento horizontal de un clúster**. ● **Scale In**: Para más información, consulte **Escalamiento vertical de un clúster**. ● **Auto Scaling**: Para más información, consulte **Configuración de reglas de escalado automático**. ● **View Roles**: Puede ver información sobre los roles desplegados en el grupo de nodos. Esta función solo se aplica a clústeres personalizados de 3.x y posteriores.

3.2.4 Consulta de información de parches de clúster

Para ver información de parches acerca de los componentes del clúster, puede descargar el parche necesario si el componente del clúster, como Hadoop o Spark, está defectuoso. En la consola de MRS, elija **Clusters > Active Clusters**, seleccione un clúster y haga clic en el nombre del clúster. En la página de detalles del clúster que se muestra, actualice el componente y rectifique el error.

NOTA

MRS 3.x no tiene información sobre la versión del parche. Por lo tanto, esta sección no está involucrada.

- Nombre del parche: nombre del paquete de parches
- Publicado: hora en que se libera el paquete de parches
- Estado: estado del parche
- Descripción del parche: descripción de la versión del parche
- Operación: instalación o desinstalación de parches

3.2.5 Gestión de componentes y monitoreo de hosts

Puede gestionar el siguiente estado y métricas de todos los componentes (incluidas las instancias de rol) y hosts en la consola de MRS:

- Información de estado: incluye el estado de operación, estado, configuración e instancia de rol.
- Información sobre indicadores: incluye indicadores clave de seguimiento para cada componente.
- Exportar métricas de monitoreo. (Esta función no se admite en MRS 3.x o posterior.)

NOTA

- Para versiones anteriores a MRS 3.x, consulte **Gestión de servicios y monitoreo de hosts**.
- Para MRS 3.x o posterior, consulte **Procedimiento**.
- Puede establecer el intervalo para actualizar automáticamente la página o hacer clic en  para actualizar la página inmediatamente.
- La gestión de componentes admite los siguientes valores de parámetros:
  - Refrescar cada 30 segundos
  - Refrescar cada 60 segundos
  - Dejar de actualizar

Prerrequisitos

Tiene usuarios de IAM sincronizados. (En la página **Dashboard**, haga clic en **Synchronize** en el lado derecho de **IAM User Sync** para sincronizar usuarios de IAM.)

Procedimiento

Gestionar componentes.

NOTA

Para obtener más información acerca de cómo realizar operaciones en MRS Manager, consulte **Gestión de monitoreo de servicios**.

Paso 1 En la página de detalles del clúster de MRS, haga clic en **Components**.

- Tabla 3-11 describe el estado de funcionamiento del servicio.

Tabla 3-11 Estado de funcionamiento del servicio

Estado	Descripción
Started	Se ha iniciado el servicio.
Stopped	El servicio está detenido.
Failed to start	Error al iniciar la instancia de rol.
Failed to stop	Error al detener el servicio.
Unknown	Indica el estado inicial del servicio después de reiniciar el sistema en segundo plano.

- Tabla 3-12 describe el estado del servicio.

Tabla 3-12 Estado de salud del servicio

Estado	Descripción
Good	Indica que todas las instancias de rol del servicio se están ejecutando correctamente.
Faulty	Indica que el estado de ejecución de al menos una instancia de rol es **Faulty** o que el estado del servicio del que depende el servicio actual es anormal.
Unknown	Indica que todas las instancias de rol del servicio están en estado **Unknown**.
Restoring	Indica que el sistema en segundo plano está reiniciando el servicio.
Partially Healthy	Indica que el estado del servicio del que depende es anormal y que los sistemas externos no pueden invocar las API relacionadas con el servicio anormal.

- Tabla 3-13 describe el estado del servicio.

Tabla 3-13 Estado de la configuración del servicio

Estado	Descripción
Synchronized	La última configuración entra en vigor.

Estado	Descripción
Configuration expired	La última configuración no tiene efecto después de la modificación del parámetro. Los servicios relacionados deben reiniciarse.
Configuration failed	La comunicación es incorrecta o los datos no se pueden leer o escribir durante la configuración del parámetro. Utilice **Synchronize Configuration** para rectificar la falla.
Configuring	Los parámetros se están configurando.
Unknown	Indica que no se puede obtener el estado de configuración.

Paso 2 Haga clic en un servicio especificado en la lista para ver su estado y la información de métrica.

Paso 3 Personalizar y ver gráficos de monitoreo.

1. En el área **Charts**, haga clic en **Customize** para personalizar las métricas de monitoreo de servicios.
2. En el área **Period**, seleccione una hora del período y haga clic en **View** para ver los datos de supervisión dentro del período de tiempo.

----Fin

Gestionar instancias de rol.

NOTA

Para versiones anteriores a MRS 3.x, consulte **Gestión de instancias de rol**.

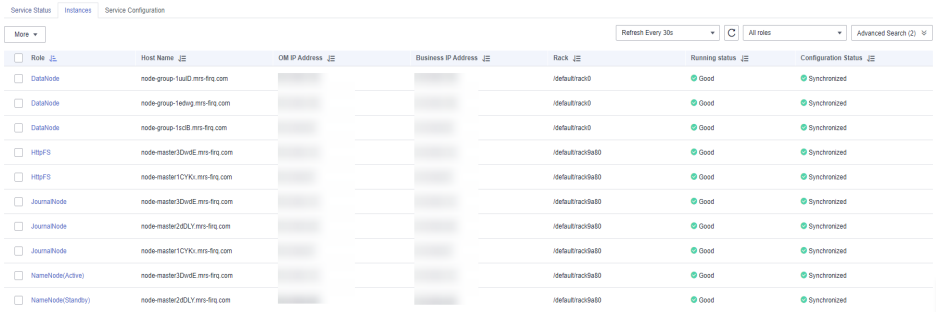
Paso 1 En la página de detalles del clúster de MRS, haga clic en **Components**. En la lista de componentes, haga clic en el nombre del servicio especificado.

Figura 3-4 Página de pestaña de componentes

Name	Version	Operating Status	Health Status	Configuration Status
Hadoop	3.1.1			
Spark2x	2.4.5	Started	Good	Synchronized
HBase	2.2.3	Started	Good	Synchronized
Hive	3.1.0	Started	Good	Synchronized
Hue	4.7.0	Started	Good	Synchronized
Kafka	2.11-2.4.0	Started	Good	Synchronized
Flume	1.9.0	Started	Good	Synchronized
Flink	1.12.0	Started	Good	Synchronized
Oozie	5.1.0	Started	Good	Synchronized
ZooKeeper	3.5.6	Started	Good	Synchronized

Paso 2 Haga clic en **Instances** para ver el estado del rol.

Figura 3-5 Página de pestaña de instancias



La lista de instancias de rol contiene el rol, el nombre de host, la dirección IP de gestión, la dirección IP de servicio, el rack, el estado de ejecución y el estado de configuración de cada instancia.

- Tabla 3-14 muestra el estado de ejecución de una instancia de rol.

  Tabla 3-14 Estado de ejecución de instancia de rol

Estado	Descripción
Good	Indica que la instancia se está ejecutando correctamente.
Bad	Indica que la instancia no se puede ejecutar correctamente.
Decommissioned	Indica que la instancia está fuera de servicio.
Not started	Indica que la instancia está detenida.
Unknown	Indica que no se puede detectar el estado inicial de la instancia.
Starting	Indica que se está iniciando la instancia.
Stopping	Indica que se está deteniendo la instancia.
Restoring	Indica que puede producirse una excepción en la instancia y que la instancia se está rectificando automáticamente.
Decommissioning	Indica que la instancia se está desmantelando.
Recommissioning	Indica que se está reiniciando la instancia.
Failed to start	Indica que no se puede iniciar el servicio.
Failed to stop	Indica que no se puede detener el servicio.

- Tabla 3-15 muestra el estado de configuración de una instancia de rol.

Tabla 3-15 Estado de configuración de instancia de rol

Estado	Descripción
Synchronized	La última configuración entra en vigor.
Configuration expired	La última configuración no tiene efecto después de la modificación del parámetro. Los servicios relacionados deben reiniciarse.
Configuration failed	La comunicación es incorrecta o los datos no se pueden leer o escribir durante la configuración del parámetro. Utilice **Synchronize Configuration** para rectificar la falla.
Configuring	Los parámetros se están configurando.
Unknown	No se puede obtener el estado de configuración actual.

De forma predeterminada, la columna **Role** está ordenada en orden ascendente. Puede hacer clic en el icono de ordenación situado junto a **Role**, **Host Name**, **OM IP Address**, **Business IP Address**, **Rack**, **Running Status** o **Configuration Status** para cambiar el modo de ordenación.

Puede filtrar todas las instancias del mismo rol en la columna **Role**.

Para establecer criterios de búsqueda en el área de búsqueda de roles, haga clic en **Advanced Search** y haga clic en **Search** para ver la información de roles especificada. Puede hacer clic en **Reset** para restablecer los criterios de búsqueda. Se soporta la búsqueda difusa.

Paso 3 Haga clic en la instancia de rol de destino para ver su estado y la información de métrica.

Paso 4 Personalizar y ver gráficos de monitoreo.

1. En el área **Charts**, haga clic en **Customize** para personalizar las métricas de monitoreo de servicios.
2. En el área **Period**, seleccione una hora del período y haga clic en **View** para ver los datos de supervisión dentro del período de tiempo.

----Fin

Gestionar hosts.

NOTA

Para versiones anteriores a MRS 3.x, consulte **Gestión de hosts**.

Paso 1 En la página de detalles del clúster de MRS, haga clic en la pestaña **Nodes** y expanda un grupo de nodos para ver el estado del host.

La lista de hosts contiene **Node Name**, **IP Address**, **Rack**, **Operating Status**, **Health Status**, **CPU Usage**, **Memory Usage**, **Disk Usage**, **Network Speed**, Specification Name, **Specifications Billing Type**, y **AZ**.

- **Tabla 3-16** muestra el estado operativo del host.

Tabla 3-16 Estado de funcionamiento del host

Estado	Descripción
Normal	Los roles de host y servicio en el host se están ejecutando correctamente.
Isolated	El host está aislado y los roles de servicio en el host dejan de ejecutarse.

- **Tabla 3-17** describe el estado de salud del host.

Tabla 3-17 Estado del estado del host

Estado	Descripción
Good	El host puede enviar correctamente los latidos del corazón.
Bad	El host no puede enviar los latidos debido al tiempo de espera.
Unknown	El estado inicial del host es desconocido durante la operación de agregar o eliminar un host.

Los nodos se ordenan en orden ascendente de forma predeterminada. Puede hacer clic en **Node Name**, **IP Address**, **Rack**, **Operating Status**, **Health Status**, **CPU Usage**, **Memory Usage**, **Disk Usage**, **Network Speed**, **Specification Name** o **Specifications** para cambiar el modo de ordenación.

Paso 2 Haga clic en el nodo de destino de la lista para ver su estado y la información de métrica.

----Fin

3.3 Consulta y personalización de métricas de monitoreo de clústeres

Los nodos de clúster de MRS se clasifican en nodos de gestión, nodos de control y nodos de datos. Las tendencias de cambio de las métricas clave de monitoreo de host en cada tipo de nodo se pueden calcular y mostrar como gráficos de curvas en informes basados en los períodos personalizados. Si un host pertenece a varios tipos de nodo, las estadísticas de métricas se recopilarán repetidamente.

Esta sección proporciona una visión general de los clústeres de MRS y describe cómo ver, personalizar y exportar métricas de monitoreo de nodos en MRS Manager.

NOTA

Las métricas de clúster se monitorizan periódicamente. El intervalo de monitorización histórico promedio es de aproximadamente 5 minutos.

- Escenario 1: **applicable a clústeres anteriores a MRS 3.*x***
  - Método 1:

i. Elija **Clusters** > **Active Clusters** y haga clic en un nombre de clúster para acceder a su página de detalles.

ii. Haga clic en la pestaña **Dashboard**, puede ver las estadísticas de estado del host del clúster en la parte inferior de la página de pestaña mostrada.

iii. Para ver o exportar un informe de otras métricas, inicie sesión en Manager haciendo referencia a **Acceder a Manager**.

iv. En la página de Manager, vea, personalice y exporte el informe de métrica de monitoreo de nodos haciendo referencia a **Panel**.

– Método 2:

i. Inicie sesión en la consola de MRS.

ii. Elija **Clusters** > **Active Clusters** y haga clic en un nombre de clúster para acceder a su página de detalles.

iii. En la página de pestaña **Dashboard**, haga clic en **Click to synchronize** junto a **IAM User Sync** para sincronizar los usuarios de IAM.

iv. Una vez completada la sincronización, haga clic en la pestaña **Monitor** para ver el informe de métricas de monitoreo del clúster.

v. En el área de intervalo de tiempo, especifique un período para ver los datos de monitoreo. Las opciones son las siguientes:

- Última hora
- Últimas 3 horas
- Últimas 12 horas
- Últimas 24 horas
- Últimos 7 días
- Últimos 30 días
- Personalizar: Puede personalizar el período para ver los datos de monitoreo.

vi. Personalizar un informe de métricas de monitoreo.

1) Haga clic en **Customize** y seleccione las métricas de monitoreo que desea mostrar.

2) Haga clic en **OK** para guardar las métricas de monitoreo seleccionadas para mostrarlas.

NOTA

Haga clic en **Clear** para cancelar todas las métricas de monitoreo seleccionadas en un lote.

vii. Exportar un informe de monitoreo.

1) Seleccione un período.

Las opciones son las siguientes:

Last 1 hour, **Last 3 hours**, **Last 12 hours**, **Last 24 hours**, **Recent 7 days**, **Recent 30 days** o **Customize** (selección de un intervalo de tiempo)

2) Haga clic en **Export**. MRS generará un informe sobre las métricas de monitoreo seleccionadas en un intervalo de tiempo especificado. Guarde el informe.

- **Escenario 2 (aplicable a clústeres MRS 3.*x* o posteriores)**

a. Inicie sesión en la consola de MRS.
b. Elija **Clusters** > **Active Clusters** y haga clic en un nombre de clúster para acceder a su página de detalles.
c. En la página de pestaña **Dashboard**, haga clic en **Click to synchronize** junto a **IAM User Sync** para sincronizar los usuarios de IAM.
d. Una vez completada la sincronización, haga clic en la pestaña **Monitor** para ver el informe de métricas de monitoreo del clúster.
e. En el área de intervalo de tiempo, especifique un período para ver los datos de monitoreo. Las opciones son las siguientes:
   - Última hora
   - Últimas 3 horas
   - Últimas 12 horas
   - Últimas 24 horas
   - Últimos 7 días
   - Últimos 30 días
   - Personalizar: Puede personalizar el período para ver los datos de monitoreo.
f. Personalizar un informe de métricas de monitoreo.
   i. Haga clic en **Customize** y seleccione las métricas de monitoreo que se mostrarán.
   ii. Haga clic en **OK** para guardar las métricas de monitoreo seleccionadas para mostrarlas.

   NOTA

   Haga clic en **Clear** para cancelar todas las métricas de monitoreo seleccionadas en un lote.

3.4 O&M de clúster

3.4.1 Importación y exportación de datos

A través de la pestaña **Files**, puede crear, eliminar, importar, exportar, eliminar archivos en el clúster de análisis. Actualmente, no se admite la creación de archivos. Los clústeres de streaming no admiten la función de gestión de archivos en la GUI de MRS. En un clúster con autenticación de Kerberos habilitada, para leer o escribir las carpetas en el directorio raíz, agregue un rol que tenga los permisos necesarios en las carpetas haciendo referencia a **Creación de un rol**. A continuación, agregue el nuevo rol al grupo de usuarios al que pertenece el usuario que envía el trabajo haciendo referencia a **Tareas relacionadas**.

Antecedentes

Las fuentes de datos procesadas por MRS son de OBS o HDFS. OBS es un servicio de almacenamiento basado en objetos que le proporciona capacidades de almacenamiento de datos masivas, seguras, confiables y rentables. MRS puede procesar datos en OBS directamente. Puede ver, gestionar y usar datos utilizando la página web de la plataforma de control de gestión o el cliente de OBS. Además, puede utilizar las API de REST de forma independiente o integrar las API en aplicaciones de servicio para gestionar y acceder a los datos.

Antes de crear trabajos, cargue los datos locales en OBS para que MRS calcule y analice. MRS permite exportar datos de OBS a HDFS para computación y análisis. Después de completar el análisis de datos y la computación, puede almacenar los datos en HDFS o exportarlos a OBS. HDFS y OBS también pueden almacenar los datos comprimidos en el formato **bz2** o **gz**.

Importación de datos

Actualmente, MRS solo puede importar datos de OBS a HDFS. La tasa de carga de archivos disminuye con el aumento del tamaño del archivo. Este modo se aplica a escenarios en los que el volumen de datos es pequeño.

Puede realizar los siguientes pasos para importar archivos y directorios:

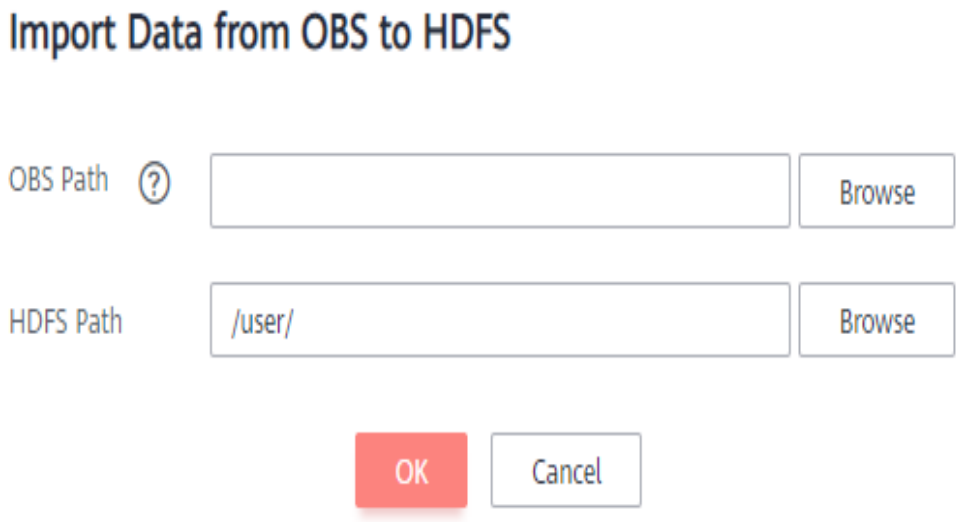
1. Inicie sesión en la consola de MRS.
2. Elija **Clusters > Active Clusters** y haga clic en el nombre del clúster que se va a consultar para entrar en la página que muestra la información del clúster.
3. Haga clic en la pestaña **Files**, y vaya a la página de gestión de archivos.
4. Seleccione **HDFS File List**.
5. Vaya al directorio de almacenamiento de datos, por ejemplo, **bd_app1**.

   El directorio **bd_app1** es solo un ejemplo. Puede utilizar cualquier directorio de la página o crear uno nuevo.

   Los requisitos para crear una carpeta son los siguientes:

   – El nombre de la carpeta contiene un máximo de 255 caracteres.
   – El nombre de la carpeta no puede estar vacío.
   – El nombre de la carpeta no puede contener las siguientes characters especiales: /:*?"<>|\;&,'`!{}[]$%+
   – El valor no puede comenzar ni finalizar con un período (.).
   – Los espacios al principio y al final se ignoran.
6. Haga clic en **Import Data** y configure las rutas de HDFS y OBS correctamente. Cuando configure la ruta de acceso OBS o HDFS, haga clic en **Browse**, seleccione un directorio de archivo y haga clic en **Yes**.

Figura 3-6 Importación de datos



- Ruta de OBS
  - El camino debe comenzar con **obs://**.
  - Los archivos o programas cifrados por KMS no se pueden importar.
  - No se puede importar una carpeta vacía.
  - El directorio y el nombre del archivo pueden contener letras, dígitos, guiones (-) y guiones bajos (_), pero no pueden contener los siguientes caracteres especiales ;|&>,<'$*?\
  - El directorio y el nombre de archivo no pueden comenzar o terminar con un espacio, pero pueden contener espacios entre ellos.
  - La ruta de acceso completa de OBS contiene un máximo de 255 caracteres.
- Ruta de HDFS
  - La ruta comienza por **/user** de forma predeterminada.
  - El directorio y el nombre del archivo pueden contener letras, dígitos, guiones (-) y guiones bajos (_), pero no pueden contener los siguientes caracteres especiales: ;|&>,<'$*?\:
  - El directorio y el nombre de archivo no pueden comenzar o terminar con un espacio, pero pueden contener espacios entre ellos.
  - La ruta de acceso completa de HDFS contiene un máximo de 255 caracteres.

7. Haga clic en **OK**.

   Puede ver el progreso de la carga de archivos en la pestaña **File Operation Records**. MRS procesa la operación de importación de datos como un trabajo de DistCp. También puede comprobar si el trabajo DistCp se ejecuta correctamente en la página de pestaña **Jobs**.

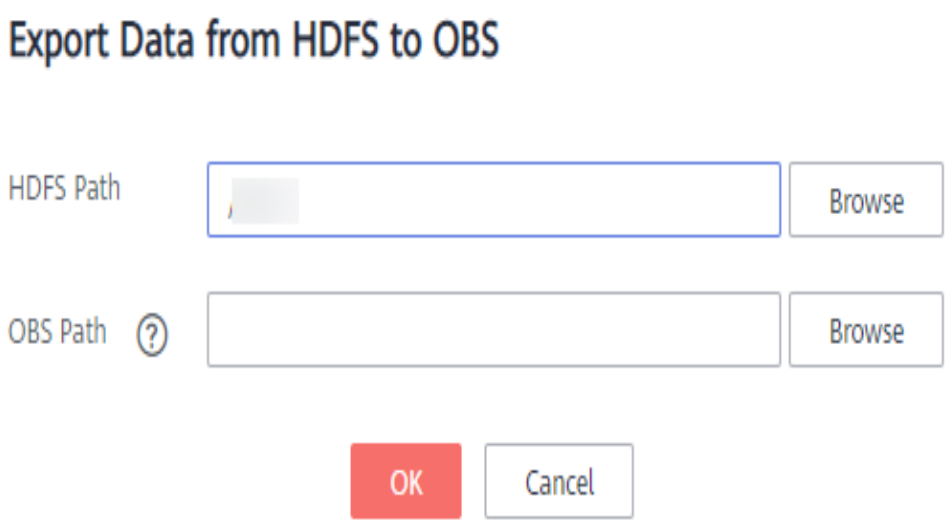
Exportación de datos

Después de completar el análisis de datos y la computación, puede almacenar los datos en HDFS o exportarlos a OBS.

Puede realizar los siguientes pasos para exportar archivos y directorios:

1. Inicie sesión en la consola de MRS.
2. Elija **Clusters > Active Clusters** y haga clic en el nombre del clúster que se va a consultar para entrar en la página que muestra la información básica del clúster.
3. Haga clic en la pestaña **Files** y aparecerá la página de gestión de archivos.
4. Seleccione **HDFS File List**.
5. Vaya al directorio de almacenamiento de datos, por ejemplo, **bd_app1**.
6. Haga clic en **Export Data** y configure las rutas OBS y HDFS. Cuando configure la ruta de acceso OBS o HDFS, haga clic en **Browse**, seleccione un directorio de archivo y haga clic en **Yes**.

Figura 3-7 Exportación de datos



- Ruta de OBS
  - El camino debe comenzar con **obs:**//.
  - El directorio y el nombre del archivo pueden contener letras, dígitos, guiones (-) y guiones bajos (_), pero no pueden contener los siguientes caracteres especiales: ;|&>,<'$*?\
  - El directorio y el nombre de archivo no pueden comenzar o terminar con un espacio, pero pueden contener espacios entre ellos.
  - La ruta de acceso completa de OBS contiene un máximo de 255 caracteres.
- Ruta de HDFS
  - La ruta comienza por **/user** de forma predeterminada.
  - El directorio y el nombre del archivo pueden contener letras, dígitos, guiones (-) y guiones bajos (_), pero no pueden contener los siguientes caracteres especiales: ;|&>,<'$*?\:
  - El directorio y el nombre de archivo no pueden comenzar o terminar con un espacio, pero pueden contener espacios entre ellos.
  - La ruta de acceso completa de HDFS contiene un máximo de 255 caracteres.

> NOTA
>
> Cuando se exporta una carpeta a OBS, se agrega un archivo de etiquetas denominado **folder name_$folder$** a la ruta de acceso de OBS. Asegúrese de que la carpeta exportada no está vacía. Si la carpeta exportada está vacía, OBS no puede mostrarla y solo genera un archivo denominado **folder name_$folder$**.

7. Haga clic en **OK**.

   Puede ver el progreso de la carga de archivos en la pestaña **File Operation Records**. MRS procesa la operación de exportación de datos como un trabajo DistCp. También puede comprobar si el trabajo DistCp se ejecuta correctamente en la página de pestaña **Jobs**.

Visualización de registros de operación

Al importar y exportar datos en la consola de gestión de MRS, puede elegir **Files > File Operation Records** para ver el progreso de importación y exportación de datos.

Tabla 3-18 describe los parámetros del registro de operación del archivo.

Tabla 3-18 Parámetros de registro de operación de archivo

Parámetro	Descripción
Submitted	Hora de inicio de la importación o exportación de datos.
Source Path	Ruta de origen de los datos. ● Ruta OBS durante la importación de datos. ● Ruta HDFS durante la exportación de datos.
Target Path	Ruta de destino de los datos. ● Ruta de acceso HDFS durante la importación de datos. ● Ruta OBS durante la importación de datos.
Status	Estado durante la importación o exportación de datos. ● Submitted ● Accepted ● Running ● Completed ● Terminated ● Abnormal
Duration (min)	Tiempo de importación o exportación de datos. La unidad es un minuto.
Result	Resultado de la importación o exportación de datos. ● Successful ● Failed ● Killed ● Undefined

Parámetro	Descripción
Operation	Ver registro: le permite ver los registros de operaciones de archivos.

3.4.2 Cambio de la subred de un clúster

Si la subred actual no tiene suficientes direcciones IP, puede cambiar a otra subred en la misma VPC del clúster actual para obtener más direcciones IP de subred disponibles. El cambio de una subred no afecta a las direcciones IP ni a las subredes de los nodos existentes.

Para obtener detalles acerca de cómo configurar reglas de salida de ACL de red, vea **¿Cómo configuro una regla de salida de ACL de red?**

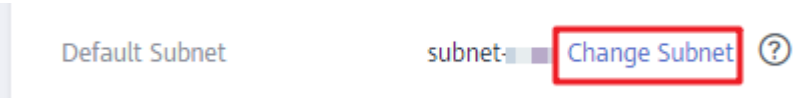
Cambio de una subred cuando no hay ACL de red asociada

Paso 1 Inicie sesión en la consola de MRS.

Paso 2 Haga clic en el nombre del clúster de destino para ir a su página de detalles.

Paso 3 Haga clic en **Change Subnet** a la derecha de **Default Subnet**.

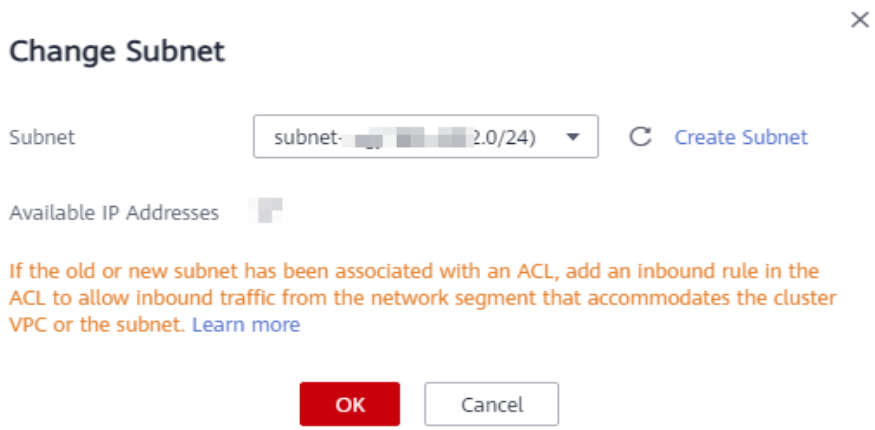
Figura 3-8 Cambio de una subred



Paso 4 Seleccione la subred de destino y haga clic en **OK**.

Si no hay ninguna subred disponible, haga clic en **Create Subnet** para crear una subred primero.

Figura 3-9 Selección de la subred de destino



----Fin

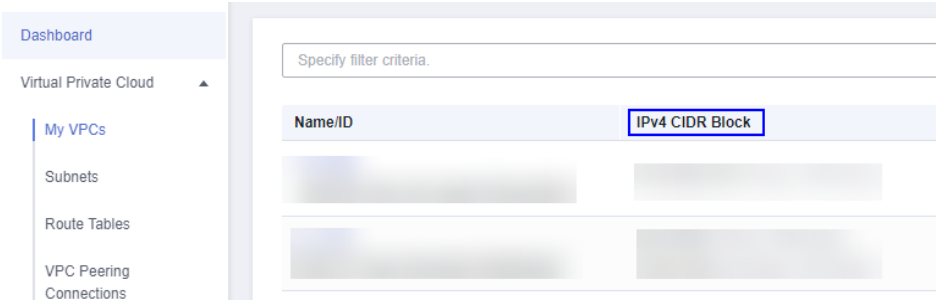
Cambio de una subred cuando se asocia una ACL de red

Paso 1 Inicie sesión en la consola MRS y haga clic en el clúster de destino para ir a su página de detalles.

Paso 2 En el área **Basic Information**, vea **VPC**.

Paso 3 Inicie sesión en la consola de VPC. En el panel de navegación de la izquierda, elija **Virtual Private Cloud** y obtenga el bloque CIDR IPv4 correspondiente a la VPC obtenida en **Paso 2**.

Figura 3-10 Obtención del bloque CIDR de IPv4

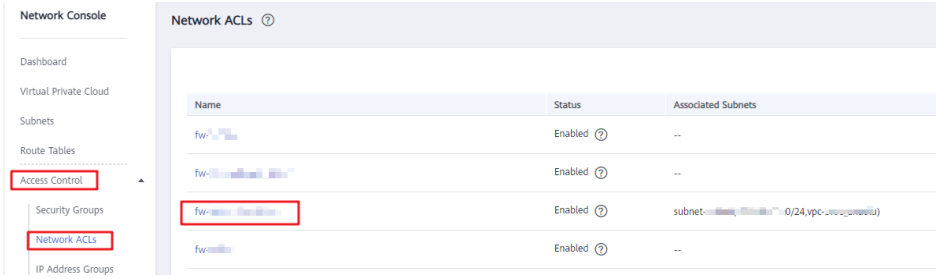


Paso 4 Elija **Access Control** > **Network ACLs** y haga clic en el nombre de la ACL de red asociada a las subredes predeterminadas y nuevas.

NOTA

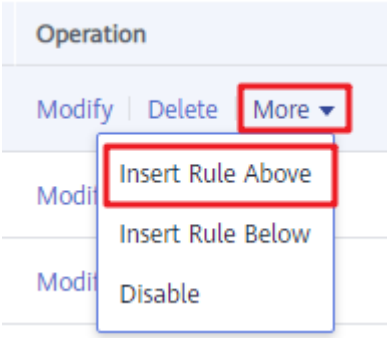
Si tanto las subredes predeterminadas como las nuevas están asociadas con una ACL de red, agregue reglas entrantes a la ACL de red haciendo referencia a **Paso 5** a **Paso 7**.

Figura 3-11 ACL de red



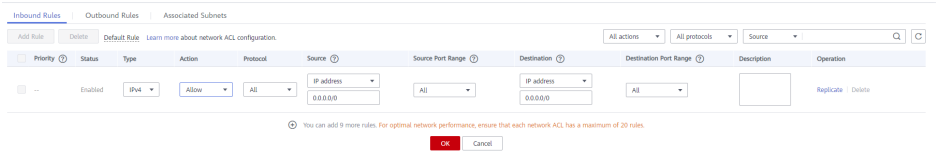
Paso 5 En la página **Inbound Rules**, elija **More** > **Insert Rule Above** en la columna **Operation**.

Figura 3-12 Inserción de regla arriba



Paso 6 Agregue una regla de ACL de red. Establezca **Action** en **Allow**, **Source** en el bloque CIDR de IPv4 de VPC obtenido en **Paso 3** y conserve los valores predeterminados para otros parámetros.

Figura 3-13 Adición de una regla de ACL de red



Paso 7 Haga clic en **OK**.

NOTA

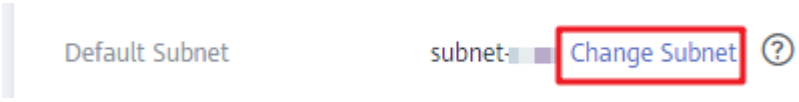
Si no desea permitir el acceso desde todos los bloques CIDR IPv4 de la VPC, agregue los bloques CIDR IPv4 de las subredes predeterminada y nueva realizando **Paso 8** a **Paso 12**. Si se han agregado las reglas para los bloques CIDR de IPv4 de VPC, omita **Paso 8** a **Paso 12**.

Paso 8 Inicie sesión en la consola de MRS.

Paso 9 Haga clic en el clúster de destino para ir a su página de detalles.

Paso 10 Haga clic en **Change Subnet** a la derecha de **Default Subnet**.

Figura 3-14 Cambio de una subred

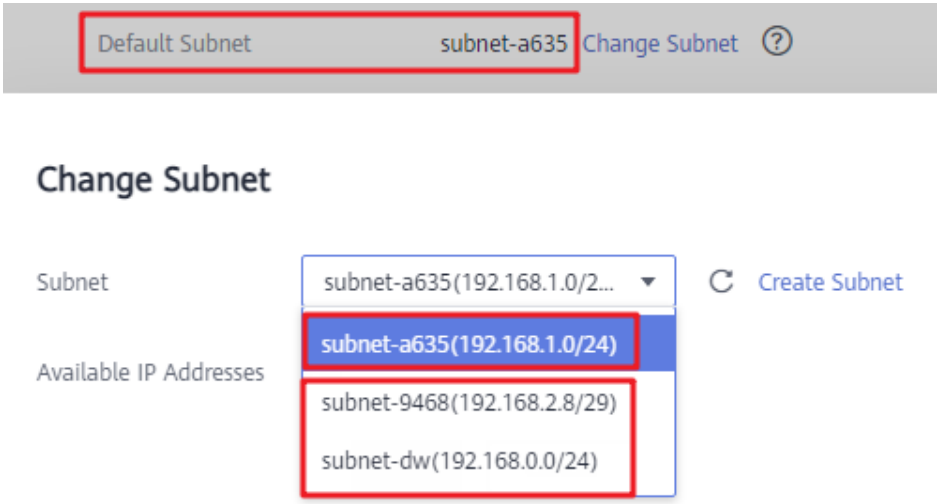


Paso 11 Obtenga los bloques CIDR IPv4 de las subredes predeterminadas y nuevas.

AVISO

En este caso, no es necesario hacer clic en **OK** que se muestra en el cuadro de diálogo **Change Subnet**. De lo contrario, la subred predeterminada se actualizará a la nueva subred, lo que dificultará la consulta del bloque CIDR IPv4 de la subred predeterminada. Tenga cuidado al realizar esta operación.

Figura 3-15 Obtención de la dirección IP de subred



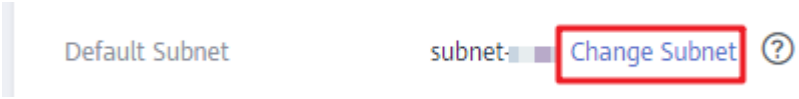
Paso 12 Agregue los bloques CIDR IPv4 de las subredes predeterminadas y de destino a las reglas entrantes de la ACL de red vinculada a las dos subredes haciendo referencia a **Paso 4** a **Paso 7**.

Paso 13 Inicie sesión en la consola de MRS.

Paso 14 Haga clic en el clúster de destino para ir a su página de detalles.

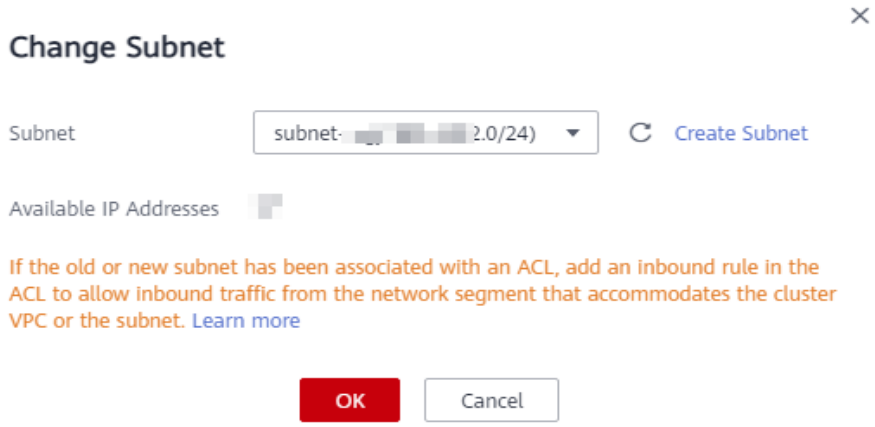
Paso 15 Haga clic en **Change Subnet** a la derecha de **Default Subnet**.

Figura 3-16 Cambio de una subred



Paso 16 Seleccione la subred de destino y haga clic en **OK**.

Figura 3-17 Selección de la subred de destino



----Fin

¿Cómo configuro una regla de salida de ACL de red?

- Método 1

  Permitir todo el tráfico saliente. Este método garantiza que los clústeres se pueden crear y utilizar correctamente.

  Figura 3-18 Permitir todo el tráfico saliente

Status	Type	Action	Protocol	Source	Source Port Range	Destination	Destination Port Range
Enabled	IPv4	Allow	All	0.0.0.0/0	All	0.0.0.0/0	All

- Método 2

  Permitir las reglas salientes obligatorias que pueden garantizar la creación exitosa de clústeres. No se recomienda utilizar este método porque es posible que los clústeres creados no se ejecuten correctamente debido a la ausencia de reglas salientes. Si se produce el problema anterior, póngase en contacto con el personal de O&M.

  De forma similar al ejemplo proporcionado en el método 1, establezca **Action** en **Allow** y añada las reglas salientes cuyos destinos sean la dirección con **Secure Communications** habilitadas, la dirección del servidor NTP, la dirección del servidor OBS, la dirección de OpenStack y la dirección del servidor DNS, respectivamente.

3.4.3 Configuración de la notificación de mensaje

MRS utiliza SMN para ofrecer un modelo de publicación/suscripción para lograr suscripciones y notificaciones de uno a varios mensajes en una variedad de tipos de mensajes (SMS y correos electrónicos).

Escenario

En la consola de gestión de MRS, puede habilitar o deshabilitar el servicio de notificación en la página **Alarms**. Las funciones en los siguientes escenarios solo se pueden implementar después de que se habilite la función de clúster requerida:

- Después de que un usuario se suscriba al servicio de notificación, el plano de gestión de MRS notifica al usuario el éxito o el fracaso de expansión horizontal y reducción horizontal de clústeres manuales, la terminación de clústeres y el escalamiento automático mediante correos electrónicos o mensajes SMS.
- El plano de gestión comprueba las alarmas sobre el grupo de MRS y envía una notificación al tenant si las alarmas son críticas.
- Si cualquiera de las operaciones tales como eliminación, apagado, modificación de especificaciones, reinicio y actualización del sistema operativo se realiza en un ECS en un clúster, el clúster de MRS funciona de forma anormal. El plano de gestión notifica a un usuario cuando detecta que la VM del usuario está en cualquiera de las operaciones anteriores.

Creación de un tema

Un tema es un evento especificado para la publicación de mensajes y la suscripción de notificaciones. Funciona como un canal de envío de mensajes, en el que los suscriptores y editores pueden interactuar entre ellos.

1. Inicie sesión en la consola de gestión.

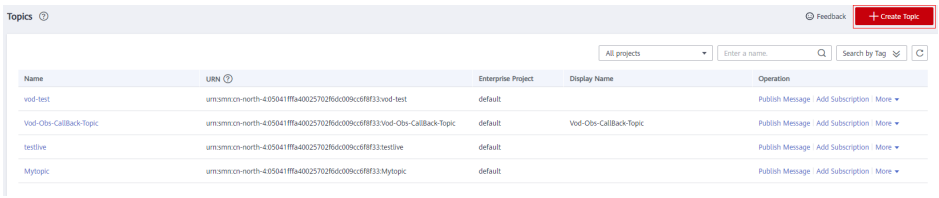
2. Haga clic en **Service List**. En **Management & Governance**, haga clic en **Simple Message Notification**.

   Se muestra la página **SMN**.

3. En el panel de navegación, elija **Topic Management** >**Topics**.

   Se muestra la página **Topics**.

4. Haga clic en **Create Topic**.



   Aparece el cuadro de diálogo **Create Topic**.

5. En **Topic Name**, introduzca un nombre de tema. En **Display Name**, introduzca un nombre para mostrar.
6. Seleccione un proyecto existente en la lista desplegable **Proyecto empresarial** o haga clic en **Create Proyecto empresarial** para crear un proyecto de empresa en la página **Proyecto empresarial Management** y, a continuación, selecciónelo.
7. Establecer claves de etiqueta y valores de etiqueta. Las etiquetas consisten en claves y valores. Identifican los recursos de la nube para que pueda clasificar y buscar fácilmente sus recursos.

Adición de suscripciones a un tema

Para enviar mensajes publicados en un tema a los suscriptores, debe agregar puntos de conexión de suscripción al tema. SMN envía automáticamente un mensaje de confirmación al punto de conexión de la suscripción. El mensaje de confirmación es válido solo dentro de las 48 horas. Los suscriptores deben confirmar la suscripción en un plazo de 48 horas para que puedan recibir mensajes de notificación. De lo contrario, el mensaje de confirmación no será válido y deberá enviarlo de nuevo.

1. Inicie sesión en la consola de gestión.
2. En **Management & Governance**, haga clic en **Simple Message Notification**.

   Se muestra la página **SMN**.

3. En el panel de navegación, elija **Topic Management** >**Topics**.

   Se muestra la página **Topics**.

4. Busque el tema al que desea agregar una suscripción, haga clic en **More** en la columna **Operation** y seleccione **Add Subscription**.

   Se muestra el cuadro **Add Subscription**.

   El protocolo se puede ajustar a **SMS**, FunctionGraph (función), a **HTTP**, **HTTPS**, y a **Email**.

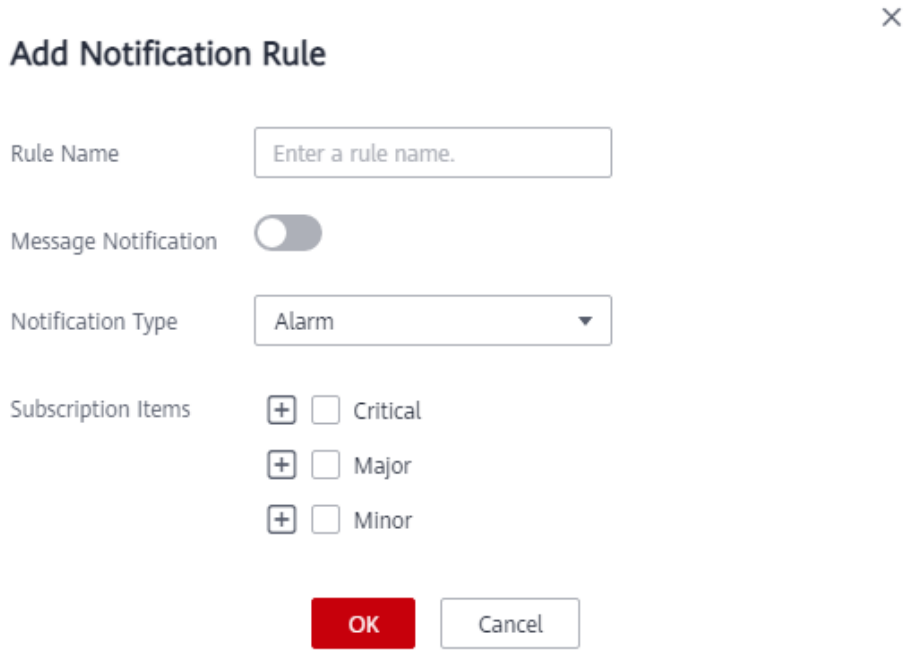
   Endpoint indica la dirección del punto de conexión de suscripción. SMS y correo electrónico, los puntos de conexión se pueden introducir en lotes. Al agregar puntos de conexión en lotes, cada dirección de punto de conexión ocupa una línea. Puede introducir un máximo de 10 puntos de conexión.

5. Haga clic en **OK**.

La suscripción que ha agregado se muestra en la lista de suscripción.

Envío de notificaciones a suscriptores

1. Inicie sesión en la consola de MRS.
2. Elija **Clusters > Active Clusters** y seleccione un clúster en ejecución y haga clic en su nombre para cambiar a la página de detalles del clúster.
3. Haga clic en **Alarms**.
4. Elija **Notification Rules** > **Add Notification Rule**. Se muestra la página **Add Notification Rule**.



5. Establezca los parámetros de la regla de notificación.

Tabla 3-19 Parámetros de una regla de notificación

Parámetro	Descripción
Rule Name	Nombre de regla de notificación definida por el usuario. Solo se permiten dígitos, letras, guiones (-) y guiones bajos (_).
Message Notification	● Si habilita esta función, el sistema envía notificaciones a los suscriptores basándose en la regla de notificación. ● Si deshabilita esta función, la regla no tiene efecto, es decir, las notificaciones no se envían a los suscriptores.
Topic Name	Seleccione un tema existente o haga clic en **Create Topic** para crear un tema.

Parámetro	Descripción
Notification Type	Seleccione el tipo de notificación a la que desea suscribirse. ● Alarma ● Evento
Subscription Items	Seleccione los elementos a los que se suscribirá. Puede seleccionar todos o algunos elementos según sea necesario. Reglas de suscripción en MRS 3.*x* o posterior: Severidad de la alarma: crítica, mayor y menor Evento: mayor, menor y advertencia Reglas de suscripción en versiones anteriores a MRS 3.x: ● Crítica ● Grave ● Menor ● Sugerencia

6. Haga clic en **OK**.

3.4.4 Comprobación del estado de salud

3.4.4.1 Antes de comenzar

Esta sección describe cómo gestionar las comprobaciones de estado en la consola MRS.

Las operaciones de gestión de comprobación de estado en la consola MRS solo se aplican a los clústeres de **MRS 1.9.2**.

La gestión de comprobación de estado en Manager se aplica a todas las versiones. Para las versiones MRS 3.x y posteriores, consulte **Consulta de una tarea de comprobación de estado**. Para versiones anteriores a MRS 3.x, consulte **Realización de una comprobación de estado**.

3.4.4.2 Realización de una comprobación de estado

Escenario

Para asegurarse de que los parámetros, las configuraciones y el monitoreo del clúster son correctos y que el clúster puede ejecutarse de forma estable durante mucho tiempo, puede realizar una comprobación de estado durante el mantenimiento de rutina.

NOTA

Una comprobación de estado del sistema incluye las comprobaciones de estado de MRS Manager, de nivel de servicio y de nivel de host:

- Las comprobaciones de estado de MRS Manager se centran en si la plataforma de gestión unificada puede proporcionar funciones de gestión.
- Las comprobaciones de estado a nivel de servicio se centran en si los componentes pueden proporcionar servicios correctamente.
- Las comprobaciones de estado a nivel de host se centran en si los indicadores de host son normales.

La comprobación de estado del sistema incluye tres tipos de elementos de comprobación: estado de estado, alarmas relacionadas e indicadores de monitoreo personalizados para cada objeto de comprobación. Los resultados de la comprobación de estado no siempre son los mismos que los del **Health Status** del portal.

Procedimiento

- Realice manualmente la comprobación de estado de todos los servicios.

  En la página de detalles de MRS, elija **Management Operations** > **Start Cluster Health Check**.

  NOTA

  Para las operaciones en MRS Manager, consulte **Realización de una comprobación de estado**; para las operaciones en FusionInsight Manager de MRS 3.*x* o posterior, consulte **Descripción**.

  - La comprobación del estado del clúster incluye comprobaciones del estado del Manager, del servicio y del host.
  - Para realizar comprobaciones de estado de clúster, también puede elegir **System** > **Check Health Status** > **Start Cluster Health Check** en MRS Manager.
  - Para exportar el resultado de la comprobación de estado, haga clic en **Export Report** en la esquina superior izquierda.

- Realice manualmente la comprobación de estado de un servicio.

  a. En la página de detalles del clúster de MRS, haga clic en **Components**.
  b. Seleccione el servicio de destino en la lista de servicios.
  c. Elija **More** > **Start Service Health Check** para iniciar la comprobación de estado del servicio.

- Realice manualmente la comprobación de estado de un host.

  a. En la página de detalles de MRS, haga clic en **Nodes**.
  b. Expanda la información del grupo de nodos y active la casilla de verificación del host que se va a marcar.
  c. Elija **Node** > **Start Host Health Check** para iniciar la comprobación de estado del host.

3.4.4.3 Consulta y exportación de un informe de comprobación de estado

Escenario

Puede ver el resultado de la comprobación de estado en MRS y exportarlo para su análisis posterior.

NOTA

Una comprobación de estado del sistema incluye las comprobaciones de estado de MRS Manager, de nivel de servicio y de nivel de host:

- Las comprobaciones de estado de MRS Manager se centran en si la plataforma de gestión unificada puede proporcionar funciones de gestión.
- Las comprobaciones de estado a nivel de servicio se centran en si los componentes pueden proporcionar servicios correctamente.
- Las comprobaciones de estado a nivel de host se centran en si los indicadores de host son normales.

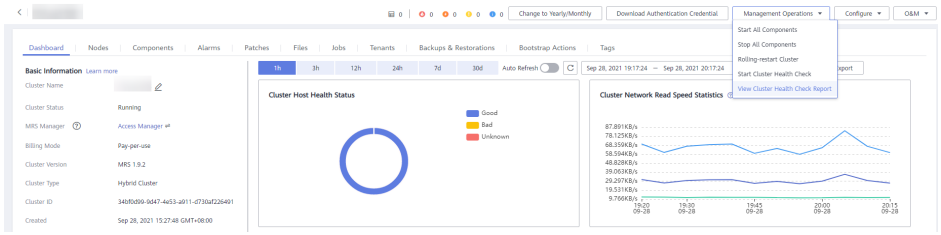
La comprobación de estado del sistema incluye tres tipos de elementos de comprobación: estado de estado, alarmas relacionadas e indicadores de monitoreo personalizados para cada objeto de comprobación. Los resultados de la comprobación de estado no siempre son los mismos que los del **Health Status** del portal.

Prerrequisitos

Ha realizado una comprobación de salud.

Procedimiento

Paso 1 En la página de pestaña **Dashboard** del clúster, seleccione **Management Operations** > **View Cluster Health Check Report**.



Paso 2 Haga clic en **Export Report** en el panel de informe de comprobación de estado para exportar el informe y ver información detallada sobre los elementos de comprobación.

----Fin

3.4.5 O&M remoto

3.4.5.1 Autorización de O&M

Si necesita personal de soporte técnico de Huawei Cloud para ayudarle con la solución de problemas, puede usar la función de autorización O&M para autorizar al personal de soporte técnico de Huawei Cloud a acceder a su host local para la localización de fallas.

Procedimiento

Paso 1 Inicie sesión en la consola de gestión de MRS.

Paso 2 En el árbol de navegación de la consola de gestión de MRS, elija **Clusters** > **Active Clusters**, seleccione un clúster en ejecución y haga clic en su nombre para cambiar a la página de detalles del clúster.

Paso 3 En la esquina superior derecha de la página, haga clic en **O&M**, seleccione **Authorize for Cluster Nodes** o **Authorize for Manager** y seleccione la fecha límite para que el personal de

soporte de Huawei Cloud acceda al host local. Antes de la fecha límite, el personal de soporte tiene el permiso temporal para acceder al host local.

Paso 4 Después de corregir el error, haga clic en **O&M** en la esquina superior derecha de la página y seleccione **Cancel Cluster Node Authorization** o **Cancel Manager Authorization** para recuperar el permiso de acceso otorgado al personal de soporte de Huawei Cloud.

----Fin

3.4.5.2 Compartir registros

Si necesita personal de soporte técnico de Huawei Cloud para ayudarle con la solución de problemas, puede utilizar la función de uso compartido de registros para proporcionar registros en un momento específico al personal de soporte técnico de Huawei Cloud para la localización de fallas.

Procedimiento

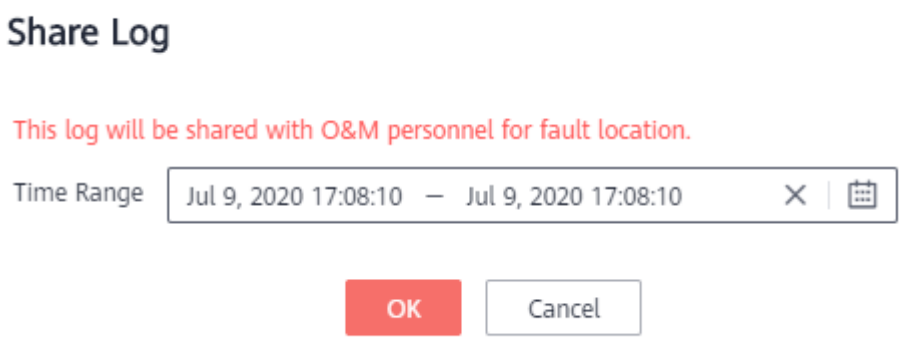
Paso 1 Inicie sesión en la consola de gestión de MRS.

Paso 2 En el árbol de navegación de la consola de gestión de MRS, elija **Clusters** > **Active Clusters**, seleccione un clúster y haga clic en su nombre para cambiar a la página de detalles del clúster.

Paso 3 En la esquina superior derecha de la página mostrada, seleccione **O&M** > **Share Log** para abrir el cuadro de diálogo **Share Log**.

Paso 4 Seleccione la hora de inicio y la hora de finalización en **Time Range**.

Figura 3-19 Compartir registros



NOTA

- Seleccione **Time Range** según las sugerencias del personal de soporte de Huawei Cloud.
- **End Date** debe ser más tarde de lo **Start Date**. De lo contrario, los registros no se pueden filtrar por tiempo.

----Fin

3.4.6 Consulta de registros de operaciones de MRS

Puede ver los registros de operaciones de clústeres y trabajos en la página **Operation Logs**. La información de registro se utiliza normalmente para localizar rápidamente fallas en caso de excepciones de clúster, lo que ayuda a los usuarios a resolver problemas.

Tipo de operación

Actualmente, MRS proporciona los siguientes registros de operación. Puede filtrar los registros en el cuadro de búsqueda.

- Operaciones de clúster
  - Creación, eliminación, escalamiento horizontal y escalamiento vertical en un clúster
  - Creación y eliminación de un directorio, eliminación de un archivo
- Operaciones del trabajo: Creación, detención y eliminación de un trabajo
- Operaciones de datos: tareas de usuario de IAM, adición de usuario y adición de grupo de usuarios

Campos de registro

Los registros se muestran en orden cronológico de forma predeterminada en la lista de registros, con los registros más recientes mostrados en la parte superior.

Tabla 3-20 describe varios campos en un registro.

Tabla 3-20 Descripción del registro

Parámetro	Descripción
Operation Type	Diversos tipos de operaciones, incluidos: ● Operaciones de clúster ● Operaciones de trabajo ● Operaciones de datos
Operation IP	Dirección IP donde se realiza una operación. **NOTA** Si un clúster MRS no se implementa, el clúster se elimina automáticamente y los registros de operaciones del clúster eliminado automáticamente no contienen el **Operation IP** del usuario.
Operation	Detalles de la operación. El valor puede contener un máximo de 2048 caracteres.
Time	Tiempo de operación. Para un clúster eliminado, solo se muestran los registros generados durante los últimos seis meses. Para ver los registros generados hace seis meses, póngase en contacto con soporte técnico de Huawei Cloud.
Enterprise Project	Proyecto de empresa al que pertenece el clúster

Tabla 3-21 Descripción de íconos

Ícono	Descripción
	Seleccione un proyecto de empresa en el cuadro de lista desplegable para filtrar los registros.
	Seleccione un tipo de operación en el cuadro de lista desplegable para filtrar los registros. ● **All Operation Types**: Filtra todos los registros. ● **Cluster**: Registros de filtros para **Cluster**. ● **Job**: Registros de filtros para **Job**. ● **Data**: Registros de filtros para **Data**.
	Filtrar los registros por tiempo. 1. Haga clic en el cuadro de entrada. 2. Especifique la fecha y la hora. 3. Haga clic en **OK**. El cuadro de entrada del lado izquierdo indica la hora de inicio y el del lado derecho indica la hora de finalización. La hora de inicio debe ser anterior o igual a la hora de finalización. De lo contrario, los registros no se pueden filtrar.
	Ingrese una palabra clave del **Operation Details** en el cuadro de búsqueda y haga clic en  para buscar registros.
	Haga clic en  para actualizar manualmente la lista de registros.

3.4.7 Changing Billing Mode to Yearly/Monthly

This section describes how to change the billing mode of a cluster from **Pay-per-use** to **Yearly/Monthly**.

This operation can be performed only when the cluster status is **Running** or **Stopping**.

Paso 1 Log in to the MRS console.

Paso 2 In the navigation tree of the MRS management console, choose **Clusters** > **Active Clusters**.

Paso 3 In the **Operation** column corresponding to the cluster for which you want to change the billing mode, click **Change to Yearly/Monthly**.

Paso 4 If you are sure you want to change the billing mode, click **Yes**.

Paso 5 On the **Change Subscription** page that is displayed, choose how often you would like to renew and click **Pay**.

After the order is submitted, the cluster status changes from **Running** to **Changing to Yearly/Monthly**.

After the order is paid successfully, the cluster billing mode starts changing to **Yearly/Monthly**. After the billing mode is successfully changed, the cluster status is **Running**.

NOTA

After the billing mode is changed to yearly/monthly, task nodes in a cluster are still billed in pay-per-use mode. During the change, the configured AS rules do not trigger scaling actions. Change the billing mode at an appropriate time to avoid any adverse impact on your services.

----Fin

3.4.8 Cancelar la suscripción a un clúster

Si no se requiere un clúster cargado en modo **Yearly/Monthly** después de la ejecución del trabajo, puede cancelar su suscripción. Después de cancelar la suscripción al clúster, los recursos y los datos se eliminarán y no se podrán restaurar. Asegúrese de que se haga una copia de respaldo de los datos antes de cancelar la suscripción del clúster.

Para obtener más información sobre las reglas de cancelación de suscripción, consulte **Cancelación de suscripción condicional**.

Antecedentes

Por lo general, después de analizar y almacenar los datos, o cuando el clúster encuentra una excepción y no puede funcionar, puede cancelar la suscripción de un clúster. Cuando el clúster de MRS no se despliega, el clúster se cancela automáticamente.

Procedimiento

Paso 1 Inicie sesión en la consola de gestión de MRS.

Paso 2 En el árbol de navegación de la consola de gestión de MRS, elija **Clusters** > **Active Clusters**.

Paso 3 En la columna **Operation** del clúster del que desea cancelar la suscripción, haga clic en **Unsubscribe**.

Paso 4 En la página **Unsubscribe**, confirme la información del clúster, seleccione los motivos de la cancelación de la suscripción y confirme el importe de la cancelación de la suscripción y las tarifas relacionadas.

Paso 5 Haga clic en **Confirm**.

Paso 6 Confirme la información de cancelación de suscripción y haga clic en **Yes** para enviar la solicitud de cancelación de suscripción.

Después de enviar la solicitud de cancelación de suscripción, el estado del clúster cambia de **Running** a **Deleting**. Después de eliminar el clúster, el estado del clúster cambia a **Deleted** y se muestra en el archivo **Cluster History**.

----Fin

3.4.9 Cancelar la suscripción de un nodo especificado en un clúster anual/mensual

Puede reducir el número de nodos específicos a escalar en un clúster para que MRS ofrezca mejores capacidades de almacenamiento e informática con menores costos de operación según los requisitos de servicio.

Actualmente, puede darse de baja de un máximo de 20 nodos principales a la vez, pero debe haber al menos 2 nodos principales disponibles después de darse de baja.

NOTA

Puede darse de baja de un nodo solo después de que el nodo se aísle o retire correctamente. De lo contrario, puede ocurrir la pérdida de datos.

Actualmente, solo los clústeres anuales/mensuales de las siguientes versiones admiten la cancelación de la suscripción de nodos especificados:

- MRS 1.8.10 (parche 1.8.10.6 o posterior)
- MRS 1.9.3 (parche 1.9.3.5 o posterior)
- MRS 3.1.5 o posterior

Restricciones de uso

- Si el número de nodos de Core en el clúster es menor o igual que el número de copias de HDFS, MRS no admite la cancelación de la suscripción de nodos para garantizar la confiabilidad de los datos. El número de copias de HDFS se puede consultar utilizando el parámetro **dfs.replication** en la configuración del parámetro de HDFS.
- MRS no admite la cancelación de la suscripción de nodos en los que se despliega ZooKeeper, Kudu, Kafka, o ClickHouse.

Cómo darse de baja de un nodo especificado en un clúster anual/mensual

Paso 1 Deshabilite la función de renovación automática del clúster donde se encuentra el nodo que se va a cancelar la suscripción. Para obtener más información, consulte **Desactivación de renovación automática**.

Paso 2 Inicie sesión en la consola de MRS.

Paso 3 Seleccione **Clusters** > **Active Clusters** activos y haga clic en el nombre del clúster de destino que se va a operar. Se muestra la página de detalles del clúster.

Paso 4 En la página **Dashboard** del clúster, haga clic en **Synchronize** a la derecha de **IAM User Sync**.

Paso 5 Cancelar la suscripción o aislar un nodo.

- Si la versión del clúster es anterior a MRS 3.1.5:
  a. Haga clic en **Isolate Node** en la columna **Operation** del grupo de nodos del que desea cancelar la suscripción.
  b. Seleccione el nodo del que desea cancelar la suscripción y haga clic en **OK**.

     El tiempo requerido para aislar un nodo depende del volumen de datos en el nodo. Un volumen de datos mayor indica un tiempo más largo.

     Después de aislar el nodo, el estado del nodo cambia a **Isolated**. El botón **Unsubscribe from Node** aparece en la página de pestaña **Nodes**.
- Si la versión del clúster es MRS 3.1.5 o posterior:
  a. Haga clic en **Decommission Node** en la columna **Operation** del grupo de nodos del que desea cancelar la suscripción.
  b. Seleccione el nodo que se va a retirar del servicio y haga clic en **OK**.

     El tiempo necesario para desmantelar un nodo depende del volumen de datos del nodo. Un volumen de datos mayor indica un tiempo más largo.

     Después de que el nodo se retira del servicio, el estado del nodo cambia a **Decommissioned**.

NOTA

- Solo se puede aislar o desmantelar un nodo a la vez. Puede darse de baja de un nodo solo después de que el nodo se aísle o retire correctamente.
- Si el nodo no puede aislar o desmantelar, inicie sesión en Manager. Haga clic en y busque el nombre de la tarea que no puede aislar o desmantelar el host de la lista de tareas, haga clic en el nombre y rectifique el error según se le solicite.

Paso 6 En la página de detalles del clúster, seleccione **Nodes** > **Unsubscribe from Node**.

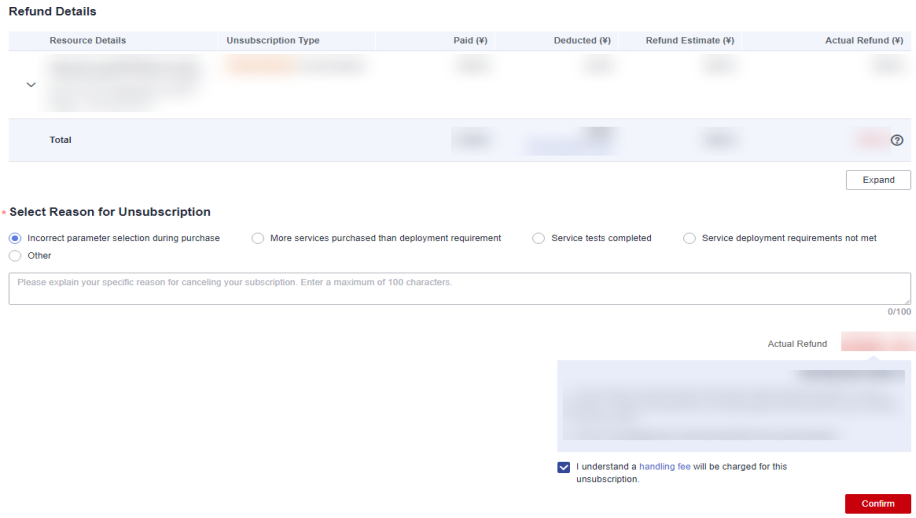
Paso 7 Seleccione el nodo del que desea cancelar la suscripción y haga clic en **OK**.

Actualmente, puede darse de baja de un máximo de 20 nodos principales a la vez, pero debe haber al menos 2 nodos principales disponibles después de darse de baja.

Paso 8 En la página mostrada, seleccione. "I understand a handling fee will be charged for this unsubscription" y haga clic en **Confirm**.

El estado del clúster cambia a **Scaling in**. Una vez completada la escala, el estado del clúster cambia a **Running** y se elimina el nodo especificado.

Figura 3-20 Detalles del reembolso



Paso 9 (Opcional) Para habilitar la renovación automática de un clúster, consulte **Habilitación de renovación automática**.

----Fin

3.4.10 Terminación de un clúster

Puede terminar un clúster MRS una vez completada la ejecución del trabajo. El clúster terminado o cancelado ya no se factura.

Antecedentes

Puede terminar manualmente un clúster una vez completado el análisis de datos o cuando el clúster encuentra una excepción. Un clúster que no se despliega se terminará automáticamente.

Un clúster de facturación anual/mensual no se puede cancelar, pero se puede cancelar la suscripción. Para obtener más información acerca de cómo cancelar la suscripción a un clúster, consulte **Cancelar la suscripción a un clúster**.

Procedimiento

Paso 1 Inicie sesión en la consola de gestión de MRS.

Paso 2 En el panel de navegación de la izquierda, elija **Clusters** > **Active Clusters**.

Paso 3 En la lista de clústeres, busque la fila que contiene el clúster que se va a terminar y haga clic en **Terminate** en la columna **Operation**.

El estado del clúster cambia de **Running** a **Terminating** y finalmente a **Terminated**. Puede ver el clúster terminado de **Cluster History**. El clúster terminado ya no se factura.

----Fin

3.5 Gestión de nodos

3.5.1 Escalamiento horizontal de un clúster

Las capacidades de almacenamiento y computación de MRS se pueden mejorar simplemente agregando nodos de Core o nodos de Task en lugar de modificar la arquitectura del sistema, reduciendo los costos de operación. Los nodos principales pueden procesar y almacenar datos. Puede agregar nodos de Core para expandir las cantidades de nodo y controlar las cargas máximas. Los nodos de Task se utilizan para procesar datos en lugar de almacenar datos persistentes.

Antecedentes

Only Core nodes and Task nodes can be added.

Restricciones

- Cuando expanda un grupo de nodos donde está instalado HBase:

  Si el registro DNS automático no está habilitado para un nodo del clúster, no inicie HBase al expandir el grupo de nodos. A continuación, actualice la configuración del cliente HBase haciendo referencia a **Actualización de un cliente** e inicie las instancias HBase en el nodo que se va a expandir.

  El registro automático de DNS está habilitado de forma predeterminada en las siguientes versiones de MRS:

  MRS 1.9.3, 2.1.1, 3.0.5, 3.1.0, y 3.1.1-LTS
- Después de un escalamiento horizontal, no es necesario actualizar el cliente instalado en los nodos del clúster. Para obtener más información acerca de cómo actualizar el cliente instalado en nodos fuera del clúster, consulte **Actualización de un cliente**.

Escalamiento horizontal de un clúster facturado en modo de pago por uso

Paso 1 Inicie sesión en la consola de MRS.

Paso 2 Elija **Clusters** > **Active Clusters** y seleccione un clúster en ejecución y haga clic en su nombre para cambiar a la página de detalles del clúster.

Paso 3 Haga clic en la pestaña **Nodes**. En la columna **Operation** del grupo de nodos, haga clic en **Scale Out**. Se muestra la página **Scale Out**.

La operación de escalamiento horizontal solo se puede realizar en los clústeres en ejecución.

Paso 4 Defina el tipo de **System Disk** y **Data Disk**, **Scale-Out Nodes**, **Enable Components** y **Run Bootstrap Action** y haga clic en **OK**. Los parámetros **Enable Components** y **Run Bootstrap Action** solo son compatibles con clústeres de versiones anteriores a MRS 3.x.

NOTA

- Si el grupo de nodos Task no existe en el clúster, configure el nodo Task haciendo referencia a **Tareas relacionadas**.
- Si se agrega una acción de arranque durante la creación del clúster, el parámetro **Run Bootstrap Action** es válido. Si esta función está habilitada, las acciones de arranque agregadas durante la creación del clúster se ejecutarán en todos los nodos escalados.
- Si el parámetro **New Specifications** está disponible, las especificaciones que son las mismas que las de los nodos originales se han agotado o descontinuado. Se agregarán nodos con nuevas especificaciones.
- Antes de ampliar el clúster, compruebe si la configuración del grupo de seguridad es correcta. Asegúrese de que una regla de grupo de seguridad entrante contenga una regla en la que **Protocol & Port** esté establecida en **All** y **Source** esté establecida en un intervalo de direcciones IP accesible de confianza.

Paso 5 En el cuadro de diálogo **Add Node**, haga clic en **OK**.

Paso 6 En la esquina superior derecha de la página aparece un cuadro de diálogo que indica que la tarea de escalamiento horizontal se ha enviado correctamente.

Los siguientes parámetros explican el proceso de escalamiento horizontal del clúster:

- Durante el escalamiento horizontal: si se está escalando un clúster, su estado es de **Scaling out**. Los trabajos enviados se ejecutarán y podrá enviar nuevos trabajos. No se le permite continuar escalando o terminando el clúster. Se recomienda no reiniciar el clúster ni modificar la configuración del clúster.
- Escalamiento horizontal exitoso: El estado del clúster es **Running**. Se cobran los recursos utilizados en los nodos antiguos y en los nodos expandidos.
- Error de escalamiento horizontal: el estado del clúster es **Running**. Puede ejecutar trabajos y escalar el clúster de nuevo.

Después de ampliar el clúster, puede ver la información de nodo del clúster en la página **Nodes**.

----Fin

Escalamiento de un clúster facturado en modo anual/mensual

Paso 1 Inicie sesión en la consola de MRS.

Paso 2 Elija **Clusters** > **Active Clusters** y seleccione un clúster en ejecución y haga clic en su nombre para cambiar a la página de detalles del clúster.

Paso 3 Haga clic en la pestaña **Nodes**. En la columna **Operation** del grupo de nodos, haga clic en **Scale Out**. Se muestra la página **Scale Out**.

La operación de escalamiento horizontal solo se puede realizar en los clústeres en ejecución.

Paso 4 Establezca el tipo de **System Disk** y **Data Disk**, **Scale-Out Nodes**, **Enable Components** y **Run Bootstrap Action**. El sistema muestra el tiempo de caducidad del clúster y la tarifa requerida para agregar nodos. Los parámetros **Enable Components** y **Run Bootstrap Action** solo son compatibles con clústeres de versiones anteriores a MRS 3.x.

NOTA

- Si se agrega una acción de arranque durante la creación del clúster, el parámetro **Run Bootstrap Action** es válido. Si esta función está habilitada, las acciones de arranque agregadas durante la creación del clúster se ejecutarán en todos los nodos escalados. Las acciones de arranque se admiten en versiones anteriores a MRS 3.*x*.
- Si el parámetro **New Specifications** está disponible, las especificaciones que son las mismas que las de los nodos originales se han agotado o descontinuado. Se agregarán nodos con nuevas especificaciones.
- Antes de ampliar el clúster, compruebe si la configuración del grupo de seguridad es correcta. Asegúrese de que una regla de grupo de seguridad entrante contenga una regla en la que **Protocol & Port** esté establecida en **All** y **Source** esté establecida en un intervalo de direcciones IP accesible de confianza.

- Haga clic en **Submit Order**.

En la página **Purchase MapReduce Service**, haga clic en **Pay**.

- Haga clic en **Confirm order, not pay**.

En la página de información del clúster, elija **Fee > My Order** y haga clic en **Pay**.

Paso 5 Una vez que el pago se haya realizado correctamente, vuelva a la consola de gestión de MRS para ver el estado del clúster.

Los siguientes parámetros explican el proceso de escalamiento horizontal del clúster:

- Durante el escalamiento horizontal: si se está escalando un clúster, su estado es de **Scaling out**. Los trabajos enviados se ejecutarán y podrá enviar nuevos trabajos. No se le permite continuar escalando o terminando el clúster. Se recomienda no reiniciar el clúster ni modificar la configuración del clúster.
- Escalamiento horizontal exitoso: El estado del clúster es **Running**. Se cobran los recursos utilizados en los nodos antiguos y en los nodos expandidos.
- Error de escalamiento horizontal: el estado del clúster es **Running**. Puede ejecutar trabajos y escalar el clúster de nuevo.

Después de ampliar el clúster, puede ver la información de nodo del clúster en la página **Nodes**.

----Fin

Adición de un nodo de Task

Puede escalar un clúster de MRS agregando manualmente nodos de tarea.

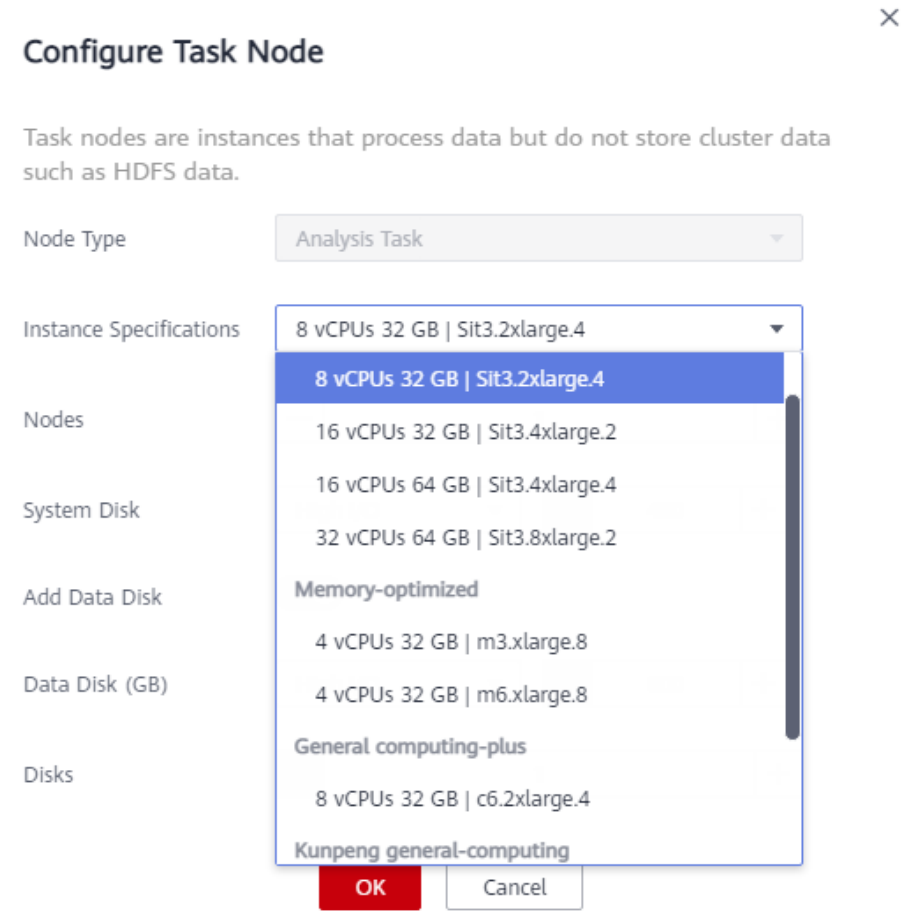
Para agregar un nodo de tarea a un clúster personalizado, realice los siguientes pasos:

1. En la página de detalles del clúster, haga clic en la pestaña **Nodes** y haga clic en **Add Node Group**. Se muestra la página **Add Node Group**.
2. Seleccione **NM** para **Deploy Roles** y establezca otros parámetros según sea necesario.

Para agregar un nodo de task a un clúster no personalizado, realice los siguientes pasos:

1. En la página de detalles del clúster, haga clic en la pestaña **Nodes** y haga clic en **Configure Task Node**. Se muestra la página **Configure Task Node**.

2. En la página **Configure Task Node**, establezca **Node Type**, **Instance Specifications**, **Nodes**, **System Disk**. Además, si **Add Data Disk** está habilitado, configure el tipo de almacenamiento, el tamaño y el número de discos de datos.



3. Haga clic en **OK**.

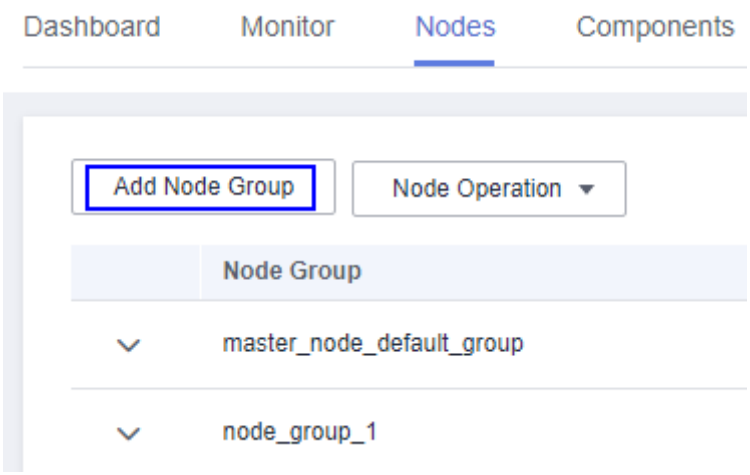
Adición de un grupo de nodos

NOTA

Se utiliza para agregar grupos de nodos y se aplica a clústeres personalizados de MRS 3.*x*.

1. En la página de detalles del clúster, haga clic en la pestaña **Nodes** y haga clic en **Add Node Group**. Se muestra la página **Add Node Group**.

Figura 3-21 Haga clic en Add Node Group



2. Establezca los parámetros según sea necesario.
3. Haga clic en **OK**.

3.5.2 Escalamiento vertical de un clúster

Puede reducir el número de nodos principales o de tareas a escalar en un clúster en función de los requisitos de servicio, de modo que MRS ofrezca mejores capacidades de almacenamiento e informática con menores costos de operación.

No se permite la operación de escalamiento vertical en un clúster que realiza la sincronización activa/en espera.

NOTA

Solo se pueden escalar clústeres de pago por uso. Para obtener más información acerca de cómo escalar en un nodo anual/mensual, consulte **Cancelar la suscripción de un nodo especificado en un clúster anual/mensual**.

Antecedentes

Un clúster puede tener tres tipos de nodos: nodos de master, core, y task. Actualmente, solo se pueden eliminar los nodos principales y de tareas. Para escalar en un clúster, solo necesita ajustar el número de nodos en la consola MRS. A continuación, MRS selecciona automáticamente los nodos que se van a eliminar.

Las políticas para que MRS seleccione automáticamente nodos son las siguientes:

- MRS no selecciona los nodos con componentes básicos instalados, como ZooKeeper, DBService, KrbServer y LdapServer, porque estos componentes básicos son la base para que se ejecute el clúster.
- Los nodos principales almacenan datos de servicio de clúster. Al escalar en un clúster, asegúrese de que todos los datos de los nodos principales que se van a eliminar se han migrado a otros nodos. Puede realizar operaciones de escalado de seguimiento solo después de que se retiren todos los servicios de componentes, por ejemplo, quitar nodos del Manager y eliminar los ECS. Al seleccionar los nodos de core, MRS selecciona preferentemente los nodos con una pequeña cantidad de datos e instancias sanas que se van a desmantelar para evitar fallos en el desmantelamiento. Por ejemplo, si DataNodes se instalan en nodos de core en un clúster de análisis, MRS selecciona preferentemente

los nodos con un volumen de datos pequeño y un buen estado de salud durante el escalamiento vertical.

Cuando se eliminan los nodos centrales, sus datos se migran a otros nodos. Si la empresa de usuario ha almacenado en caché la ruta de almacenamiento de datos, el cliente actualizará automáticamente la ruta, lo que puede aumentar la latencia de procesamiento del servicio temporalmente. El escalamiento vertical del clúster puede ralentizar la respuesta del primer acceso a algunos datos de HBase en HDFS. Puede reiniciar HBase o deshabilitar o habilitar tablas relacionadas para resolver este problema.

- Los nodos de task son nodos informáticos y no almacenan datos de clúster. La migración de datos no implica la eliminación de nodos de task. Por lo tanto, al seleccionar nodos de task, MRS selecciona preferentemente nodos cuyo estado de salud es defectuoso, desconocido o subsano. En la pestaña **Components** de la consola MRS, haga clic en un servicio y, a continuación, en la pestaña **Instances** para ver el estado de las instancias de nodo.

Política de verificación de escalamiento vertical

Para evitar fallos de desmantelamiento de componentes, los componentes proporcionan diferentes restricciones de desmantelamiento. El escalamiento vertical solo se permite cuando se cumplen las restricciones de todos los componentes instalados. **Tabla 3-22** describe las políticas de verificación de escalamiento vertical.

Tabla 3-22 Restricciones de desmantelamiento

Componente	Restricción
HDFS/DataNode	El número de nodos disponibles tras el escalamiento vertical es mayor o igual que el número de copias HDFS y el volumen total de datos HDFS no supera el 80% de la capacidad total del clúster HDFS. Esto asegura que el espacio restante es suficiente para almacenar los datos existentes después de la escalación y reserva algo de espacio para su uso futuro. **NOTA** Para garantizar la fiabilidad de los datos, se genera automáticamente una copia de respaldo por cada archivo guardado en HDFS, es decir, se generan dos copias en total.
HBase/ RegionServer	La memoria total disponible de RegionServers en todos los nodos excepto los nodos que se van a eliminar es superior a 1.2 veces la memoria que RegionServers utiliza actualmente en estos nodos. Esto garantiza que el nodo al que se migra la región de un nodo dado de baja tiene memoria suficiente para soportar la región del nodo dado de baja.
Storm/ Supervisor	Después del escalamiento vertical, asegúrese de que el número de ranuras en el clúster es suficiente para ejecutar las tareas enviadas. Esto evita que no haya suficientes recursos disponibles para ejecutar las tareas de procesamiento de flujo después del escalamiento vertical.

Componente	Restricción
Flume/FlumeServer	Si FlumeServer está instalado en un nodo y se han configurado tareas de Flume para el nodo, el nodo no se puede eliminar. Esto evita que el programa de servicio desplegado se elimine por error.
ClickHouse/ ClickHouseServer	Para obtener más información, consulte **Restricciones en la reducción de ClickHouseServer**. Esto garantiza que los datos de los nodos retirados de servicio se migren a los nodos en uso.

Escalamiento vertical de un clúster mediante especificación de la cantidad de nodo

Paso 1 Inicie sesión en la consola de MRS.

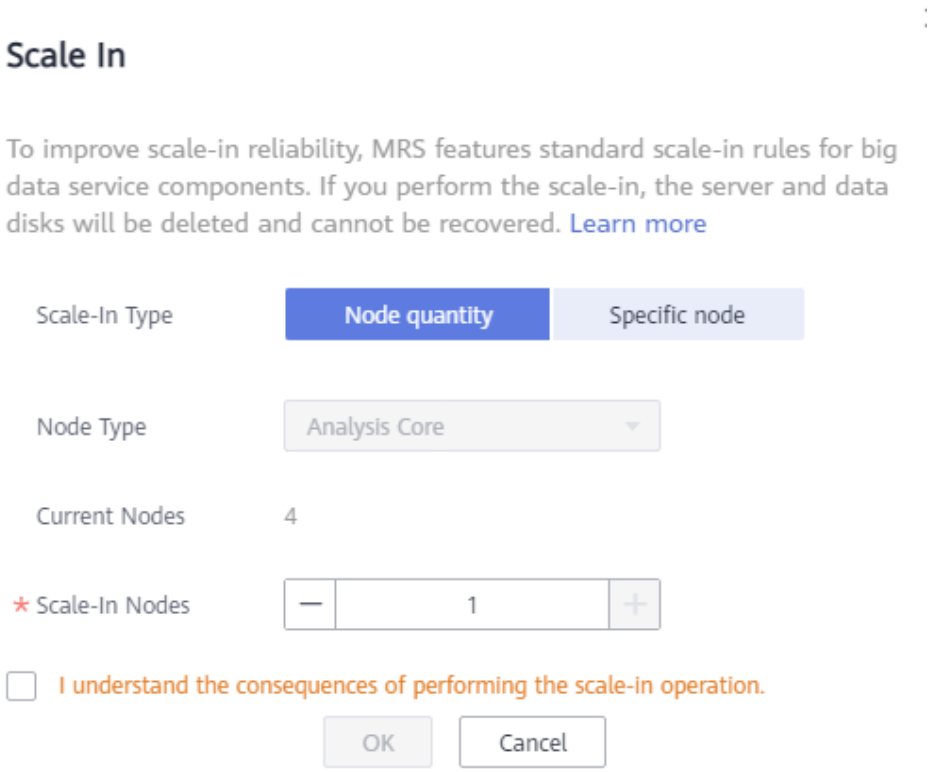
Paso 2 Seleccione **Clusters** > **Active Clusters**, seleccione un clúster en ejecución y haga clic en su nombre para cambiar a la página de detalles del clúster.

Paso 3 Haga clic en la pestaña **Nodes**. En la columna **Operation** del grupo de nodos, haga clic en **Scale In** para ir a la página **Scale In**.

Esta operación solo se puede realizar cuando el clúster y todos los nodos en él se están ejecutando.

Paso 4 Establezca **Scale-In Type** en **Node quantity**.

Paso 5 Establezca **Scale-In Nodes** y haga clic en **OK**.



NOTA

- Antes de escalar verticalmente el clúster, compruebe si la configuración del grupo de seguridad es correcta. Asegúrese de que una regla de grupo de seguridad entrante contenga una regla en la que **Protocol & Port** esté establecida en **All** y **Source** esté establecida en un intervalo de direcciones IP accesible de confianza.
- Si existen bloques de datos dañados en HDFS, puede fallar el escalamiento vertical. Póngase en contacto con soporte técnico de Huawei Cloud.

Paso 6 Un cuadro de diálogo que aparece en la esquina superior derecha de la página indica que la tarea de quitar el nodo se ha ejecutado correctamente.

El proceso de escalado de clústeres se explica de la siguiente manera:

- Durante el escalado: el estado del clúster es **Scaling In**. Los trabajos enviados se ejecutarán, y usted puede enviar nuevos trabajos. No se le permite continuar escalando verticalmente o terminando el clúster. Se recomienda no reiniciar el clúster ni modificar la configuración del clúster.
- Escalamiento vertical exitoso: El estado del clúster es **Running**. Se facturan los recursos que se utilizan después del escalamiento vertical del clúster.
- Error de escalado: el estado del clúster es **Running**. Puede ejecutar trabajos o escalar de nuevo en el clúster.

Después de escalar el clúster, puede ver la información de nodo del clúster en la página **Nodes**.

----Fin

Escalar verticalmente en un clúster mediante la eliminación de nodos que ya no se necesitan

If a faulty node is no longer needed, you can use this function to remove it. When the node is removed, the instance of the component role will not be decommissioned. Before deleting the node, ensure that the data on the node has been backed up. For details about how to remove ClickHouseServer nodes, see **Eliminación de nodos de instancia ClickHouseServer**. Only pay-per-use nodes can be scaled in.

Paso 1 Log in to MRS Manager and choose **Hosts**.

Paso 2 Select the host to be removed, choose **More**, and select **Isolate** to isolate the host.

For versions earlier than MRS 3.x, isolate the node to be removed by referring to **Aislamiento de un host**.

The time required for isolating a host depends on the data volume on the host. A larger data volume requires a longer time.

After the node is isolated, the node status changes to **Isolated**.

NOTA

- If the host isolation fails, log in to MRS Manager, click to search for the task that fails to isolate the host in the task list, and rectify the fault as prompted.
- Isolating a host helps you decommission a node. If data on the node has been backed up, you can skip the operation of isolating a host, directly stop the host on the ECS console, and scale in the host.
- If a host is faulty, forcibly remove the node.

Paso 3 Log in to the MRS console.

Paso 4 Click the name of the cluster to go to its details page.

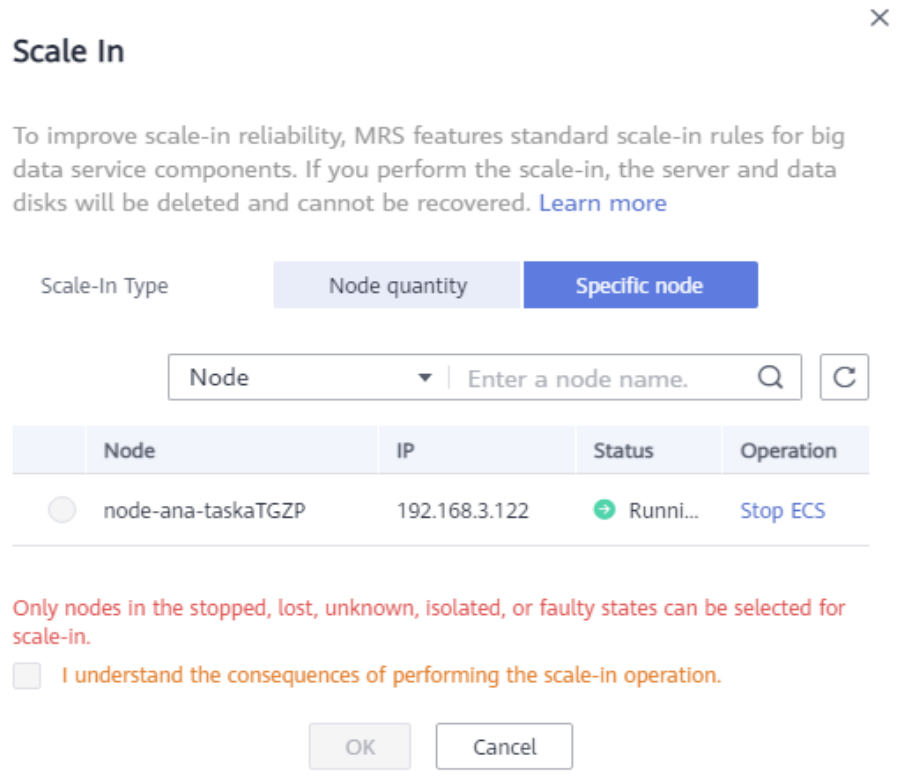
Paso 5 Click the **Nodes** tab.

Paso 6 Locate the row that contains the target node group and click **Scale In** in the **Operation** column to go to the **Scale In** page.

Paso 7 Set **Scale-In Type** to **Specific node** and select the node to be removed.

Nodes in the **Stopped**, **Lost**, **Unknown**, **Isolated**, or **Faulty** status can be specified for scale-in. If the node cannot be selected, click **Stop ECS** to go to the ECS console to stop the node. On the cluster details page of the MRS console, click the **Alarms** tab and check whether any service fault alarms are generated after the node is stopped. If no such an alarm is generated, go back to the **Scale In** page and select the corresponding node for scale-in. If such an alarm is generated, clear the alarm before the scale-in.

Figura 3-22 Removing a specific node



Paso 8 Select **I understand the consequences of performing the scale-in operation**, and click **OK**.

Paso 9 Click the **Components** tab and check whether each component is normal. If any component is abnormal, wait for 5 to 10 minutes and check the component status again. If the fault persists, contact Huawei Cloud technical support.

Paso 10 Click the **Alarms** tab and check whether there are exception alarms. If there are exception alarms, clear them before performing other operations.

----Fin

3.5.3 Eliminación de nodos de instancia ClickHouseServer

3.5.3.1 Restricciones en la reducción de ClickHouseServer

Escala de clúster

- Si un clúster solo tiene un shard, los nodos de instancia no se pueden quitar del clúster.
- Múltiples nodos de instancia en el mismo shard **deben desmantelarse o volver a ponerse en servicio al mismo tiempo**.

  La información del fragmento del clúster se puede consultar ejecutando la sentencia SQL **select cluster,shard_num,replica_num,host_name from system.clusters;**.

Almacenamiento de clústeres

Asegúrese de que el espacio en disco de los nodos que no se desmantelarán sea suficiente para almacenar datos de todos los nodos desmantelados. Debe haber aproximadamente un 10% de espacio de almacenamiento redundante después del desmantelamiento para garantizar que las instancias restantes puedan funcionar correctamente. El procedimiento es el siguiente:

1. Ejecute el siguiente comando para comprobar el uso del disco en cada nodo:

   select * from system.disks;

   free_space indica el espacio libre en disco, y **total_space** indica el espacio total en disco. El espacio usado se calcula restando el valor de **free_space** del de **total_space** y su unidad es byte.
2. Ejecute el comando anterior en un nodo que desea retirar del servicio y calcule el volumen de datos en el nodo mediante la fórmula anterior.
3. Ejecute el comando anterior en un nodo que no se retirará del servicio y, a continuación, utilice la siguiente fórmula: (Valor de **free_space** - Volumen de datos del nodo que se va a desmantelar)/Valor de **total_space**. Si el resultado es superior al 10%, el nodo se puede retirar del servicio.

Estado del clúster

Si hay algún nodo de instancia de ClickHouseServer defectuoso en el clúster, no se pueden retirar todos los nodos de instancia del clúster. Elija **Cluster** > **Services** > **ClickHouse**, haga clic en **Instance** y vea el estado de ejecución de cada nodo del clúster.

Base de datos

Si una base de datos solo se implementa en un nodo de instancia que desea desmantelar, no se puede desmantelar el nodo de instancia. Para quitar el nodo de instancia, debe crear la base de

datos en todos los nodos de instancia de ClickHouseServer del clúster. El procedimiento es el siguiente:

1. Ejecute el comando **select * from system.databases;** para recopilar la lista de base de datos de cada nodo.

   name indica el nombre de la base de datos. **engine** indica el motor de base de datos y el valor predeterminado es **Atomic**. Si se utiliza el motor predeterminado, no es necesario especificar el motor al crear una tabla.

2. Para la base de datos desplegada solo en el nodo de instancia que se va a desmantelar, ejecute el siguiente comando para crear la base de datos:

   create database xxx engine=xxx on cluster xxx;

Tabla local no replicada

Si una tabla no replicada local se despliega solo en un nodo de instancia que desea desmantelar, no se puede desmantelar el nodo de instancia. Para desmantelar el nodo, cree una tabla local no replicada con el mismo nombre en cualquier nodo que no se desmantelar.

Por ejemplo, el clúster actual tiene dos shards, el shard 1 tiene dos nodos A y B, y el shard 2 tiene dos nodos C y D. La tabla no replicada **test** se creó sin la palabra clave **ON CLUSTER**, por lo que la tabla solo se crea en el nodo A.

En este caso, para desmantelar los nodos A y B en shard 1, es necesario crear la tabla **test** en el nodo C o D en shard 2.

Ejecute el siguiente comando para listar las tablas de datos de cada nodo:

select database,name,engine,create_table_query from system.tables where database != 'system';

Realice las siguientes operaciones según el resultado:

- Compruebe la columna **engine**. La tabla que no contiene el campo **Replicated** es una tabla local no replicada.
- Si no hay tablas replicadas en ningún nodo que no se retiren, cree una basada en la tabla creada por **create_table_query**. La siguiente sentencia de creación es un ejemplo:

  CREATE TABLE {database}.{table} ('column name' type...) ENGINE = MergeTree;

Tabla replicada

Si solo existe una tabla replicada en algunos nodos del clúster, no se pueden retirar los nodos en los que se despliega la tabla replicada. Debe crear manualmente la tabla replicada en todos los nodos de instancia en los que no se despliega ninguna tabla replicada en el clúster antes de retirar el servicio.

Por ejemplo, el clúster actual tiene dos particiones, la partición 1 tiene dos nodos A y B, y la partición 2 tiene dos nodos C y D. La tabla replicada **test** se creó sin la palabra clave **ON CLUSTER** por lo que la tabla solo se crea en los nodos A y B.

Para desmantelar los nodos A y B en el fragmento 1, es necesario crear la tabla **test** en los nodos C y D en la partición 2.

Ejecute el siguiente comando para listar las tablas de datos de cada nodo:

select database,name,engine,create_table_query from system.tables where database != 'system';

Realice las siguientes operaciones según el resultado:

- Compruebe la columna **engine**. La tabla que contiene el campo **Replicated** es una tabla replicada.
- Si no hay tablas replicadas en ningún nodo que no se retiren, cree una basada en la tabla creada por **create_table_query**.

Tabla distribuida

Las tablas distribuidas no se migrarán automáticamente para el desmantelamiento. Cree tablas distribuidas en los nodos que no se retirarán del servicio.

Ejecute el siguiente comando para listar las tablas de datos de cada nodo y compruebe la columna **engine**. Estas tablas son tablas distribuidas si esta columna contiene el campo **Distributed**.

select database,name,engine from system.tables where database != 'system';

NOTA

La creación de tablas distribuidas en estos nodos no afectará al desmantelamiento, pero puede afectar a las operaciones de servicio posteriores.

Vista

Las vistas no se migrarán automáticamente para el desmantelamiento y las vistas no almacenan datos. Ejecute el siguiente comando para listar las tablas de datos de cada nodo y compruebe la columna **engine**. Estas tablas son vistas si esta columna contiene el campo **View**.

select database,name,engine from system.tables where database != 'system';

Ejecute el siguiente comando para eliminar las vistas una por una:

drop view {database_name}.{table_name};

Vistas materializadas

Las vistas materializadas no se migrarán automáticamente para Desmantelamiento. Cree vistas materializadas en los nodos que no se retirarán del servicio. Si la vista materializada de un nodo que se va a desmantelar no muestra la tabla de agregación especificada, pero utiliza una tabla incrustada, el nodo no se puede desmantelar.

Ejecute el siguiente comando para listar las tablas de datos de cada nodo y compruebe la columna **engine**. Estas tablas son vistas materializadas si esta columna contiene el campo **MaterializedView**.

select database,name,engine, create_table_query from system.tables where database != 'system';

La tabla cuya columna **create_table_query** contiene el campo **POPULATE** es una tabla incrustada. Las vistas se inicializan cuando se crean y los datos recién insertados se omiten durante la inicialización. Una tabla que no contiene el campo **POPULATE** es una tabla de agregación. Los datos recién insertados se insertan directamente en los gráficos de vista y las

tablas de soporte, y los datos originales se cargan manualmente en las vistas y las tablas de soporte. Las operaciones de creación de tabla de la tabla de agregación y la tabla incrustada son diferentes.

Realice las siguientes operaciones para procesar las vistas materializadas del nodo que se va a retirar del servicio:

1. Registre las vistas materializadas y elimínelas.

   drop view {database_name}.{table_name};

2. Una vez completada la retirada de nodos, elimine y vuelva a crear las vistas materializadas correspondientes en los nodos en uso para actualizar las vistas materializadas.
3. Para crear una tabla de agregación, especifique **WHERE** para buscar datos históricos e importar manualmente los datos históricos a las vistas materializadas. De lo contrario, los datos históricos no se pueden importar a las vistas materializadas según condiciones unificadas. Como resultado, los datos se importan repetidamente. Por ejemplo, se puede especificar un punto de actualización para garantizar que los datos antes del punto de actualización se carguen manualmente en modo **INSERT**.
   - Agregue **WHERE** *{ Time field (for example, date)}***>= toDate (***{ Current time (for example, '2022-12-01 00:00:00')}***)** a la sentencia de creación de tabla.
   - **insert into** *{table}* **select** *{Table field}* **from** *{Source table}* **where** *{Time field}***< toDate** *({Current time})* is used to load original data.
4. Las tablas incrustadas perderán los datos generados durante la creación de tablas. Puede especificar **WHERE** para filtrar todos los datos históricos. En este caso, se crea una tabla vacía y solo es necesario insertar manualmente todos los datos en la tabla de origen de datos históricos.

Tablas de motores de terceros

Actualmente, las tablas de motores de terceros no se pueden migrar automáticamente para su desmantelamiento.

Ejecute el siguiente comando para listar las tablas de datos de cada nodo y compruebe la columna **engine**. Estas tablas son tablas de motores de terceros si esta columna no contiene ninguno de los siguientes campos: **MergeTree**, **View**, **MaterializedView**, **Distributed**, and **Log**. (La columna **engine** de una tabla de motor de terceros puede contener campo **Memory**, **HDFS**, o **MySQL**.)

select database,name,engine from system.tables where database != 'system';

Cree tablas de motor de terceros en los nodos que no se retirarán del servicio y elimine las de los nodos que se retirarán del servicio.

Datos desvinculados

Si la tabla de un nodo que se va a retirar del servicio se ha desconectado y todavía existen datos en el directorio **detached**, el nodo no se puede retirar del servicio. Es necesario adjuntar los datos del directorio **detached** a otros directorios antes de retirar el servicio.

1. Ejecute el siguiente comando para ver el catálogo del sistema **system.detached_parts** del nodo que se va a retirar del servicio:

   select * from system.detached_parts;

2. Si existen datos de **detached part** y estas particiones ya no se utilizan, ejecute el siguiente comando para eliminar los datos de **detached part**:

   ALTER TABLE {table_name} DROP DETACHED PARTITION {partition_expr} SETTINGS allow_drop_detached = 1;

3. Ejecute el siguiente comando para comprobar si hay algún dato **detached part** en el catálogo del sistema **system.detached_parts**:

   select * from system.detached_parts;

   Si la salida del comando está vacía, no hay datos de **detached part** en este catálogo del sistema.

3.5.3.2 Reducción de nodos de ClickHouseServer

Antes de eliminar los nodos de instancia de ClickHouseServer, debe retirarlos del servicio. Múltiples réplicas de nodo de la misma partición **deben desmantelarse al mismo tiempo**. Si hay un nodo de instancia de ClickHouseServer defectuoso en el clúster, no se pueden retirar todos los nodos de instancia del clúster. Para obtener más restricciones, consulte **Restricciones en la reducción de ClickHouseServer**.

NOTA

- Realice el desmantelamiento en horas inactivas porque la operación ocupará ciertos recursos de ancho de banda.
- La operación de desmantelamiento solo se puede realizar a ClickHouseServer. ClickHouseBalancer no puede ser dado de baja.
- **Esta operación sólo es compatible con MRS 3.1.2 y posteriores.**

Paso 1 Utilice PuTTY para iniciar sesión en el nodo donde está instalado ClickHouseServer como usuario **root** y ejecute el siguiente comando:

echo 'select * from system.clusters' | curl -k 'https://*IP address of the node where the ClickHouseServer instance is located***:***Port number***/' -u** *ck_user*:*Password* **--data-binary @-**

Registre los nodos de la misma partición. En la siguiente salida del comando, los nodos con el mismo número en negrita pertenecen a la misma partición.

```
[root@kwephispra44948 ~]# echo 'select * from  system.clusters' | curl -k
'https://10.112.17.189:21422/' -u ck_user:Bigdata_2013  --data-binary @-
default_cluster 1       1       1       kwephispra44947 10.112.17.150  21427
0                       0       0
default_cluster 1       1       2       kwephispra44948 10.112.17.189  21427
0                       0       0
```

NOTA

- Para ver el número de puerto de los nodos de instancia de ClickHouseServer, inicie sesión en FusionInsight Manager, seleccione **Cluster** > **Services** > **ClickHouse**, click **Configuration** > **All Configurations**, y elija **ClickHouseServer (Role)** a la izquierda.

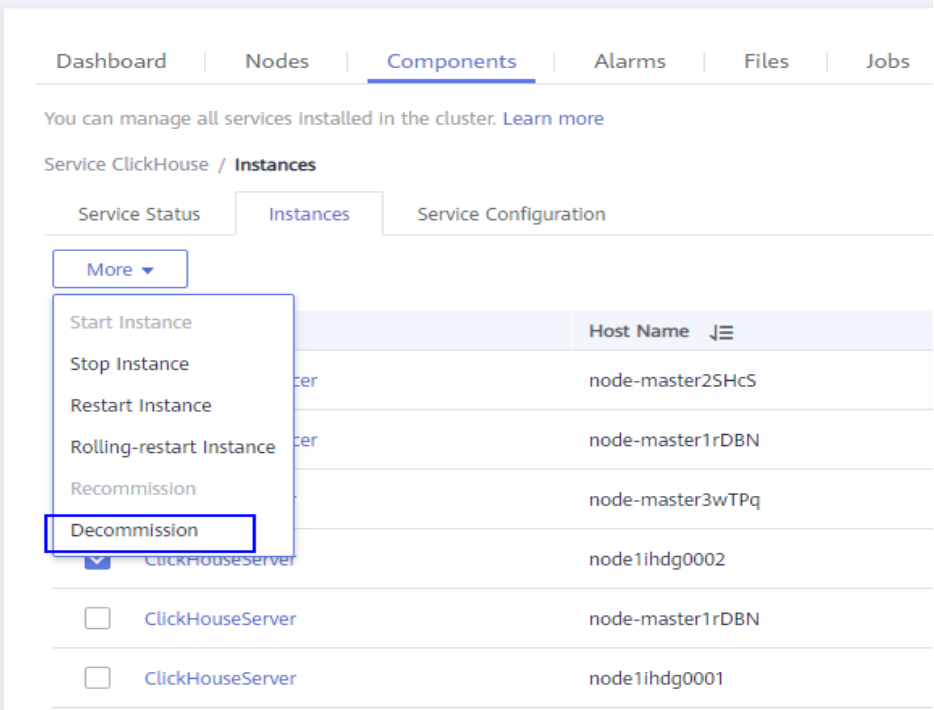
  En modo de seguridad (autenticación Kerberos activada), compruebe el valor de **https_port** que es el puerto de un nodo de instancia de ClickHouseServer.

  En el modo común (la autenticación Kerberos está deshabilitada), compruebe el valor de **http_port** que es el puerto de un nodo de instancia de ClickHouseServer.

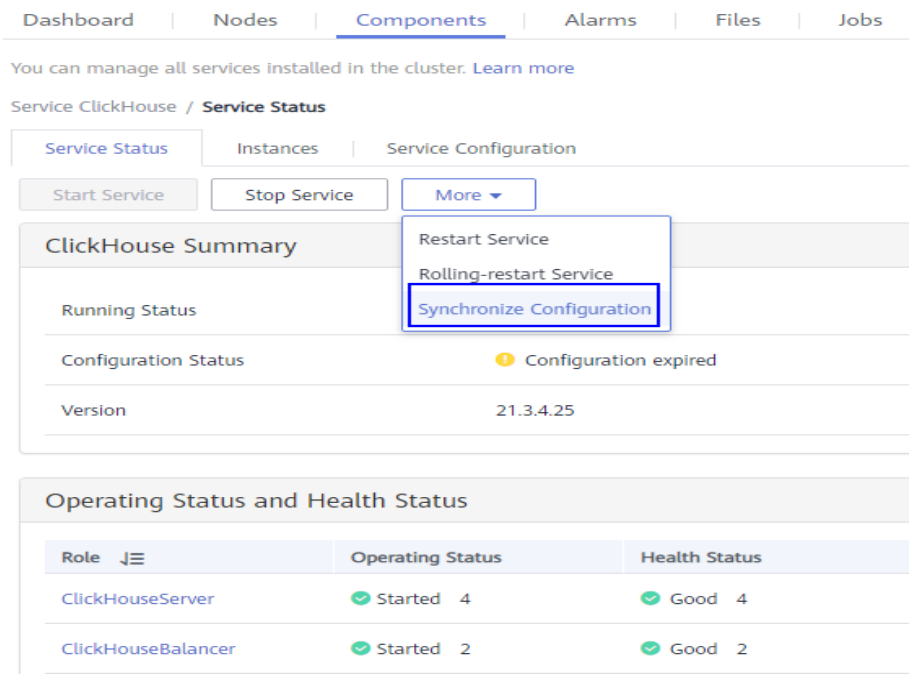
- **ck_user** indica el usuario ClickHouse creado, que debe estar enlazado a un rol con el permiso de administrador de ClickHouse. Para obtener más información sobre cómo crear un usuario y un rol, consulte **Creación de un usuario** y **Gestión de roles** respectivamente.

Paso 2 Inicie sesión en la consola MRS y haga clic en el nombre del clúster para ir a la página de detalles del clúster.

Paso 3 Haga clic en la pestaña **Components** y haga clic en **ClickHouse**. A continuación, cambie a **Instances** y seleccione las instancias del **ClickHouseServer** que desea eliminar, haga clic en **More** y seleccione **Decommission**.



Paso 4 Haga clic en la pestaña **Components** y haga clic en **ClickHouse**. A continuación, haga clic en **More** y seleccione **Synchronize Configuration**.



Paso 5 Haga clic en la pestaña **Nodes** y haga clic en el nodo de instancia ClickHouseServer que se ha dado de baja.

Paso 6 En la página ECS, haga clic en **Stop**. En el cuadro de diálogo que se muestra, seleccione **Forcibly stop the preceding ECSs** y haga clic en **Yes**.

Paso 7 Vuelva a la consola MRS, haga clic en la pestaña **Nodes**, busque la fila que contiene el grupo de nodos de destino y haga clic en **Scale In** en la columna **Operation** para ir a la página **Scale In**.

Paso 8 Establezca **Scale-In Type** en **Specific node** y seleccione el nodo que desea eliminar.

Paso 9 Seleccione **I understand the consequences of performing the scale-in operation**. Haga clic en **OK**.

Paso 10 Haga clic en la pestaña **Components** y compruebe si cada componente es normal. Si algún componente es anormal, espere de 5 a 10 minutos y vuelva a comprobar el estado del componente. Si el fallo persiste, póngase en contacto con el soporte técnico de Huawei Cloud.

Paso 11 Haga clic en la pestaña **Alarms** y compruebe si hay alarmas de excepción. Si hay alarmas de excepción, elimínelas antes de realizar otras operaciones.

----Fin

3.5.4 Gestión de un host (Nodo)

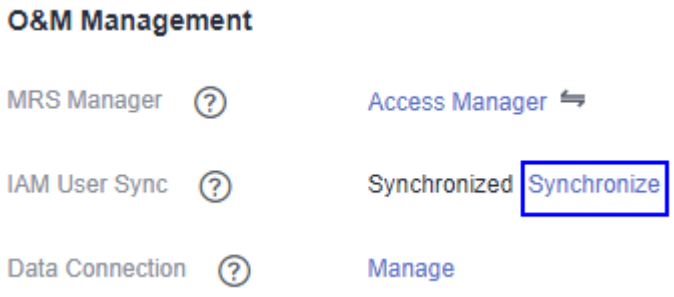
Escenario

Para comprobar un host (nodo) anormal o defectuoso, debe detener todos los roles de host en MRS. Para recuperar los servicios del host después de corregir el error del host, reinicie todos los roles.

Prerrequisitos

Ha sincronizado los usuarios de IAM. (En la página **Dashboard**, haga clic en **Synchronize** en el lado derecho de **IAM User Sync** para sincronizar usuarios de IAM.)

Figura 3-23 Sincronización de usuarios de IAM



Procedimiento

Paso 1 En la página de detalles de MRS, haga clic en **Nodes**.

Paso 2 Despliegue la información del grupo de nodos y active la casilla de verificación del nodo de destino.

Paso 3 Seleccione **Node Operation** > **Start All Roles** o **Stop All Roles** para realizar la operación requerida.

----Fin

3.5.5 Aislamiento de un host

Escenario

Si se detecta que un host es anormal o defectuoso, que afecta al rendimiento del clúster o impide que se proporcionen servicios, puede excluir temporalmente ese host de los nodos disponibles en el clúster. De esta manera, el cliente puede acceder a otros nodos disponibles. En los escenarios en los que se van a instalar parches en un clúster, también puede excluir un nodo especificado de la instalación de parches.

Puede aislar un host manualmente en MRS según los requisitos de servicio reales o el plan de O&M. Solo se pueden aislar nodos que no sean de gestión.

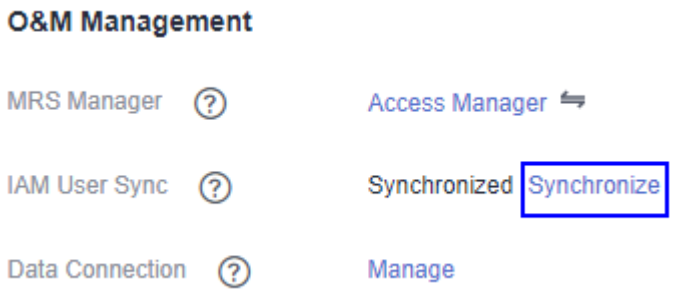
Impacto en el sistema

- Después de aislar un host, se detendrán todas las instancias de rol en el host. No puede iniciar, detener ni configurar el host ni ninguna instancia del host.
- Después de aislar un host, no se pueden recopilar ni mostrar estadísticas del estado de supervisión y los datos indicadores del hardware y las instancias del host.

Prerrequisitos

Tiene usuarios de IAM sincronizados. (Para sincronizar usuarios de IAM, en la página de pestaña **Dashboard**, haga clic en **Synchronize** junto a **IAM User Sync**.)

Figura 3-24 Sincronización de usuarios de IAM



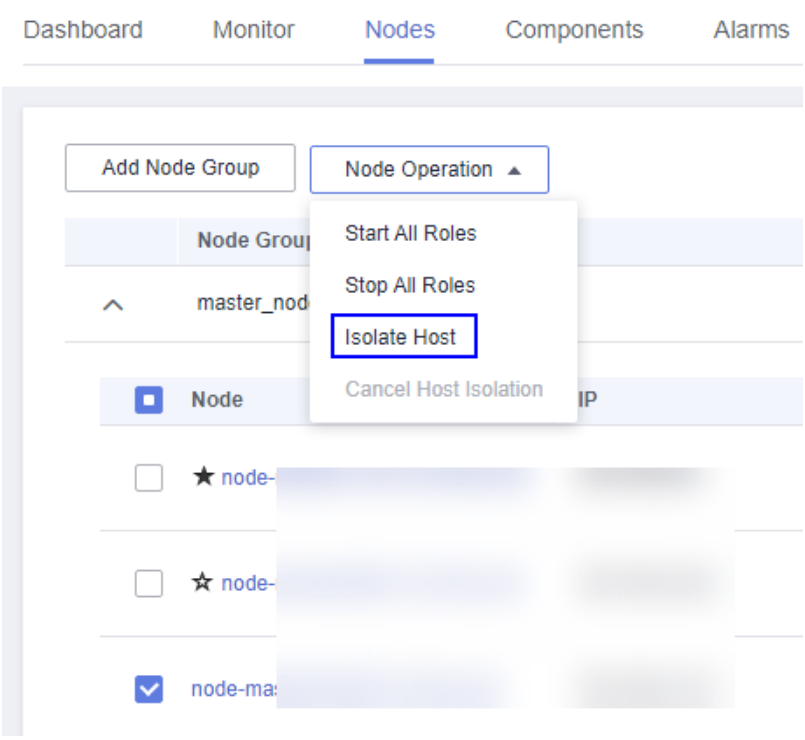
Procedimiento

Paso 1 En la página de detalles de MRS, haga clic en **Nodes**.

Paso 2 Despliegue la información del grupo de nodos y active la casilla de verificación del host de destino.

Paso 3 Elija **Node Operation** > **Isolate Host**.

Figura 3-25 Aislamiento de un host



Paso 4 Confirme la información sobre el host que se va a aislar y haga clic en **OK**.

Cuando se muestre **Operation successful**, haga clic en **Finish**. El host se aísla correctamente y el valor de **Operating Status** se convierte en **Isolated**.

NOTA

Para hosts aislados, puede cancelar el aislamiento y agregarlos de nuevo al clúster. Para obtener más información, consulte **Cancelación del aislamiento del host**.

----Fin

3.5.6 Cancelación del aislamiento del host

Escenario

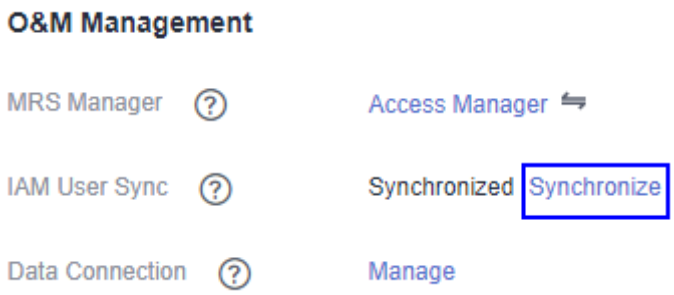
Después de que se haya manejado la excepción o la falla de un host, debe cancelar el aislamiento del host para su uso correcto.

Puede cancelar el aislamiento de un host en MRS.

Prerrequisitos

- El host se encuentra en el estado **Isolated**.
- Se ha rectificado la excepción o falla del host.
- Tiene usuarios de IAM sincronizados. (En la página **Dashboard**, haga clic en **Synchronize** en el lado derecho de **IAM User Sync** para sincronizar usuarios de IAM.)

Figura 3-26 Sincronización de usuarios de IAM



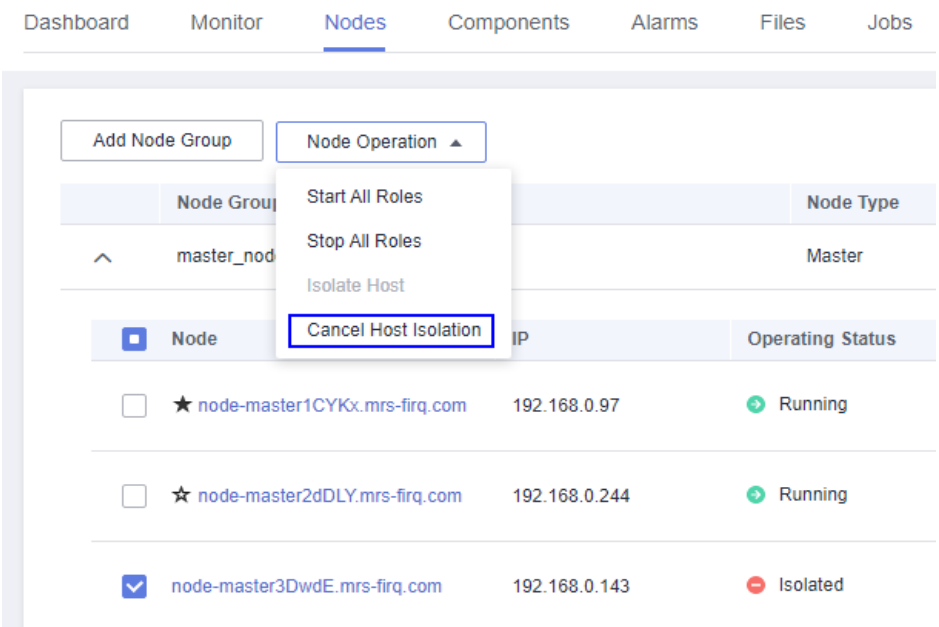
Procedimiento

Paso 1 En la página de detalles de MRS, haga clic en **Nodes**.

Paso 2 Despliegue la información del grupo de nodos y seleccione la casilla de verificación del host de destino que desea cancelar su aislamiento.

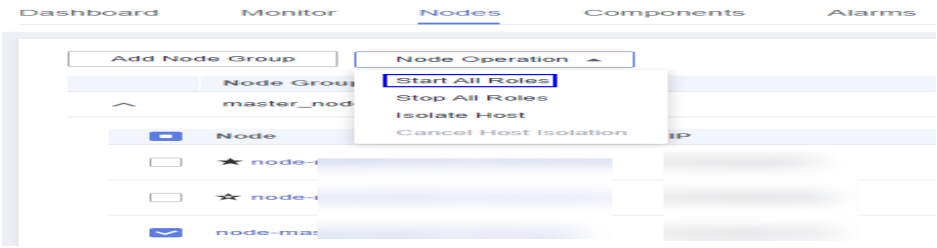
Paso 3 Elija **Node Operation** > **Cancel Host Isolation**.

Figura 3-27 Cancelación del aislamiento del host



Paso 4 Confirme la información sobre el host para el que se va a cancelar el aislamiento y haga clic en **OK**.

Cuando se muestre **Operation successful**, haga clic en **Finish**. El host se desaisla con éxito, y el valor de **Operating Status** se convierte en **Normal**.



----Fin

3.5.7 Scaling Up Master Node Specifications

As users' increasing services lead to Core node scale-out and high CPU usage, Master node specifications cannot meet user requirements and need to be scaled up. This section describes how to scale up Master node specifications.

Prerequisites

- You have checked whether the Host Security Service (HSS) is enabled. If HSS is enabled, disable the HSS monitoring on the MRS cluster before you scale up master node specifications.
- Ensure that sufficient specification resources are available throughout the steps in **Scaling Up Master Node Specifications (Step-by-Step Upgrade)**.

Use Restrictions

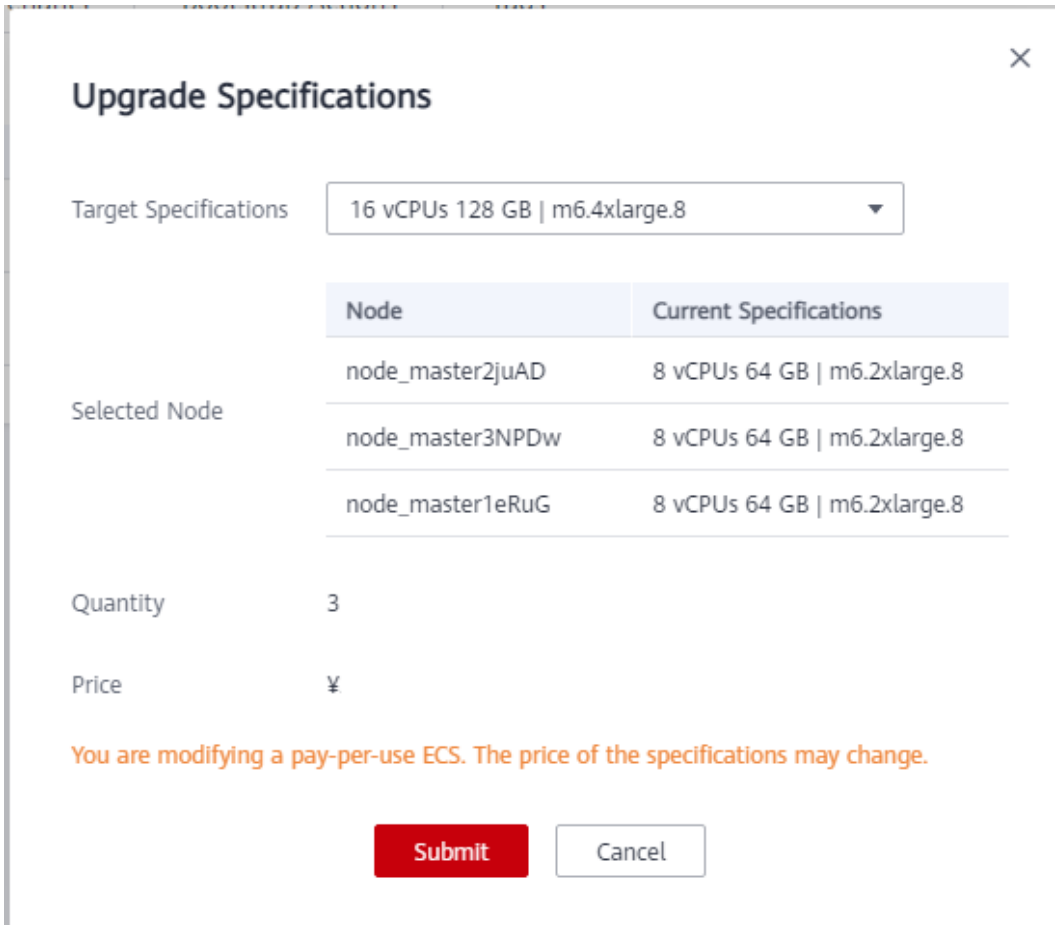
- Master nodes can be scaled up for clusters with two or more master nodes.
- The specifications of the Master node in a BMS cluster cannot be upgraded.
- For MRS 1.8.2 or later to a version earlier than MRS 3.*x* or MRS 3.1.0 or later, see **Scaling Up Master Node Specifications (One-Click Upgrade)**.
- For MRS 3.0.5 and a version earlier than MRS 1.8.2, see **Scaling Up Master Node Specifications (Step-by-Step Upgrade)**.
- Do not perform other operations on the cluster during the scale-up.

Scaling Up Master Node Specifications (One-Click Upgrade)

Paso 1 Log in to the MRS console.

Paso 2 In the left navigation pane, choose **Clusters** > **Active Clusters**, select the cluster for which you want to scale up Master node specifications, and click its name to switch to the cluster details page.

Paso 3 On the **Nodes** tab page, select **Scale Up Specifications** in the **Operation** column of the Master node group. The **Scale Up Master Node Specifications** page is displayed.



Paso 4 Select the target specifications and click **Submit Order**. The order has been submitted successfully.

The node specification scale-up takes some time. After the scale-up is successful, the cluster status changes to **Running**.

NOTA

- The VM to be scaled up is automatically stopped during the scale-up and started after the scale-up is complete.
- The scale-up does not automatically upgrade the memory of components due to different component usage requirements. You can adjust the memory of components as needed.

----Fin

Scaling Up Master Node Specifications (Step-by-Step Upgrade)

Preparing for Scaling Up Master Node Specifications

Paso 1 Log in to the MRS console.

Paso 2 In the left navigation pane, choose **Clusters** > **Active Clusters**, select the cluster for which you want to scale up Master node specifications, and click its name to switch to the cluster details page.

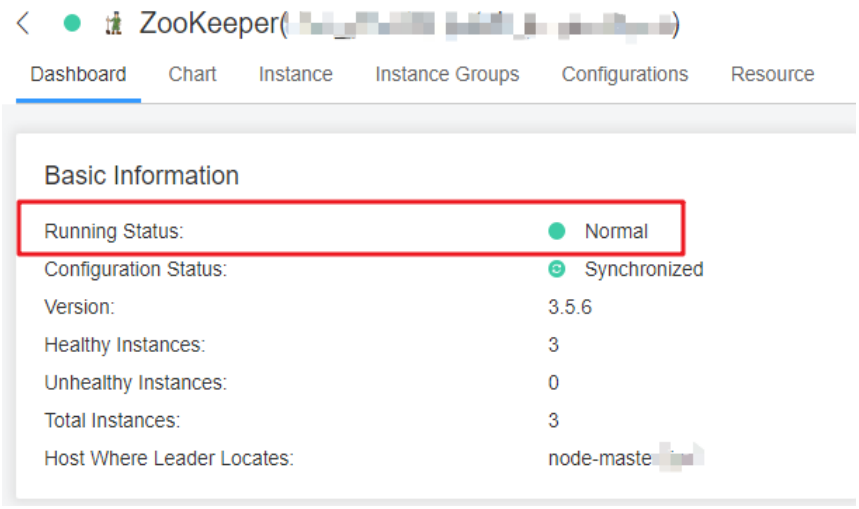
Paso 3 Ensure that the cluster status is **Running**.

Paso 4 On the **Nodes** tab page, ensure that all nodes in the cluster are in the **Running** state.

Paso 5 Log in to Manager and go to the cluster management page. For details, see **Acceso a MRS Manager (MRS 2.x o anterior)**.

Paso 6 Choose **Cluster > Services > ZooKeeper > Dashboard** and ensure that **Running Status** of the ZooKeeper service is **Normal**.

Figura 3-28 ZooKeeper service status



Paso 7 Update service parameter settings as required. For details, see **Configuración de parámetros de servicio**.

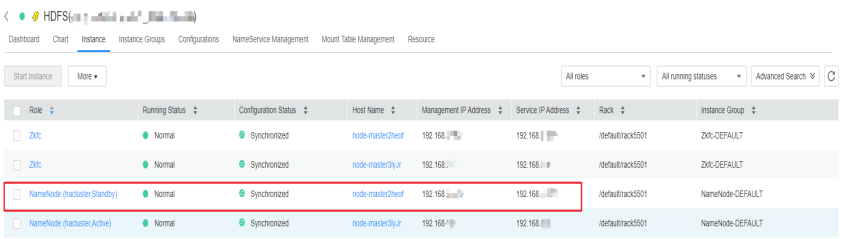
NOTA

You need to perform this step only once before scaling up the standby Master node.

Paso 8 Choose **Cluster** > **Services** > **HDFS** > **Instance**.

Paso 9 Record the business IP address of **NameNode (Standby)**. When upgrading the specifications of the active Master node, record the business IP address of **NameNode (Active)**. **Figura 3-29** shows the location of the business IP address.

Figura 3-29 Business IP address of the NameNode



NOTA

Only when the cluster is an analysis cluster, you can perform **Paso 8** to **Paso 9** to record the IP addresses of the active and standby nodes.

Paso 10 On the upper right of the Manager page, check the number next to the  icon. If the number is 0, there is no running tasks in the cluster.

Paso 11 Click **Hosts**. If the cluster is an analysis cluster, select the checkbox of the host corresponding to the business IP address of the **NameNode** recorded in **Paso 9**. If the cluster is a streaming cluster, you do not need to distinguish the active and standby nodes. You only need to choose hosts for the scale-up.

Paso 12 Choose **More** > **Stop All Instances** and wait until all instances are stopped.

NOTA

- When the node where Manager resides is scaled up, Manager may not be accessed due to an active/standby switchover. It is a normal phenomenon. Try to log in to Manager later. If the login fails for a long time, contact O&M personnel.
- After all roles are stopped, the following alarms may be generated. After the scale-up of Master node specifications is complete and all roles are started, the alarms are automatically cleared.
  - **ALM-12006 Falla de nodo**
  - **ALM-12010 Interrupción del latido del corazón de Manager entre los nodos activo y en espera**
  - **ALM-12039 Bases de datos de OMS activas/en espera no sincronizadas**
  - **ALM-14000 Servicio HDFS no disponible**
  - **ALM-14010 El servicio NameService es anormal**
  - **ALM-14012 El JournalNode no está sincronizado**
  - **ALM-16004 Servicio Hive no disponible**
  - **ALM-18000 Servicio de Yarn no disponible**
  - **ALM-19000 Servicio HBase no disponible**
  - **ALM-20002 Servicio de Hue no disponible**
  - **ALM-27001 DBService no disponible**
  - **ALM-27003 La interrupción del latido del corazón entre los nodos activo y en espera de DBService**
  - **ALM-27004 Incoherencia de datos entre DBServices activos y en espera**
  - **ALM-43001 Servicio Spark2x no disponible**

----Fin

Scaling Up Master Node Specifications

Paso 1 Log in to the MRS console.

Paso 2 In the left navigation pane, choose **Clusters** > **Active Clusters**, select the cluster for which you want to scale up Master node specifications, and click its name to switch to the cluster details page.

Paso 3 On the **Nodes** tab page, select **Scale Up Specifications** in the **Operation** column of the Master node group.

Paso 4 Select the target specifications and click **Next**.

NOTA

Ensure that target specification resources are sufficient. Otherwise, the active node cannot be scaled up.

Paso 5 On the **Confirm** page that is displayed, confirm the target node specifications and fees and click **OK**.

Paso 6 Ensure that all services on the standby Master node have been stopped. For operation details, refer to **Paso 1** to **Paso 12** in the **Preparing for Scaling Up Master Node Specifications** part. On the **Scale Up Master Node Specifications** page, select **Are you sure you have stopped all services on the standby Master node?** and **If not all services are stopped before the scale-up, data saving failure or data damage may occur.** and click **Submit Order**.

Paso 7 On the **Warning** page that is displayed, confirm again that all services on the standby Master node are stopped and click **OK** to start scaling up the specifications of the standby Master node.

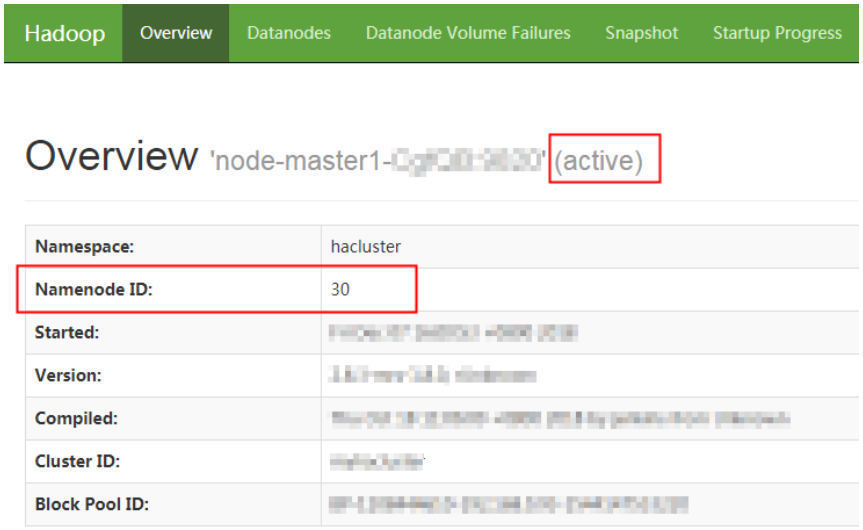
The node specification scale-up takes some time. Please wait. After the scale-up is successful, the cluster status changes to **Scaled-up-first**. Otherwise, contact O&M personnel.

Paso 8 After the standby Master node has been scaled up successfully, start all services and set parameters on the standby Master node by referring to **Paso 1** to **Paso 11** in the **Operations After the Master Node Specifications Scale-up** part.

Paso 9 After the services on the standby Master node are started, perform an active/standby NameNode switchover. Perform this step only for an analysis cluster and skip this step for a streaming cluster.

1. Access the NameNode web UI of the active and standby nodes separately. For details about how to access the NameNode web UI, see **Paso 11**.
2. In the navigation bar on the NameNode web UI, choose **Overview** and record the NameNode IDs of the active and standby nodes. Do not close the page after recording.

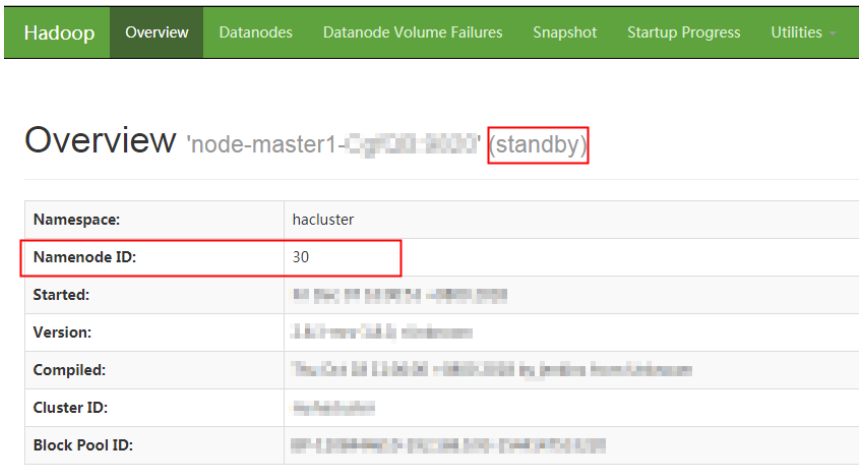
Figura 3-30 NameNode ID of the active node



3. Log in to the ECS of any Master node and run the following command to configure environment variables:
   ```
   source /opt/Bigdata/client/bigdata_env
   ```
4. If the Kerberos authentication is enabled for the current cluster, run the following command to authenticate the user. If the Kerberos authentication is disabled for the current cluster, skip this step.
   ```
   kinit MRS cluster user
   ```
   For example, **kinit admin**.

5. Run the following command to perform an active/standby NameNode switchover:
```
hdfs haadmin -failover <NameNode ID of the active node> <NameNode ID of the standby node>
```
6. Go to the NameNode web UI page that is not closed in **Paso 9.2** and refresh the page. You can view that the active/standby NameNode switchover is complete.

Figura 3-31 NameNode



Paso 10 Stop all services on the active Master node by referring to **Paso 1** to **Paso 12** in the **Preparing for Scaling Up Master Node Specifications** part.

Paso 11 On the **Scale Up Master Node Specifications** page, select **I confirm that all services on the standby Master node have been started.** and **I confirm that all services on the active Master node have been stopped**, and click **Submit**.

Paso 12 On the **Confirm** page that is displayed, confirm again that all services on the active Master node are stopped and click **OK** to start scaling up the specifications of the active Master node.

The node specification scale-up takes some time. Please wait. After the scale-up is successful, the cluster status changes to **Scaled-up-success**. Otherwise, contact O&M personnel.

Paso 13 Start all services and set parameters on the active Master node by referring to **Paso 1** to **Paso 11** in the **Operations After the Master Node Specifications Scale-up** part.

Paso 14 On the **Scale Up Master Node Specifications** page, select **Are you sure you have started all services on the active Master node?** and click **OK** to complete the scale-up.

----Fin

Operations After the Master Node Specifications Scale-up

Paso 1 Log in to Manager and go to the cluster management page. For details, see **Acceso a MRS Manager (MRS 2.x o anterior)**.

Paso 2 Click **Hosts**. Check basic information about the host corresponding to the business IP address of the NameNode recorded in **Paso 9** in the **Preparing for Scaling Up Master Node Specifications** part. If the **Running Status** is **Good** and **Disk**, **Memory**, and **CPU** have values, perform **Paso 9**. If any of the preceding conditions is not met, go to the next step.

Paso 3 Log in to the standby Master node remotely. For details, see **Inicio de sesión en un ECS**.

Paso 4 Run the following command to switch to user **omm**:


```
su - omm
```

Paso 5 Run the following command to start the Agent:

```
sh /opt/Bigdata/nodeagent/bin/start-agent.sh
```

Paso 6 Run the following command to check whether the Agent is started successfully:

```
jps | grep NodeAgent
```

Paso 7 Log in to Manager and go to the cluster management page. For details, see **Acceso a MRS Manager (MRS 2.x o anterior)**.

Paso 8 Click **Hosts**. Check basic information about the host corresponding to the business IP address of the NameNode recorded in **Paso 9** in the **Preparing for Scaling Up Master Node Specifications** part to ensure that **Running Status** is **Good** and **Disk**, **Memory**, and **CPU** have values.

NOTA

It may take 3 minutes until the host status is normal after the Agent is started successfully. Please wait. If the host status is abnormal for a long time, contact O&M personnel.

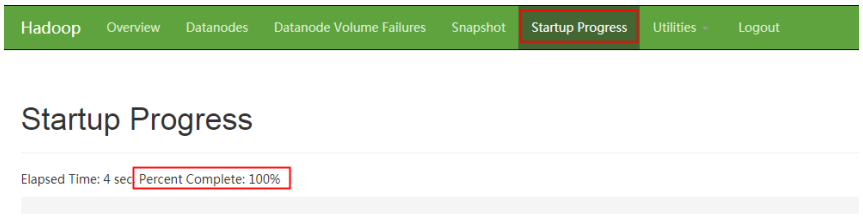
Paso 9 On the Manager page, click **Hosts** and select the checkbox of the host corresponding to the business IP address of the NameNode recorded in **Paso 9** in the **Preparing for Scaling Up Master Node Specifications** part.

Paso 10 Choose **More** > **Start All Instances** and wait until all instances are started.

Paso 11 Access the NameNode web UI and check the NameNode startup status.

1. On FusionInsight Manager, choose **Cluster > Services > HDFS > Dashboard**.
2. In the **HDFS Summary** column, click **NameNode** of the active or standby node that has been scaled up on the right of **NameNode Web UI**.
3. Go to the **NameNode Web UI** page, choose **Startup Progress** in the navigation bar. After ensuring that **Percent Complete** is displayed as 100%, go to the next step, as shown in **Figura 3-32**.

Figura 3-32 NameNode startup status



NOTA

Perform **Paso 11** for an analysis cluster and skip this step for a streaming cluster.

----Fin

3.5.8 Synchronizing Disk Information

To obtain the latest EVS disk status, you need to synchronize disk information on the MRS console. This function updates the disk information in the cluster.

Background

If the information displayed on the console is not the actual disk information or "Data disk: --(Synchronize disk information)" is displayed in the node list, you can use this function to update disk information.

Constraints

- Only cloud disk information can be synchronized.
- If disk information is being synchronized, the cluster cannot be scaled or upgraded.

Procedure

Paso 1 On the MRS details page, click **Nodes**.

Paso 2 Click **Synchronize Disk Info**.

Wait until "Disk information synchronization request issued successfully." is displayed in the upper right corner of the page.

----Fin

3.6 Gestión de trabajo

3.6.1 Introducción a los trabajos de MRS

Un trabajo MRS es la plataforma de ejecución de programas de MRS. Se utiliza para procesar y analizar datos de usuario. Después de crear un trabajo, toda la información del trabajo se muestra en la página de pestaña **Jobs**. Puede ver una lista de todos los trabajos y crear y gestionar trabajos. Si la pestaña **Jobs** no se muestra en la página de detalles del clúster, envíe un trabajo en segundo plano.

Las fuentes de datos procesadas por MRS son de OBS o HDFS. OBS es un servicio de almacenamiento basado en objetos que le proporciona capacidades de almacenamiento de datos masivas, seguras, confiables y rentables. MRS puede procesar datos en OBS directamente. Puede ver, gestionar y usar datos utilizando la página web de la plataforma de control de gestión o el cliente de OBS. Además, puede utilizar las API de REST de forma independiente o integrar las API en aplicaciones de servicio para gestionar y acceder a los datos.

Antes de crear trabajos, cargue los datos locales en OBS para que MRS calcule y analice. MRS permite exportar datos de OBS a HDFS para computación y análisis. Después de completar el análisis y la computación, puede almacenar los datos en HDFS o exportarlos a OBS. HDFS y OBS también pueden almacenar los datos comprimidos en el formato **bz2** o **gz**.

Categoría

Un clúster de MRS permite crear y gestionar los siguientes trabajos: Si un clúster en estado **Running** no puede crear un trabajo, compruebe el estado de los componentes relacionados en la página de gestión del clúster. Para obtener más información, consulte **Consulta y personalización de métricas de monitoreo de clústeres**.

- MapReduce: proporciona la capacidad de procesar datos masivos de forma rápida y paralela. Es un modo de procesamiento de datos distribuido y entorno de ejecución. MRS apoya la presentación de los programas de JAR de MapReduce.
- Spark: un marco de computación en memoria distribuido. MRS admite trabajos de SparkSubmit, Spark Script y Spark SQL.
  - SparkSubmit: Puede enviar los programas JAR y Python de Spark, ejecutar la aplicación de Spark y calcular y procesar datos de usuario.
  - SparkScript: Puede enviar los scripts SparkScript y ejecutar por lotes sentencias de Spark SQL.
  - Spark SQL: Puede usar sentencias de Spark SQL (similar a las sentencias SQL) para consultar y analizar datos de usuario en tiempo real.
- Hive: un almacén de datos de código abierto basado en Hadoop. MRS le permite enviar scripts de HiveScript y ejecutar sentencias SQL de Hive.
- Flink: proporciona un motor de procesamiento de big data distribuido que puede realizar cálculos con estado sobre flujos de datos tanto finitos como infinitos.

Lista de trabajos

Las tareas se muestran en orden cronológico de forma predeterminada en la lista de tareas, con los trabajos más recientes mostrados en la parte superior. **Tabla 3-23** describe los parámetros en la lista de trabajos.

Tabla 3-23 Parámetros de lista de trabajos

Parámetro	Descripción
Name/ID	Nombre del trabajo, que se establece cuando se crea un trabajo. ID es el identificador único de un trabajo. Después de agregar un trabajo, el sistema asigna automáticamente un valor a ID.
Username	Nombre del usuario que envía un trabajo.
Type	Se admiten los siguientes tipos de datos: ● DistCp: importación y exportación de datos ● MapReduce ● Spark ● SparkSubmit ● SparkScript ● Spark SQL ● Hive SQL ● HiveScript ● Flink **NOTA** ● Después de importar y exportar archivos en la página de pestaña **Files**, puede ver el trabajo de DistCp en la página de pestaña **Jobs**. ● Los trabajos de Spark, Hive y Flink solo se pueden agregar cuando se seleccionan los componentes de Spark, Hive y Flink durante la creación del clúster y el clúster se está ejecutando.

Parámetro	Descripción
Status	Estado del trabajo. ● Submitted ● Accepted ● Running ● Completed ● Terminated ● Abnormal
Result	Resultado de ejecución de un trabajo. ● Undefined: indica que el trabajo se está ejecutando. ● **Successful**: indica que el trabajo se ha ejecutado correctamente. ● **Killed**: indica que el trabajo se termina manualmente durante la ejecución. ● **Failed**: indica que el trabajo no se puede ejecutar. **NOTA** Una vez que un trabajo ha tenido éxito o ha fallado, no puede volver a ejecutarlo. Sin embargo, puede agregar un trabajo y establecer parámetros de trabajo para volver a enviarlo.
Queue Name	Nombre de la cola enlazada al usuario que envía el trabajo
Submitted	Hora en que se envía un trabajo.
Ended	Hora en que se completa un trabajo o se detiene manualmente.

Parámetro	Descripción
Operation	● Ver registro: Haga clic en **View Log** para ver los registros en tiempo real de los trabajos en ejecución. Para obtener más información, consulte **Consulta de la configuración de trabajos y registros**. ● Ver detalles: Haga clic en **View Details** para ver la información de configuración detallada sobre los trabajos. Para obtener más información, consulte **Consulta de la configuración de trabajos y registros**. ● Más – Detener: Puede hacer clic en **Stop** para detener un trabajo en ejecución. Para obtener más información, consulte **Detener un trabajo**. – Eliminar: Haga clic en **Delete** para eliminar un trabajo. Para obtener más información, consulte **Eliminación de un trabajo**. – Ver resultado: Haga clic en **View Result** para ver los resultados de ejecución de los trabajos de SparkSQL y SparkScript cuyo estado es de **Completed** y el resultado de **Successful**. **NOTA** ● No se puede restaurar un trabajo eliminado. Por lo tanto, tenga cuidado al eliminar un trabajo. ● Si decide guardar los registros de trabajos en OBS o HDFS, el sistema comprime y guarda los registros en la ruta correspondiente una vez completada la ejecución del trabajo. Por lo tanto, una vez completada la ejecución de un trabajo de este tipo, el estado del trabajo sigue siendo **Running**. Una vez que el registro se ha almacenado correctamente, el estado del trabajo cambia a **Completed**. La duración del almacenamiento del registro depende del tamaño del registro y toma varios minutos.

Tabla 3-24 Descripción de íconos

Ícono	Descripción
	Seleccione un intervalo de tiempo para el envío de trabajos para filtrar los trabajos enviados en el intervalo de tiempo.
	Seleccione un resultado de ejecución de trabajo determinado de la lista desplegable para mostrar trabajos del estado. ● All statuses: Filtra todos los trabajos. ● Successful: Filtrar trabajos que se ejecutan correctamente. ● Undefined: Filtrar los trabajos que se están ejecutando. ● Killed: Filtrar trabajos que se detienen manualmente. ● Failed: Filtrar trabajos que no se pueden ejecutar.

Ícono	Descripción
	Seleccione un tipo de trabajo determinado en la lista desplegable para mostrar trabajos del tipo. ● All types ● MapReduce ● HiveScript ● Distcp ● SparkScript ● Spark SQL ● Hive SQL ● SparkSubmit ● Flink
	En el cuadro de búsqueda, busque un trabajo mediante el establecimiento de la condición de búsqueda correspondiente y haga clic en  . ● Job name. ● Job ID. ● Username. ● Queue name.
	Haga clic en  para actualizar manualmente la lista de trabajos.

Descripción del permiso de ejecución del trabajo

Para un clúster de seguridad con autenticación de Kerberos habilitada, un usuario debe sincronizar un usuario de IAM antes de enviar un trabajo en la interfaz de usuario web de MRS. Una vez completada la sincronización, el sistema MRS genera un usuario con el mismo nombre de usuario IAM. Si un usuario tiene el permiso para enviar trabajos depende de la política de IAM vinculada al usuario durante la sincronización de IAM. Para obtener más información sobre la política de envío de trabajos, consulte **Tabla 1-3** en **Sincronización de usuarios de IAM a MRS**.

Cuando un usuario envía un trabajo que implica el uso de recursos de un componente específico, como el acceso a directorios HDFS y tablas Hive, el usuario **admin** (Manager administrator) debe conceder el permiso correspondiente al usuario. A continuación, se detallan los pasos:

Paso 1 Inicie sesión en Manager como usuario **admin**.

Paso 2 Agregue el rol del componente cuyo permiso es requerido por el usuario. Para obtener más información, consulte **Creación de un rol**.

Paso 3 Cambie el grupo de usuarios al que pertenece el usuario que envía el trabajo y agregue el nuevo rol de componente al grupo de usuarios. Para obtener más información, consulte **Tareas relacionadas**.

NOTA

Después de modificar el rol de componente enlazado al grupo de usuarios al que pertenece el usuario, los permisos de rol tardan algún tiempo en surtir efecto.

----Fin

3.6.2 Ejecución de un trabajo de MapReduce

Puede enviar programas desarrollados por usted mismo a MRS para ejecutarlos y obtener los resultados. Esta sección describe cómo enviar un trabajo de MapReduce en la consola de gestión de MRS. Los trabajos de MapReduce se utilizan para enviar programas JAR para procesar rápidamente cantidades masivas de datos en paralelo y crear un entorno de procesamiento y ejecución de datos distribuidos.

Si las funciones de gestión de archivos y trabajos no se admiten en la página de detalles del clúster, envíe los trabajos en segundo plano.

Prerrequisitos

Ha cargado los paquetes de programas y archivos de datos necesarios para ejecutar trabajos en OBS o HDFS.

Antes de cargar los paquetes de programas y archivos de datos en OBS, debe crear una delegación OBS y vincularla al clúster MRS.

Enviar un trabajo en la GUI

Paso 1 Inicie sesión en la consola de MRS.

Paso 2 Elija **Clusters > Active Clusters** y seleccione un clúster en ejecución y haga clic en su nombre para cambiar a la página de detalles del clúster.

Paso 3 Si la autenticación de Kerberos está habilitada para el clúster, realice los siguientes pasos. Si la autenticación de Kerberos no está habilitada para el clúster, omita este paso.

En el área **Basic Information** de la página **Dashboard**, haga clic en **Synchronize** en el lado derecho de **IAM User Sync** para sincronizar usuarios de IAM. Para más detalles, consulte **Sincronización de usuarios de IAM a MRS**.

NOTA

- Cuando la política del grupo de usuarios al que pertenece el usuario de IAM cambia de MRS ReadOnlyAccess a MRS CommonOperations, MRS FullAccess o MRS Administrator, esperar 5 minutos hasta que la nueva política entre en vigor una vez completada la sincronización, ya que la caché **SSSD** de los nodos del clúster necesita tiempo para actualizarse. Luego, envíe un trabajo. De lo contrario, es posible que el trabajo no se envíe.
- Cuando la política del grupo de usuarios al que pertenece el usuario de IAM cambia de MRS CommonOperations, MRS FullAccess o MRS Administrator a MRS ReadOnlyAccess, esperar 5 minutos hasta que la nueva política entre en vigor una vez completada la sincronización porque la caché **SSSD** de los nodos del clúster necesita tiempo para actualizarse.

Paso 4 Haga clic en la pestaña **Jobs**.

Paso 5 Haga clic en **Create**. Se muestra la página **Create Job**.

> **NOTA**
>
> Si el nombre de usuario de IAM contiene espacios (por ejemplo, **admin 01**), no se puede crear un trabajo.

Paso 6 En **Type**, seleccione **MapReduce**. Configurar otra información del trabajo.

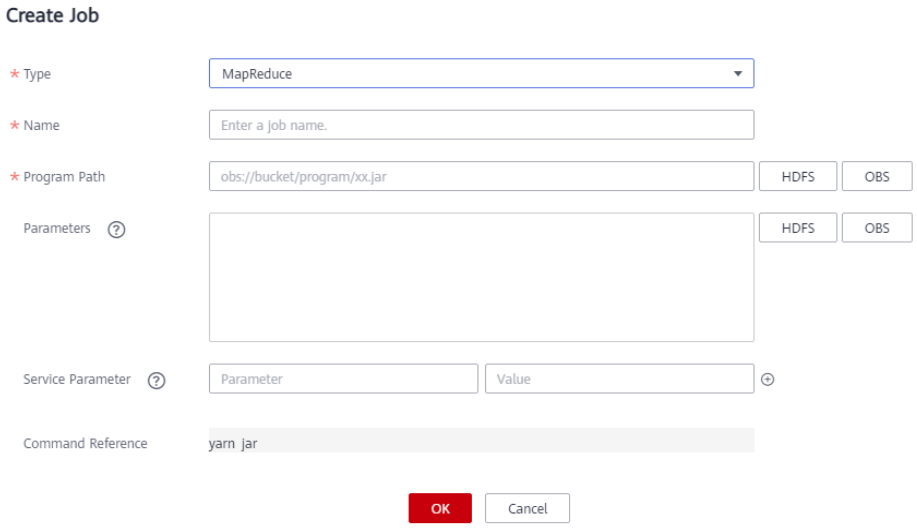


Tabla 3-25 Información de configuración del trabajo

Parámetro	Descripción
Name	Nombre del trabajo. Contiene de 1 a 64 caracteres. Solo se permiten letras, dígitos, guiones medios (-) y guiones bajos (_). **NOTA** Se recomienda establecer diferentes nombres para diferentes trabajos.
Program Path	Ruta del paquete de programa que se va a ejecutar. Se deben cumplir los siguientes requisitos: ● Contiene un máximo de 1,023 caracteres, sin incluir caracteres especiales como ;|&><'$. El valor del parámetro no puede estar vacío ni lleno de espacios. ● La ruta del programa a ejecutar se puede almacenar en HDFS u OBS. La ruta de acceso varía según el sistema de archivos. – OBS: La ruta debe comenzar con **obs://**. Ejemplo: **obs://wordcount/program/*xxx*.jar** – HDFS: La ruta debe comenzar con **/user**. Para obtener más información sobre cómo importar datos a HDFS, consulte **Importación de datos**. ● Para SparkScript y HiveScript, el camino debe terminar con **.sql**. En el caso de MapReduce, la ruta debe terminar con **.jar**. Para Flink y SparkSubmit la ruta debe terminar con **.jar** o **.py**. El **.sql**, **.jar** y el **.py** no distinguen entre mayúsculas y minúsculas.

Parámetro	Descripción
Parameters	(Opcional) Es el parámetro clave para la ejecución del programa. Múltiples parámetros están separados por espacio. Método de configuración: *Program class name Data input path Data output path* ● Nombre de la clase del programa: Es especificada por una función en su programa. MRS es responsable de la transferencia de parámetros solamente. ● Ruta de entrada de datos: Haga clic en **HDFS** u **OBS** para seleccionar una ruta o introduzca manualmente una ruta correcta. ● Ruta de salida de datos: Ingrese un directorio que no existe. El parámetro contiene un máximo de 150,000 caracteres. No puede contener caracteres especiales ;|&><'$, pero puede dejarse en blanco. **ATENCIÓN** Si introduce un parámetro con información confidencial (como la contraseña de inicio de sesión), el parámetro puede estar expuesto en la pantalla de detalles del trabajo y en la impresión del registro. Tenga cuidado al realizar esta operación.
Service Parameter	(Opcional) Se utiliza para modificar los parámetros de servicio para el trabajo. La modificación del parámetro sólo se aplica al trabajo actual. Para que la modificación surta efecto permanentemente para el clúster, siga las instrucciones en **Configuración de parámetros de servicio**. Para agregar varios parámetros, haga clic en ⊕ a la derecha. Para eliminar un parámetro, haga clic en **Delete** a la derecha. **Tabla 3-26** muestra los parámetros de configuración de servicio comunes.
Command Reference	Comando enviado en segundo plano para su ejecución cuando se envía un trabajo.

Tabla 3-26 Parámetros de **Service Parameter**

Parámetro	Descripción	Valor de ejemplo
fs.obs.access.key	ID de clave para acceder a OBS.	-
fs.obs.secret.key	Clave correspondiente al ID de clave para acceder a OBS.	-

Paso 7 Confirme la información de configuración del trabajo y haga clic en **OK**.

Después de crear el trabajo, puede gestionarlo.

----Fin

Envío de un trabajo en segundo plano

Paso 1 Inicie sesión en la consola de MRS.

Paso 2 Elija **Clusters > Active Clusters** y seleccione un clúster en ejecución y haga clic en su nombre para cambiar a la página de detalles del clúster.

Paso 3 En la página de pestaña **Nodes**, haga clic en el nombre de un nodo de Master para ir a la consola de gestión de ECS.

Paso 4 Haga clic en **Remote Login** en la esquina superior derecha de la página.

Paso 5 Introduzca el nombre de usuario y la contraseña del nodo de Master como se le solicite. El nombre de usuario es **root** y la contraseña es la que se establece durante la creación del clúster.

Paso 6 Ejecute el siguiente comando para inicializar variables de entorno:

source /opt/Bigdata/client/bigdata_env

Paso 7 Si la autenticación de Kerberos está habilitada para el clúster actual, ejecute el siguiente comando para autenticar al usuario. Si la autenticación Kerberos está deshabilitada para el clúster actual, omita este paso.

kinit ***MRS cluster user***

Ejemplo: **kinit admin**

Paso 8 Ejecute el siguiente comando para copiar el programa en el sistema de archivos de OBS al nodo de Master del clúster:

hadoop fs -Dfs.obs.access.key=AK -Dfs.obs.secret.key=SK -copyToLocal source_path.jar target_path.jar

Ejemplo: **hadoop fs -Dfs.obs.access.key=XXXX -Dfs.obs.secret.key=XXXX -copyToLocal "obs://mrs-word/program/hadoop-mapreduce-examples-XXX.jar" "/home/omm/hadoop-mapreduce-examples-XXX.jar"**

Puede iniciar sesión en OBS Console usando AK/SK. Para obtener información de AK/SK, haga clic en el nombre de usuario en la esquina superior derecha de la consola de gestión y elija **My Credentials** > **Access Keys**.

Paso 9 Ejecute el siguiente comando para enviar un trabajo de wordcount. Si es necesario leer datos de OBS o enviarlos a OBS, es necesario agregar los parámetros AK/SK.

source /opt/Bigdata/client/bigdata_env;hadoop jar execute_jar wordcount input_path output_path

Ejemplo: **source /opt/Bigdata/client/bigdata_env;hadoop jar /home/omm/hadoop-mapreduce-examples-XXX.jar wordcount -Dfs.obs.access.key=XXXX -Dfs.obs.secret.key=XXXX "obs://mrs-word/input/*" "obs://mrs-word/output/"**

En el comando anterior, el **input_path** indica una ruta para almacenar archivos de entrada de trabajo en OBS. **output_path** indica una ruta para almacenar archivos de salida de trabajo en OBS y debe establecerse en un directorio que no existe

----Fin

3.6.3 Ejecución de un trabajo de SparkSubmit o Spark

Puede enviar programas desarrollados por usted mismo a MRS para ejecutarlos y obtener los resultados. Esta sección describe cómo enviar un trabajo de Spark en la consola de MRS.

Prerrequisitos

Ha cargado los paquetes de programas y archivos de datos necesarios para ejecutar trabajos en OBS o HDFS.

Enviar un trabajo en la GUI

Paso 1 Inicie sesión en la consola de MRS.

Paso 2 Elija **Clusters > Active Clusters** y seleccione un clúster en ejecución y haga clic en su nombre para cambiar a la página de detalles del clúster.

Paso 3 Si la autenticación de Kerberos está habilitada para el clúster, realice los siguientes pasos. Si la autenticación de Kerberos no está habilitada para el clúster, omita este paso.

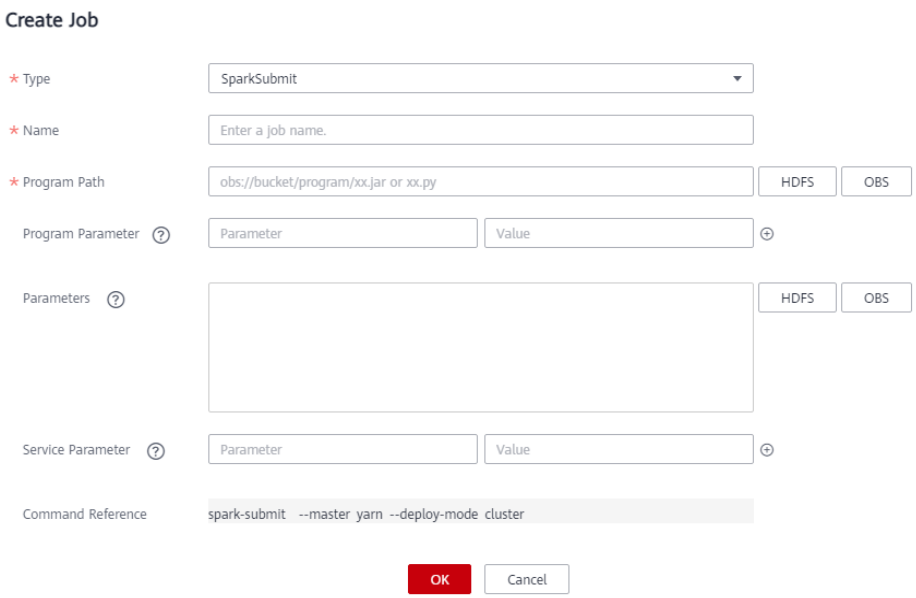
En el área **Basic Information** de la página **Dashboard**, haga clic en **Synchronize** en el lado derecho de **IAM User Sync** para sincronizar usuarios de IAM. Para más detalles, consulte **Sincronización de usuarios de IAM a MRS**.

NOTA

- Cuando la política del grupo de usuarios al que pertenece el usuario de IAM cambia de MRS ReadOnlyAccess a MRS CommonOperations, MRS FullAccess o MRS Administrator, esperar 5 minutos hasta que la nueva política entre en vigor una vez completada la sincronización, ya que la caché **SSSD** de los nodos del clúster necesita tiempo para actualizarse. Luego, envíe un trabajo. De lo contrario, es posible que el trabajo no se envíe.
- Cuando la política del grupo de usuarios al que pertenece el usuario de IAM cambia de MRS CommonOperations, MRS FullAccess o MRS Administrator a MRS ReadOnlyAccess, esperar 5 minutos hasta que la nueva política entre en vigor una vez completada la sincronización porque la caché **SSSD** de los nodos del clúster necesita tiempo para actualizarse.

Paso 4 Haga clic en la pestaña **Jobs**.

Paso 5 Haga clic en **Create**. Se muestra la página **Create Job**.



Paso 6 Configurar la información del trabajo. Establezca en **SparkSubmit** y configure otros parámetros del trabajo SparkSubmit haciendo referencia a **Tabla 3-27**

Tabla 3-27 Información de configuración del trabajo

Parámetro	Descripción
Name	Nombre del trabajo. Contiene de 1 a 64 caracteres. Solo se permiten letras, dígitos, guiones medios (-) y guiones bajos (_). **NOTA** Se recomienda establecer diferentes nombres para diferentes trabajos.
Program Path	Ruta del paquete de programa que se va a ejecutar. Se deben cumplir los siguientes requisitos: ● Contiene un máximo de 1,023 caracteres, sin incluir caracteres especiales como ;|&><'$. El valor del parámetro no puede estar vacío ni lleno de espacios. ● La ruta del programa a ejecutar se puede almacenar en HDFS u OBS. La ruta de acceso varía según el sistema de archivos. – OBS: La ruta debe comenzar con **obs://**. Ejemplo: **obs://wordcount/program/*xxx*.jar** (compatible en MRS 1.9.2 o posterior) – HDFS: La ruta debe comenzar con **/user**. Para obtener más información sobre cómo importar datos a HDFS, consulte **Importación de datos**. ● Para SparkScript y HiveScript, el camino debe terminar con **.sql**. En el caso de MapReduce, la ruta debe terminar con **.jar**. Para Flink y SparkSubmit la ruta debe terminar con **.jar** o **.py**. El **.sql**, **.jar** y el **.py** no distinguen entre mayúsculas y minúsculas.
Program Parameter	(Opcional) Se utiliza para configurar parámetros de optimización como subprocesos, memoria y vCPU para el trabajo a fin de optimizar el uso de recursos y mejorar el rendimiento de la ejecución del trabajo. **Tabla 3-28** describe los parámetros comunes de un programa en ejecución.
Parameters	(Opcional) Parámetro clave para la ejecución del programa. El parámetro es especificado por la función del programa del usuario. MRS solo es responsable de cargar el parámetro. Múltiples parámetros están separados por espacio. El parámetro contiene un máximo de 150,000 caracteres. No puede contener caracteres especiales ;|&><'$, pero puede dejarse en blanco. **ATENCIÓN** Si introduce un parámetro con información confidencial (como la contraseña de inicio de sesión), el parámetro puede estar expuesto en la pantalla de detalles del trabajo y en la impresión del registro. Tenga cuidado al realizar esta operación.

Parámetro	Descripción
Service Parameter	(Opcional) Se utiliza para modificar los parámetros de servicio para el trabajo. La modificación del parámetro sólo se aplica al trabajo actual. Para que la modificación surta efecto permanentemente para el clúster, siga las instrucciones en **Configuración de parámetros de servicio**. Para agregar varios parámetros, haga clic en ⊕ a la derecha. Para eliminar un parámetro, haga clic en **Delete** a la derecha. **Tabla 3-29** muestra los parámetros de configuración de servicio comunes. **NOTA** Si necesita ejecutar un trabajo a largo plazo, como SparkStreaming y acceder a OBS, debe usar **Service Parameter** para importar el AK/SK para acceder a OBS.
Command Reference	Comando enviado en segundo plano para su ejecución cuando se envía un trabajo.

Tabla 3-28 Parámetros del programa

Parámetro	Descripción	Valor de ejemplo
--conf	Agregue los elementos de configuración de la tarea.	spark.executor.memory=2G
--driver-memory	Establezca la memoria de ejecución del controlador.	2G
--num-executors	Establezca el número de ejecutores que se iniciarán.	5
--executor-cores	Establezca el número de núcleos del ejecutor.	2
--class	Establezca la clase principal de una tarea.	org.apache.spark.examples.SparkPi
--files	Suba archivos a una tarea. Los archivos pueden ser archivos de configuración personalizados o algunos archivos de datos de OBS o HDFS.	-
--jars	Cargue paquetes de dependencias adicionales de una tarea para agregar los paquetes de dependencias externas a la tarea.	-
--executor-memory	Establezca la memoria del ejecutor.	2G

Parámetro	Descripción	Valor de ejemplo
--conf spark-yarn.maxAppAttempts	Controle el número de reintentos de AM.	Si este parámetro se establece en **0**, no se permite volver a intentarlo. Si este parámetro se establece en **1**, se permite un reintento.

Tabla 3-29 Parámetros de **Service Parameter**

Parámetro	Descripción	Valor de ejemplo
fs.obs.access.key	ID de clave para acceder a OBS.	-
fs.obs.secret.key	Clave correspondiente al ID de clave para acceder a OBS.	-

Tabla 3-30 Job configuration information

Parámetro	Descripción
Name	Nombre del trabajo. Contiene de 1 a 64 caracteres. Solo se permiten letras, dígitos, guiones medios (-) y guiones bajos (_). **NOTA** Se recomienda establecer diferentes nombres para diferentes trabajos.
Program Path	Ruta del paquete de programa que se va a ejecutar. Se deben cumplir los siguientes requisitos: ● Contiene un máximo de 1,023 caracteres, sin incluir caracteres especiales como ;|&><'$. El valor del parámetro no puede estar vacío ni lleno de espacios. ● La ruta del programa a ejecutar se puede almacenar en HDFS u OBS. La ruta de acceso varía según el sistema de archivos. – OBS: La ruta debe comenzar con **s3a:**//. Ejemplo: **s3a:**// **wordcount/program/*xxx*.jar** – HDFS: La ruta debe comenzar con **/user**. Para obtener más información sobre cómo importar datos a HDFS, consulte **Importación de datos**. ● En el caso de SparkScript, la ruta debe terminar con **.sql**. Para MapReduce y Spark, el camino debe terminar con **.jar**. El **.sql** y el **.jar** son insensibles a mayúsculas y minúsculas.

Parámetro	Descripción
Parameters	Parámetro clave para la ejecución del programa. El parámetro es especificado por la función del programa del usuario. MRS solo es responsable de cargar el parámetro. Múltiples parámetros están separados por espacio. Método de configuración: *Package name*.*Class name* El parámetro contiene un máximo de 150,000 caracteres. No puede contener caracteres especiales ;|&><'$, pero puede dejarse en blanco. **NOTA** Al introducir un parámetro que contiene información confidencial (por ejemplo, contraseña de inicio de sesión), puede agregar un (@) de signo antes del nombre del parámetro para cifrar el valor del parámetro. Esto evita que la información sensible se mantenga en texto plano. Cuando se visualiza la información del trabajo en la consola MRS, la información confidencial se muestra como *****. Ejemplo: **username=admin @password=admin_123**
Import From	Ruta para entrada de datos Los datos se pueden almacenar en HDFS u OBS. La ruta de acceso varía según el sistema de archivos. ● OBS: La ruta debe comenzar con **s3a://**. ● HDFS: La ruta debe comenzar con **/user**. Para obtener más información sobre cómo importar datos a HDFS, consulte **Importación de datos**. El parámetro contiene un máximo de 1,023 caracteres, excluidos caracteres especiales como ;|&>,<'$, y puede dejarse en blanco.
Export To	Ruta de salida de datos **NOTA** ● Al establecer este parámetro, seleccione **OBS** o **HDFS**. Seleccione un directorio de archivos o ingrese manualmente un directorio de archivos y haga clic en **OK**. ● Si agrega el programa de ejemplo **hadoop-mapreduce-examples-x.x.x.jar** o un programa similar a **hadoop-mapreduce-examples-x.x.x.jar**, introduzca un directorio que no exista. Los datos se pueden almacenar en HDFS u OBS. La ruta de acceso varía según el sistema de archivos. ● OBS: La ruta debe comenzar con **s3a://**. ● HDFS: La ruta debe comenzar con **/user**. El parámetro contiene un máximo de 1,023 caracteres, excluidos caracteres especiales como ;|&>,<'$, y puede dejarse en blanco.

Parámetro	Descripción
Log Path	Ruta de acceso para almacenar registros de trabajos que registran el estado de ejecución del trabajo. Los datos se pueden almacenar en HDFS u OBS. La ruta de acceso varía según el sistema de archivos. ● OBS: La ruta debe comenzar con **s3a://**. ● HDFS: La ruta debe comenzar con **/user**. El parámetro contiene un máximo de 1,023 caracteres, excluidos caracteres especiales como ;|&>,<'$, y puede dejarse en blanco.

Paso 7 Confirme la información de configuración del trabajo y haga clic en **OK**.

Después de crear el trabajo, puede gestionarlo.

----Fin

Envío de un trabajo en segundo plano

Paso 1 Cree un usuario para enviar trabajos. Para obtener más información, consulte **Creación de un usuario**.

En este ejemplo, se ha creado un usuario máquina-máquina y se han asignado correctamente al usuario los grupos de usuarios (**hadoop** y **supergroup**), el grupo principal (**supergroup**) y los permisos de rol (**System_administrator** y **default**).

Paso 2 Descargue la credencial de autenticación.

- Para clústeres de MRS 3.*x* o posterior, inicie sesión en FusionInsight Manager y elija **System** > **Permission** > **User**. En la columna **Operation** del usuario recién creado, elija **More** > **Download Authentication Credential**.
- Para los clústeres cuya versión es anterior a MRS 3.*x*, inicie sesión en MRS Manager y elija **System** > **Manage User**. En la columna **Operation** del usuario recién creado, elija **More** > **Download Authentication Credential**.

Paso 3 Suba archivos de JAR relacionados con el trabajo al clúster. En este ejemplo, se utiliza el archivo de JAR de ejemplo construido en Spark. Se almacena en **$SPARK_HOME/examples/jars**.

Paso 4 Suba la credencial de autenticación del usuario creado en **Paso 2** al directorio **/opt** del clúster y ejecuta el siguiente comando para descomprimir la credencial:

tar –xvf MRSTest _*xxxxxx*_keytab.tar

Obtendrás dos archivos: **user.keytab** y **krb5.conf**.

Paso 5 Antes de realizar operaciones en el clúster, ejecute los siguientes comandos:

source /opt/Bigdata/client/bigdata_env

cd $SPARK_HOME

Paso 6 Ejecute el siguiente comando para ejecutar el trabajo de Spark:

./bin/spark-submit --master yarn --deploy-mode client --conf spark.yarn.principal=MRSTest --conf spark.yarn.keytab=/opt/user.keytab --class

org.apache.spark.examples.SparkPi examples/jars/spark-examples_2.11-2.3.2-mrs-2.0.jar 10

Descripción de parámetros:

1. Capacidad informática de Yarn, que especifica que el trabajo se envía en modo de cliente.
2. Elemento de configuración del trabajo de Spark. El archivo de autenticación y el nombre de usuario se transfieren aquí.
3. **spark.yarn.principal**: usuario creado en paso 1
4. **spark.yarn.keytab**: archivo keytab usado para la autenticación
5. *xx*.**jar**: archivo JAR utilizado por el trabajo

----Fin

3.6.4 Ejecución de un trabajo de HiveSQL

Puede enviar programas desarrollados por usted mismo a MRS para ejecutarlos y obtener los resultados. Esta sección describe cómo enviar un trabajo de HiveSQL en la consola de gestión de MRS. Los trabajos de HiveSQL se utilizan para enviar sentencias SQL y archivos de script para consultas y análisis de datos. Se admiten tanto las sentencias SQL como los scripts. Si las sentencias SQL contienen información confidencial, utilice Script para enviarlas.

Prerrequisitos

Ha cargado los paquetes de programas y archivos de datos necesarios para ejecutar trabajos en OBS o HDFS.

Enviar un trabajo en la GUI

Paso 1 Inicie sesión en la consola de MRS.

Paso 2 Elija **Clusters > Active Clusters** y seleccione un clúster en ejecución y haga clic en su nombre para cambiar a la página de detalles del clúster.

Paso 3 Si la autenticación de Kerberos está habilitada para el clúster, realice los siguientes pasos. Si la autenticación de Kerberos no está habilitada para el clúster, omita este paso.

En el área **Basic Information** de la página **Dashboard**, haga clic en **Synchronize** en el lado derecho de **IAM User Sync** para sincronizar usuarios de IAM. Para más detalles, consulte **Sincronización de usuarios de IAM a MRS**.

NOTA

- Cuando la política del grupo de usuarios al que pertenece el usuario de IAM cambia de MRS ReadOnlyAccess a MRS CommonOperations, MRS FullAccess o MRS Administrator, esperar 5 minutos hasta que la nueva política entre en vigor una vez completada la sincronización, ya que la caché **SSSD** de los nodos del clúster necesita tiempo para actualizarse. Luego, envíe un trabajo. De lo contrario, es posible que el trabajo no se envíe.
- Cuando la política del grupo de usuarios al que pertenece el usuario de IAM cambia de MRS CommonOperations, MRS FullAccess o MRS Administrator a MRS ReadOnlyAccess, esperar 5 minutos hasta que la nueva política entre en vigor una vez completada la sincronización porque la caché **SSSD** de los nodos del clúster necesita tiempo para actualizarse.

Paso 4 Haga clic en la pestaña **Jobs**.

Paso 5 Haga clic en **Create**. Se muestra la página **Create Job**.

Paso 6 Configurar la información del trabajo. Establecer **Type** en **HiveSql** y configurar la información del trabajo de HiveSQL haciendo referencia a **Tabla 3-31**.

Tabla 3-31 Información de configuración del trabajo

Parámetro	Descripción
Name	Nombre del trabajo. Contiene de 1 a 64 caracteres. Solo se permiten letras, dígitos, guiones medios (-) y guiones bajos (_). **NOTA** Se recomienda establecer diferentes nombres para diferentes trabajos.
SQL Type	Tipo de envío de la sentencia SQL ● SQL ● Script
SQL Statement	Este parámetro solo es válido cuando **SQL Type** está establecido en **SQL**. Escriba la sentencia SQL que se va a ejecutar y, a continuación, haga clic en **Check** para comprobar si la sentencia SQL es correcta. Si desea enviar y ejecutar varias sentencias al mismo tiempo, use punto y coma (;) para separarlas.
SQL File	Este parámetro solo es válido cuando **SQL Type** está establecido en **Script**. La ruta del archivo SQL que se va a ejecutar debe cumplir con los siguientes requisitos: ● Contiene un máximo de 1,023 caracteres, sin incluir caracteres especiales como ;|&><'$. El valor del parámetro no puede estar vacío ni lleno de espacios. ● La ruta del programa a ejecutar se puede almacenar en HDFS u OBS. La ruta de acceso varía según el sistema de archivos. – OBS: La ruta debe comenzar con **obs://**. Ejemplo: **obs://wordcount/program/*xxx*.jar** – HDFS: La ruta debe comenzar con **/user**. Para obtener más información sobre cómo importar datos a HDFS, consulte **Importación de datos**. ● Para SparkScript y HiveScript, el camino debe terminar con **.sql**. En el caso de MapReduce, la ruta debe terminar con **.jar**. Para Flink y SparkSubmit la ruta debe terminar con **.jar** o **.py**. El **.sql**, **.jar** y el **.py** no distinguen entre mayúsculas y minúsculas. **NOTA** A file path on OBS can start with **obs://**. To submit jobs in this format, you need to configure permissions for accessing OBS. ● If the OBS permission control function is enabled during cluster creation, you can use the **obs://** directory without extra configuration. ● If the OBS permission control function is not enabled or is not supported when you create a cluster, configure the function.

Parámetro	Descripción
Program Parameter	(Opcional) Se utiliza para configurar parámetros de optimización como subprocesos, memoria y vCPU para el trabajo a fin de optimizar el uso de recursos y mejorar el rendimiento de la ejecución del trabajo. **Tabla 3-32** describe los parámetros comunes de un programa en ejecución.
Service Parameter	(Opcional) Se utiliza para modificar los parámetros de servicio para el trabajo. La modificación del parámetro sólo se aplica al trabajo actual. Para que la modificación surta efecto permanentemente para el clúster, siga las instrucciones en **Configuración de parámetros de servicio**. Para agregar varios parámetros, haga clic en  a la derecha. Para eliminar un parámetro, haga clic en **Delete** a la derecha. **Tabla 3-33** muestra los parámetros de configuración de servicio comunes.
Command Reference	Comando enviado en segundo plano para su ejecución cuando se envía un trabajo.

Tabla 3-32 Parámetros del programa

Parámetro	Descripción	Valor de ejemplo
--hiveconf	La configuración del servicio Hive, por ejemplo, establece el motor de ejecución en MapReduce.	Configuración del motor de ejecución en MR: **--hiveconf "hive.execution.engine=mr"**
--hivevar	Variable personalizada, por ejemplo, ID de variable.	Configuración del ID de la variable: **--hivevar id="123" select * from test where id = ${hivevar:id}**

Tabla 3-33 Parámetros del servicio

Parámetro	Descripción	Valor de ejemplo
fs.obs.access.key	ID de clave para acceder a OBS.	-
fs.obs.secret.key	Clave correspondiente al ID de clave para acceder a OBS.	-
hive.execution.engine	Motor para ejecutar un trabajo.	● mr ● tez

Paso 7 Confirme la información de configuración del trabajo y haga clic en **OK**.

Después de crear el trabajo, puede gestionarlo.

----Fin

Envío de un trabajo en segundo plano

Paso 1 Inicie sesión en la consola de MRS.

Paso 2 Seleccione **Clusters** > **Active Clusters**, seleccione un clúster en ejecución y haga clic en su nombre para cambiar a la página de detalles del clúster.

Paso 3 En la página de pestaña **Nodes**, haga clic en el nombre de un nodo de Master para ir a la consola de gestión de ECS.

Paso 4 Haga clic en **Remote Login** en la esquina superior derecha de la página.

Paso 5 Introduzca el nombre de usuario y la contraseña del nodo de Master como se le solicite. El nombre de usuario es **root** y la contraseña es la que se establece durante la creación del clúster.

Paso 6 Ejecute el siguiente comando para inicializar variables de entorno:

source /opt/BigData/client/bigdata_env

NOTA

- Si utiliza el cliente para conectarse a una instancia múltiple de Hive específica en un escenario donde están instaladas varias instancias de Hive, ejecute el siguiente comando para cargar las variables de entorno de la instancia. De lo contrario, omita este paso. Por ejemplo, cargue las variables de entorno de la instancia Hive2.

  source /opt/BigData/client/Hive2/component_env

Paso 7 Si la autenticación de Kerberos está habilitada para el clúster actual, ejecute el siguiente comando para autenticar al usuario. Si la autenticación de Kerberos está deshabilitada para el clúster actual (modo normal), omita este paso.

kinit *MRS cluster user* (El usuario debe estar en el grupo de usuario **hive**.)

Paso 8 Ejecute el comando **beeline** para conectarse a HiveServer y ejecutar tareas.

beeline

Para los clústeres en modo normal, ejecute los siguientes comandos. Si no se especifica ningún usuario del servicio de componente, se utiliza el usuario actual del sistema operativo para iniciar sesión en HiveServer.

beeline -n *Component service user*

beeline -f *SQL files* (SQLs in the execution files)

----Fin

3.6.5 Ejecución de un trabajo de SparkSql

Puede enviar programas desarrollados por usted mismo a MRS para ejecutarlos y obtener los resultados. Esta sección describe cómo enviar un trabajo de SparkSQL en la consola de MRS. Los trabajos de SparkSQL se utilizan para consultas y análisis de datos. Se admiten tanto las

sentencias SQL como los scripts. Si las sentencias SQL incluyen información confidencial, use Spark Script para enviarlas.

Prerrequisitos

Ha cargado los paquetes de programas y archivos de datos necesarios para ejecutar trabajos en OBS o HDFS.

Enviar un trabajo en la GUI

Paso 1 Inicie sesión en la consola de MRS.

Paso 2 Elija **Clusters > Active Clusters** y seleccione un clúster en ejecución y haga clic en su nombre para cambiar a la página de detalles del clúster.

Paso 3 Si la autenticación de Kerberos está habilitada para el clúster, realice los siguientes pasos. Si la autenticación de Kerberos no está habilitada para el clúster, omita este paso.

En el área **Basic Information** de la página **Dashboard**, haga clic en **Synchronize** en el lado derecho de **IAM User Sync** para sincronizar usuarios de IAM. Para más detalles, consulte **Sincronización de usuarios de IAM a MRS**.

NOTA

- Cuando la política del grupo de usuarios al que pertenece el usuario de IAM cambia de MRS ReadOnlyAccess a MRS CommonOperations, MRS FullAccess o MRS Administrator, esperar 5 minutos hasta que la nueva política entre en vigor una vez completada la sincronización, ya que la caché **SSSD** de los nodos del clúster necesita tiempo para actualizarse. Luego, envíe un trabajo. De lo contrario, es posible que el trabajo no se envíe.
- Cuando la política del grupo de usuarios al que pertenece el usuario de IAM cambia de MRS CommonOperations, MRS FullAccess o MRS Administrator a MRS ReadOnlyAccess, esperar 5 minutos hasta que la nueva política entre en vigor una vez completada la sincronización porque la caché **SSSD** de los nodos del clúster necesita tiempo para actualizarse.

Paso 4 Haga clic en la pestaña **Jobs**.

Paso 5 Haga clic en **Create**. En la página **Create Job** mostrada, establezca **Type** en **SparkSql** y configure la información del trabajo de SparkSql haciendo referencia a **Tabla 3-34**.

Tabla 3-34 Información de configuración del trabajo

Parámetro	Descripción
Name	Nombre del trabajo. Contiene de 1 a 64 caracteres. Solo se permiten letras, dígitos, guiones medios (-) y guiones bajos (_). **NOTA** Se recomienda establecer diferentes nombres para diferentes trabajos.
SQL Type	Tipo de envío de la sentencia SQL ● SQL ● Script

Parámetro	Descripción
SQL Statement	Este parámetro solo es válido cuando **SQL Type** está establecido en **SQL**. Escriba la sentencia SQL que se va a ejecutar y, a continuación, haga clic en **Check** para comprobar si la sentencia SQL es correcta. Si desea enviar y ejecutar varias sentencias al mismo tiempo, use punto y coma (;) para separarlas.
SQL File	Este parámetro solo es válido cuando **SQL Type** está establecido en **Script**. La ruta del archivo SQL que se va a ejecutar debe cumplir con los siguientes requisitos: ● Contiene un máximo de 1,023 caracteres, sin incluir caracteres especiales como ;|&><'$. El valor del parámetro no puede estar vacío ni lleno de espacios. ● La ruta del programa a ejecutar se puede almacenar en HDFS u OBS. La ruta de acceso varía según el sistema de archivos. – OBS: La ruta debe comenzar con **obs://**. Ejemplo: **obs://wordcount/program/*xxx*.jar** – HDFS: La ruta debe comenzar con **/user**. Para obtener más información sobre cómo importar datos a HDFS, consulte **Importación de datos**. ● Para SparkScript y HiveScript, el camino debe terminar con **.sql**. En el caso de MapReduce, la ruta debe terminar con **.jar**. Para Flink y SparkSubmit la ruta debe terminar con **.jar** o **.py**. El **.sql**, **.jar** y el **.py** no distinguen entre mayúsculas y minúsculas. **NOTA** Una ruta de archivo en OBS puede comenzar con **obs://**. Para enviar trabajos en este formato, debe configurar permisos para acceder a OBS. ● Si la función de control de permisos de OBS está habilitada durante la creación del clúster, puede utilizar el directorio **obs://** sin configuración adicional. ● Si la función de control de permisos OBS no está habilitada o no se admite al crear un clúster, configure la función.
Program Parameter	(Opcional) Se utiliza para configurar parámetros de optimización como subprocesos, memoria y vCPU para el trabajo a fin de optimizar el uso de recursos y mejorar el rendimiento de la ejecución del trabajo. **Tabla 3-35** describe los parámetros comunes de un programa en ejecución.
Service Parameter	(Opcional) Se utiliza para modificar los parámetros de servicio para el trabajo. La modificación del parámetro sólo se aplica al trabajo actual. Para que la modificación surta efecto permanentemente para el clúster, siga las instrucciones en **Configuración de parámetros de servicio**. Para agregar varios parámetros, haga clic en ⊕ a la derecha. Para eliminar un parámetro, haga clic en **Delete** a la derecha. **Tabla 3-36** muestra los parámetros de configuración de servicio comunes.
Command Reference	Comando enviado en segundo plano para su ejecución cuando se envía un trabajo.

Tabla 3-35 Parámetros del programa

Parámetro	Descripción	Valor de ejemplo
--conf	Elementos de configuración de tareas que se agregarán.	spark.executor.memory=2G
--driver-memory	Memoria de ejecución de un driver.	2G
--num-executors	Número de executor que se iniciarán.	5
--executor-cores	Número de núcleos del executor.	2
--jars	Paquetes de dependencias adicionales de una tarea, que se utiliza para agregar los paquetes de dependencias externas a la tarea.	-
--executor-memory	Memoria del executor.	2G

Tabla 3-36 Parámetros del servicio

Parámetro	Descripción	Valor de ejemplo
fs.obs.access.key	ID de clave para acceder a OBS.	-
fs.obs.secret.key	Clave correspondiente al ID de clave para acceder a OBS.	-

Paso 6 Confirme la información de configuración del trabajo y haga clic en **OK**.

Después de crear el trabajo, puede gestionarlo.

----Fin

Envío de un trabajo en segundo plano

Paso 1 Cree un usuario para enviar trabajos. Para obtener más información, consulte **Creación de un usuario**.

En este ejemplo, se ha creado un usuario máquina-máquina y se han asignado correctamente al usuario los grupos de usuarios (**hadoop** y **supergrupo**), el grupo principal (**supergrupo**) y los permisos de rol (**System_administrator** y **default**).

Paso 2 Descargue la credencial de autenticación.

- Para clústeres de MRS 3.*x* o posterior, inicie sesión en FusionInsight Manager y elija **System** > **Permission** > **User**. En la columna **Operation** del usuario recién creado, elija **More** > **Download Authentication Credential**.
- Para los clústeres cuya versión es anterior a MRS 3.*x*, inicie sesión en MRS Manager y elija **System** > **Manage User**. En la columna **Operation** del usuario recién creado, elija **More** > **Download Authentication Credential**.

Paso 3 Inicie sesión en el nodo donde se encuentra el cliente Spark, cargue la credencial de autenticación de usuario creada en 2 en el directorio **/opt** del clúster y ejecute el siguiente comando para descomprimir el paquete:

tar -xvf MRSTest _*xxxxxx*_keytab.tar

Después de la descompresión, se obtienen los archivos **user.keytab** y **krb5.conf**.

Paso 4 Antes de realizar operaciones en el clúster, ejecute los siguientes comandos:

source /opt/Bigdata/client/bigdata_env

cd $SPARK_HOME

Paso 5 Abra la CLI de **spark-sql** y ejecute la siguiente sentencia SQL:

./bin/spark-sql --conf spark.yarn.principal=MRSTest --conf spark.yarn.keytab=/opt/user.keytab

Para ejecutar el archivo SQL, debe cargar el archivo SQL (por ejemplo, en el directorio **/opt/**). Después de cargar el archivo, ejecute el siguiente comando:

./bin/spark-sql --conf spark.yarn.principal=MRSTest --conf spark.yarn.keytab=/opt/user.keytab -f /opt/script.sql

----Fin

3.6.6 Ejecución de un trabajo de Flink

Puede enviar programas desarrollados por usted mismo a MRS para ejecutarlos y obtener los resultados. Esta sección describe cómo enviar un trabajo de Flink en la consola de gestión de MRS. Los trabajos de Flink se utilizan para enviar programas JAR para procesar datos de streaming.

Prerrequisitos

Ha cargado los paquetes de programas y archivos de datos necesarios para ejecutar trabajos en OBS o HDFS.

Enviar un trabajo en la GUI

Paso 1 Inicie sesión en la consola de MRS.

Paso 2 Elija **Clusters > Active Clusters** y seleccione un clúster en ejecución y haga clic en su nombre para cambiar a la página de detalles del clúster.

Paso 3 Si la autenticación de Kerberos está habilitada para el clúster, realice los siguientes pasos. Si la autenticación de Kerberos no está habilitada para el clúster, omita este paso.

En el área **Basic Information** de la página **Dashboard**, haga clic en **Synchronize** en el lado derecho de **IAM User Sync** para sincronizar usuarios de IAM. Para más detalles, consulte **Sincronización de usuarios de IAM a MRS**.

NOTA

- Cuando la política del grupo de usuarios al que pertenece el usuario de IAM cambia de MRS ReadOnlyAccess a MRS CommonOperations, MRS FullAccess o MRS Administrator, esperar 5 minutos hasta que la nueva política entre en vigor una vez completada la sincronización, ya que la caché **SSSD** de los nodos del clúster necesita tiempo para actualizarse. Luego, envíe un trabajo. De lo contrario, es posible que el trabajo no se envíe.
- Cuando la política del grupo de usuarios al que pertenece el usuario de IAM cambia de MRS CommonOperations, MRS FullAccess o MRS Administrator a MRS ReadOnlyAccess, esperar 5 minutos hasta que la nueva política entre en vigor una vez completada la sincronización porque la caché **SSSD** de los nodos del clúster necesita tiempo para actualizarse.

Paso 4 Haga clic en la pestaña **Jobs**.

Paso 5 Haga clic en **Create**. Se muestra la página **Create Job**.

Paso 6 Ajusta **Type** a **Flink**. Configure la información del trabajo de Flink haciendo referencia a **Tabla 3-37**.

Tabla 3-37 Información de configuración del trabajo

Parámetro	Descripción
Name	Nombre del trabajo. Contiene de 1 a 64 caracteres. Solo se permiten letras, dígitos, guiones medios (-) y guiones bajos (_). **NOTA** Se recomienda establecer diferentes nombres para diferentes trabajos.

Parámetro	Descripción
Program Path	Ruta del paquete de programa que se va a ejecutar. Se deben cumplir los siguientes requisitos: ● Contiene un máximo de 1,023 caracteres, sin incluir caracteres especiales como ;|&><'$. El valor del parámetro no puede estar vacío ni lleno de espacios. ● La ruta del programa a ejecutar se puede almacenar en HDFS u OBS. La ruta de acceso varía según el sistema de archivos. – OBS: La ruta debe comenzar con **obs://**. Ejemplo: **obs://wordcount/program/*xxx*.jar** (Compatible con MRS 3.x o posterior) – HDFS: La ruta debe comenzar con **/user**. Para obtener más información sobre cómo importar datos a HDFS, consulte **Importación de datos**. **NOTA** Si utiliza una ruta de acceso OBS que comienza por **obs://**, configure los permisos para acceder a OBS de la siguiente manera: ● Si la función de control de permisos de OBS está habilitada durante la creación del clúster, puede utilizar el directorio **obs://** sin configuración adicional. ● Si la función de control de permisos OBS no está habilitada o no está disponible durante la creación del clúster, realice los siguientes pasos: 1. En la página de detalles del clúster de MRS, haga clic en la pestaña **Nodes** y expanda un grupo de nodos. 2. Haga clic en un nombre de nodo para ir a la consola del servidor en la nube. 3. Haga clic en  a la derecha de **Agency** y seleccione **MRS_ECS_DEFAULT_AGENCY** y agréguelo. 4. Repita los pasos anteriores para agregar agencias para todos los nodos del clúster.
Program Parameter	(Opcional) Se utiliza para configurar parámetros de optimización como subprocesos, memoria y vCPU para el trabajo a fin de optimizar el uso de recursos y mejorar el rendimiento de la ejecución del trabajo. **Tabla 3-38** describe los parámetros comunes de un programa en ejecución.
Parameters	(Opcional) Parámetro clave para la ejecución del programa. El parámetro es especificado por la función del programa del usuario. MRS solo es responsable de cargar el parámetro. Múltiples parámetros están separados por espacio. El parámetro contiene un máximo de 150,000 caracteres. No puede contener caracteres especiales ;|&><'$, pero puede dejarse en blanco. **ATENCIÓN** Si introduce un parámetro con información confidencial (como la contraseña de inicio de sesión), el parámetro puede estar expuesto en la pantalla de detalles del trabajo y en la impresión del registro. Tenga cuidado al realizar esta operación.

Parámetro	Descripción
Service Parameter	(Opcional) Se utiliza para modificar los parámetros de servicio para el trabajo. La modificación del parámetro sólo se aplica al trabajo actual. Para hacer que la modificación surta efecto permanentemente para el clúster, siga las instrucciones en **Configuración de parámetros de servicio**. Para agregar varios parámetros, haga clic en a la derecha. Para eliminar un parámetro, haga clic en **Delete** a la derecha. **Tabla 3-39** describe los parámetros comunes de un servicio.
Command Reference	Comando enviado en segundo plano para su ejecución cuando se envía un trabajo.

Tabla 3-38 Parámetros del programa

Parámetro	Descripción	Valor de ejemplo
-ytm	Tamaño de memoria de cada contenedor de TaskManager. (Unidad opcional. La unidad es MB de forma predeterminada.)	1024
-yjm	Tamaño de memoria del contenedor de JobManager. (Unidad opcional. La unidad es MB de forma predeterminada.)	1024
-yn	Número de contenedores de Yarn asignados a las aplicaciones. El valor es el mismo que el número de TaskManagers.	2
-ys	Número de núcleos de TaskManager.	2
-ynm	Nombre personalizado de una aplicación en Yarn.	test
-c	Clase del punto de entrada del programa (por ejemplo, el método **main** o **getPlan()**). Este parámetro solo se requiere cuando el archivo JAR no especifica la clase de su manifiesto.	com.bigdata.mrs.test

NOTA

Para MRS 3.x o posterior, el parámetro **-yn** no es compatible.

Tabla 3-39 Parámetros del servicio

Parámetro	Descripción	Valor de ejemplo
fs.obs.access.key	ID de clave para acceder a OBS.	-

Parámetro	Descripción	Valor de ejemplo
fs.obs.secret.key	Clave correspondiente al ID de clave para acceder a OBS.	-

Paso 7 Confirme la información de configuración del trabajo y haga clic en **OK**.

Después de crear el trabajo, puede gestionarlo.

----Fin

Envío de un trabajo en segundo plano

Paso 1 Inicie sesión en el cliente de MRS.

Paso 2 Ejecute el siguiente comando para inicializar variables de entorno:

source /opt/Bigdata/client/bigdata_env

Paso 3 Si la autenticación de Kerberos está habilitada para el clúster, realice los siguientes pasos. Si la autenticación de Kerberos no está habilitada para el clúster, omita este paso.

1. Prepare un usuario para enviar trabajos de Flink.
   - MRS 3.x o anterior: Para obtener más información, consulte **Preparación de un usuario de desarrollo**.
   - MRS 3.*x* o posterior: Para obtener más información, consulte **Preparación de un usuario de desarrollo**.
2. Inicie sesión en Manager como el usuario recién creado.
   - Para MRS 3.x anterior: Inicie sesión en Manager del clúster. Elija **System** > **Manage User**. En la columna **Operation** de la fila que contiene el usuario agregado, elija **More** > **Download authentication credential** para localizar la fila que contiene el usuario.
   - Para MRS 3.*x* o posterior: Inicie sesión en el Manager del clúster. Elija **System** >**Permission** >**Manage User**. En la página mostrada, busque la fila que contiene el usuario agregado, haga clic en **More** en la columna **Operation** y seleccione **Download authentication credential**.
3. Descomprima el paquete de credenciales de autenticación descargado y copie el archivo obtenido en un directorio en el nodo cliente, por ejemplo **/opt/Bigdata/client/Flink/flink/conf**. Si el cliente está instalado en un nodo fuera del clúster, copie el archivo obtenido en el directorio **/etc/** de este nodo.
4. Para MRS 3.x o posterior: En modo de seguridad, agregue la dirección IP del servicio del nodo donde está instalado el cliente y la dirección IP flotante de Manager al elemento de configuración **jobmanager.web.allow-access-address** en el archivo **/opt/Bigdata/client/Flink/flink/conf/flink-conf.yaml**.
5. Ejecute los siguientes comandos para configurar la autenticación de seguridad agregando la ruta **keytab** y el nombre de usuario al archivo de configuración **/opt/Bigdata/client/Flink/flink/conf/flink-conf.yaml**.

   ```
   security.kerberos.login.keytab: <user.keytab file path>
   security.kerberos.login.principal: <Username>
   ```

   Ejemplo:


```
security.kerberos.login.keytab: /opt/Bigdata/client/Flink/flink/conf/
user.keytab
security.kerberos.login.principal: test
```

6. En el directorio **bin** del cliente de Flink, ejecute el siguiente comando para realizar el refuerzo de seguridad. A continuación, establezca una contraseña para enviar trabajos.

   sh generate_keystore.sh

   Este script reemplaza automáticamente el valor SSL en el archivo **/opt/Bigdata/client/Flink/flink/conf/flink-conf.yaml**. Para MRS 3.x o versiones anteriores, SSL externo está deshabilitado de forma predeterminada en los clústeres de seguridad. Para habilitar SSL externo, vuelva a ejecutar este script después de la configuración. Los parámetros de configuración no existen en la configuración predeterminada de Flink de MRS, si habilita SSL para conexiones externas, debe agregar los parámetros enumerados en **Tabla 3-40**.

Tabla 3-40 Descripción de parámetros

Parámetro	Valor de ejemplo	Descripción
security.ssl.rest.enabled	true	Interruptor para habilitar SSL externo.
security.ssl.rest.keystore	${path}/flink.keystore	Ruta de acceso para almacenar **keystore**.
security.ssl.rest.keystore-password	123456	Contraseña del **keystore**. **123456** indica que se requiere una contraseña definida por el usuario.
security.ssl.rest.key-password	123456	Contraseña de la clave SSL. **123456** indica que se requiere una contraseña definida por el usuario.
security.ssl.rest.truststore	${path}/flink.truststore	Ruta de acceso para almacenar el **truststore**.
security.ssl.rest.truststore-password	123456	Contraseña del **truststore**. **123456** indica que se requiere una contraseña definida por el usuario.

NOTA

- Para MRS 3.x o anterior: El script **generate_keystore.sh** se genera automáticamente.
- Los elementos **flink.keystore**, **flink.truststore** y **security.cookie** generados se rellenan automáticamente en los elementos de configuración correspondientes de **flink-conf.yaml**.
- Para MRS 3.*x* o posterior: Puede obtener los valores de **security.ssl.key-password**, **security.ssl.keystore-password**, and **security.ssl.truststore-password** mediante la API de cifrado de texto no cifrado de Manager ejecutando el siguiente comando:

  curl -k -i -u *<user name>*:*<password>* -X POST -HContent-type:application/json -d '{"plainText":"*<password>*"}' 'https://*x.x.x.x*:28443/web/api/v2/tools/encrypt'; En el comando anterior, *<password>* debe ser la misma que la contraseña utilizada para emitir el certificado, y *x.x.x.x* indica la dirección IP flotante del Manager en el clúster.

7. Configure las rutas para que el cliente acceda a los archivos **flink.keystore** y **flink.truststore**.
   - Ruta absoluta: Después de ejecutar el script, la ruta del archivo de **flink.keystore** y **flink.truststore** se establece automáticamente en la ruta absoluta **opt/Bigdata/client/Flink/flink/conf/** en el archivo **flink-conf.yaml**. En este caso, debe mover los archivos **flink.keystore** y **flink.truststore** desde el directorio **conf** a esta ruta absoluta en el cliente de Flink y los nodos de Yarn.
   - Ruta relativa: Realice los siguientes pasos para establecer la ruta del archivo de **flink.keystore** y **flink.truststore** a la ruta relativa y asegúrese de que el directorio donde se ejecuta el comando Flink client puede acceder directamente a las rutas relativas.
     i. En el directorio **/opt/Bigdata/client/Flink/flink/conf/**, cree un nuevo directorio, por ejemplo, **ssl**.
     ii. Mueva el archivo **flink.keystore** y **flink.truststore** al directorio /**opt/Bigdata/client/Flink/flink/conf/ssl/**.
     iii. Para MRS 3.*x* o posterior: Cambie los valores de los siguientes parámetros en el archivo **flink-conf.yaml** a rutas relativas:
     ```
     security.ssl.keystore: ssl/flink.keystore
     security.ssl.truststore: ssl/flink.truststore
     ```
     iv. Para MRS 3.x o anterior: Cambie los valores de los siguientes parámetros en el archivo **flink-conf.yaml** a rutas relativas:
     ```
     security.ssl.internal.keystore: ssl/flink.keystore
     security.ssl.internal.truststore: ssl/flink.truststore
     ```
8. Si el cliente está instalado en un nodo fuera del clúster, agregue la siguiente configuración al archivo de configuración (por ejemplo, **/opt/Bigdata/client/Flink/fink/conf/flink-conf.yaml**). Reemplace ***xx.xx.xxx.xxx*** con la dirección IP del nodo donde reside el cliente.
   ```
   web.access-control-allow-origin: xx.xx.xxx.xxx
   jobmanager.web.allow-access-address: xx.xx.xxx.xxx
   ```

Paso 4 Ejecute un trabajo de wordcount.

- Clúster normal (autenticación de Kerberos desactivada)
  - Ejecute los siguientes comandos para iniciar una sesión y enviar un trabajo en la sesión:
    ```
    yarn-session.sh -nm "session-name" -d
    flink run /opt/Bigdata/client/Flink/flink/examples/streaming/
    WordCount.jar
    ```
  - Ejecute el siguiente comando para enviar un solo trabajo en Yarn:
    ```
    flink run -m yarn-cluster /opt/Bigdata/client/Flink/flink/examples/
    streaming/WordCount.jar
    ```


- Clúster de seguridad (autenticación de Kerberos habilitada)
  - Si el archivo **flink.keystore** y **flink.truststore** se almacenan en la ruta absoluta:
    - Ejecute los siguientes comandos para iniciar una sesión y enviar un trabajo en la sesión:
      ```
      yarn-session.sh -nm "session-name" -d
      flink run /opt/Bigdata/client/Flink/flink/examples/streaming/
      WordCount.jar
      ```
    - Ejecute el siguiente comando para enviar un solo trabajo en Yarn:
      ```
      flink run -m yarn-cluster /opt/Bigdata/client/Flink/flink/examples/
      streaming/WordCount.jar
      ```
  - Si el archivo **flink.keystore** y **flink.truststore** se almacenan en la ruta relativa:
    - En el mismo directorio de SSL, ejecute el siguiente comando para iniciar una sesión y enviar trabajos en la sesión. El directorio SSL es una ruta relativa. Por ejemplo, si el directorio SSL es de **opt/Bigdata/client/Flink/flink/conf/**, ejecute el siguiente comando en este directorio:
      ```
      yarn-session.sh -t ssl/ -nm "session-name" -d
      flink run /opt/Bigdata/client/Flink/flink/examples/streaming/
      WordCount.jar
      ```
    - Ejecute el siguiente comando para enviar un solo trabajo en Yarn:
      ```
      flink run -m yarn-cluster -yt ssl/ /opt/Bigdata/client/Flink/flink/
      examples/streaming/WordCount.jar
      ```

----Fin

3.6.7 Consulta de la configuración de trabajos y registros

Esta sección describe cómo ver la configuración del trabajo y los registros.

Antecedentes

- Puede ver la información de configuración de todos los trabajos.
- Solo puede ver los registros de trabajos en ejecución.

  Dado que los registros de los trabajos de Spark SQL y DistCp no están en segundo plano, no puede ver los registros de los trabajos de Spark SQL y DistCp en ejecución.

Procedimiento

Paso 1 Inicie sesión en la consola de gestión de MRS.

Paso 2 Seleccione **Clusters** > **Active Clusters**, seleccione un clúster en ejecución y haga clic en su nombre para cambiar a la página de detalles del clúster.

Paso 3 Haga clic en **Jobs**.

Paso 4 En la columna **Operation** del trabajo que se va a ver, haga clic en **View Details**.

En la ventana **View Details** que se muestra, se muestra la configuración del trabajo seleccionado.

Paso 5 Seleccione un trabajo en ejecución y haga clic en **View Log** en la columna **Operation**.

En la nueva página que se muestra, se muestra información de registro en tiempo real del trabajo.

Cada tenant puede enviar y ver 10 trabajos simultáneamente.

----Fin

3.6.8 Detener un trabajo

Esta sección describe cómo detener la ejecución de trabajos de MRS.

Antecedentes

No puede detener los trabajos de Spark SQL. Después de detener un trabajo, su estado cambia a **Terminated** y el trabajo no se puede ejecutar de nuevo.

Procedimiento

Paso 1 Inicie sesión en la consola de gestión de MRS.

Paso 2 Elija **Clusters** > **Active Clusters**, seleccione un clúster en ejecución y haga clic en su nombre.

Se muestra la página de detalles del clúster.

Paso 3 Haga clic en **Jobs**.

Paso 4 Seleccione un trabajo en ejecución y elija **More > Stop** en la columna **Operation**.

El estado del trabajo cambia de **Running** a **Terminated**.

----Fin

3.6.9 Eliminación de un trabajo

En esta sección se describe cómo eliminar un trabajo de MRS. Después de ejecutar un trabajo, puede eliminarlo si no necesita ver su información.

Antecedentes

Los trabajos se pueden eliminar uno tras otro o en un lote. No se puede restaurar un trabajo eliminado. Por lo tanto, tenga cuidado al eliminar un trabajo.

Procedimiento

Paso 1 Inicie sesión en la consola de gestión de MRS.

Paso 2 Elija **Clusters** > **Active Clusters**, seleccione un clúster en ejecución y haga clic en su nombre.

Se muestra la página de detalles del clúster.

Paso 3 Haga clic en **Jobs**.

Paso 4 Elija **More > Delete** en el **Operation** de la fila del trabajo de destino que se va a eliminar.

En este paso, solo puede eliminar un trabajo.

Paso 5 Si selecciona varios trabajos y haga clic en **Delete** en la parte superior izquierda de la lista de trabajos.

Puede eliminar uno, varios o todos los trabajos.

----Fin

3.6.10 Uso de datos de OBS cifrados para la ejecución de trabajos

En MRS 1.9.x , los datos cifrados en sistemas de archivos de OBS se pueden usar para ejecutar trabajos, y los resultados de ejecución de trabajos cifrados se pueden almacenar en sistemas de archivos de OBS. Actualmente, solo se puede acceder a los datos a través de un protocolo de OBS.

OBS admite cifrado y descifrado de datos mediante claves de KMS. Todas las operaciones de encriptación y descifrado se realizan en OBS, y las claves son gestionadas por DEW.

Para utilizar la función de encriptación OBS en MRS, debe tener los permisos de administrador de KMS y configurar la siguiente configuración para el componente correspondiente:

Prerrequisitos

Ha configurado primero la función de acceso a OBS desde MRS para utilizar la función de encriptación de OBS.

Configuración de Hive

Paso 1 Inicie sesión en la consola de gestión de MRS. En el árbol de navegación de la izquierda, elija **Clusters** > **Active Clusters** y haga clic en el nombre del clúster.

Paso 2 Elija **Components** >**Hive** >**Service Configuration**.

Paso 3 Cambie **Basic** a **All** y busque y establezca los siguientes parámetros:

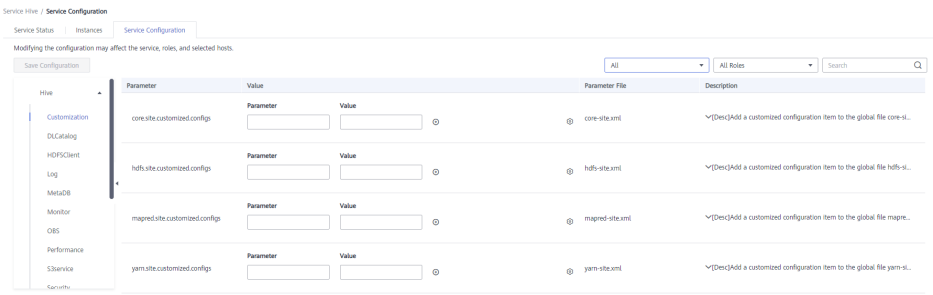


Tabla 3-41 Parámetros de encriptación de datos

Parámetro	Valor	Descripción
fs.obs.server-side-encryption-type	SSE-KMS	● **SSE-KMS**: las claves de KMS se utilizan para encriptación y descifrado ● **NONE**: La función de encriptación está deshabilitada.
fs.obs.server-side-encryption-key	-	(Opcional) Este parámetro indica un ID de la clave KMS utilizada para la encriptación. Si **fs.obs.server-side-encryption-type** se establece en **SSE-KMS** y este parámetro no se establece, OBS utiliza la clave KMS predeterminada para la encriptación.

Parámetro	Valor	Descripción
fs.obs.connection.ssl.enabled	true	Si desea establecer una conexión segura con OBS. ● **true**: La conexión segura está habilitada. Para utilizar la encriptación y el descifrado de OBS, este parámetro debe establecerse en **true**. ● **false**: La conexión segura está deshabilitada.

Paso 4 Haga clic en **Save Configuration** y guarde los parámetros modificados como se le indique.

----Fin

Configuración de Hadoop

Método 1: Configuración en la GUI

Paso 1 Inicie sesión en la consola de gestión de MRS. En el árbol de navegación de la izquierda, elija **Clusters** > **Active Clusters** y haga clic en el nombre del clúster.

Paso 2 Elija **Components** >**HDFS** >**Service Configuration**.

Paso 3 Cambie **Basic** a **All** y busque y establezca los siguientes parámetros:

Tabla 3-42 Parámetros de encriptación de datos

Parámetro	Valor	Descripción
fs.obs.server-side-encryption-type	SSE-KMS	● **SSE-KMS**: las claves de KMS se utilizan para encriptación y descifrado ● **NONE**: La función de encriptación está deshabilitada.
fs.obs.server-side-encryption-key	-	ID de la clave de KMS utilizada para encriptación. Este parámetro es opcional. Si **fs.obs.server-side-encryption-type** se establece en **SSE-KMS** y este parámetro no se establece, OBS utiliza la clave KMS predeterminada para la encriptación.
fs.obs.connection.ssl.enabled	true	Si desea establecer una conexión segura con OBS. ● **true**: La conexión segura está habilitada. Para utilizar la encriptación y el descifrado de OBS, este parámetro debe establecerse en **true**. ● **false**: La conexión segura está deshabilitada.

Paso 4 Haga clic en **Save Configuration** y seleccione **Restart the affected services or instances**. Haga clic en **OK**.

Paso 5 Inicie sesión en el nodo de Master como usuario **root**. La contraseña es la contraseña del usuario **root** que establece al crear el clúster. Si el clúster tiene varios nodos de Master, inicie sesión en cada nodo de Master y repita **Paso 5** a **Paso 7**.

Paso 6 Ejecute el siguiente comando para cambiar al directorio del cliente, por ejemplo **/opt/Bigdata/client**:

cd /opt/Bigdata/client

Paso 7 Ejecute el siguiente comando para actualizar las configuraciones del cliente e introduzca el nombre de usuario y la contraseña. El nombre de usuario es **admin** y la contraseña es la contraseña del usuario **admin** que establece al crear el clúster.

./ autoRefreshConfig.sh

----Fin

Método 2: Configuración a través del archivo de configuración del cliente

Agregue los siguientes parámetros al archivo de configuración del cliente, por ejemplo **/opt/Bigdata/client/HDFS/hadoop/etc/hadoop/core-site.xml** en el nodo de Master. Si el clúster tiene varios nodos de Master, inicie sesión en cada nodo de Master y realice esta operación.

Tabla 3-43 Parámetros de encriptación de datos

Parámetro	Valor	Descripción
fs.obs.server-side-encryption-type	SSE-KMS	● **SSE-KMS**: las claves de KMS se utilizan para encriptación y descifrado ● **NONE**: La función de encriptación está deshabilitada.
fs.obs.server-side-encryption-key	-	ID de la clave de KMS utilizada para encriptación. Este parámetro es opcional. Si **fs.obs.server-side-encryption-type** se establece en **SSE-KMS** y este parámetro no se establece, OBS utiliza la clave KMS predeterminada para la encriptación.
fs.obs.connection.ssl.enabled	true	Si desea establecer una conexión segura con OBS. ● **true**: La conexión segura está habilitada. Para utilizar la encriptación y el descifrado de OBS, este parámetro debe establecerse en **true**. ● **false**: La conexión segura está deshabilitada.

Configuración de HBase

Método 1: Configuración en la GUI

Paso 1 Inicie sesión en la consola de gestión de MRS. En el árbol de navegación de la izquierda, elija **Clusters** > **Active Clusters** y haga clic en el nombre del clúster.

Paso 2 Elija **Components** >**HBase** >**Service Configuration**.

Paso 3 Cambie **Basic** a **All** y busque y establezca los siguientes parámetros:

Tabla 3-44 Parámetros de encriptación de datos

Parámetro	Valor	Descripción
fs.obs.server-side-encryption-type	SSE-KMS	● **SSE-KMS**: las claves de KMS se utilizan para encriptación y descifrado ● **NONE**: La función de encriptación está deshabilitada.
fs.obs.server-side-encryption-key	-	ID de la clave de KMS utilizada para encriptación. Este parámetro es opcional. Si **fs.obs.server-side-encryption-type** se establece en **SSE-KMS** y este parámetro no se establece, OBS utiliza la clave KMS predeterminada para la encriptación.
fs.obs.connection.ssl.enabled	true	Si desea establecer una conexión segura con OBS. ● **true**: La conexión segura está habilitada. Para utilizar la encriptación y el descifrado de OBS, este parámetro debe establecerse en **true**. ● **false**: La conexión segura está deshabilitada.

Paso 4 Haga clic en **Save Configuration** y seleccione **Restart the affected services or instances**. Haga clic en **OK**.

Paso 5 Inicie sesión en el nodo de Master como usuario **root**. La contraseña es la contraseña del usuario **root** que establece al crear el clúster. Si el clúster tiene varios nodos de Master, inicie sesión en cada nodo de Master y repita **Paso 5** a **Paso 7**.

Paso 6 Ejecute el siguiente comando para cambiar al directorio del cliente, por ejemplo **/opt/Bigdata/client**:

cd /opt/Bigdata/client

Paso 7 Ejecute el siguiente comando para actualizar las configuraciones del cliente e introduzca el nombre de usuario y la contraseña. El nombre de usuario es **admin** y la contraseña es la contraseña del usuario **admin** que establece al crear el clúster.

./ autoRefreshConfig.sh

----Fin

Método 2: Configuración a través del archivo de configuración del cliente

Agregue los siguientes parámetros al archivo de configuración del cliente, por ejemplo **/opt/Bigdata/client/HBase/hbase/conf/core-site.xml** en el nodo de Master. Si el clúster tiene varios nodos de Master, inicie sesión en cada nodo de Master y realice esta operación.

Tabla 3-45 Parámetros de encriptación de datos

Parámetro	Valor	Descripción
fs.obs.server-side-encryption-type	SSE-KMS	● **SSE-KMS**: las claves de KMS se utilizan para encriptación y descifrado ● **NONE**: La función de encriptación está deshabilitada.
fs.obs.server-side-encryption-key	-	ID de la clave de KMS utilizada para encriptación. Este parámetro es opcional. Si **fs.obs.server-side-encryption-type** se establece en **SSE-KMS** y este parámetro no se establece, OBS utiliza la clave KMS predeterminada para la encriptación.
fs.obs.connection.ssl.enabled	true	Si desea establecer una conexión segura con OBS. ● **true**: La conexión segura está habilitada. Para utilizar la encriptación y el descifrado de OBS, este parámetro debe establecerse en **true**. ● **false**: La conexión segura está deshabilitada.

Configuración de Spark

Método 1: Configuración en la GUI

Paso 1 Inicie sesión en la consola de gestión de MRS. En el árbol de navegación de la izquierda, elija **Clusters** > **Active Clusters** y haga clic en el nombre del clúster.

Paso 2 Elija **Components** >**Spark** >**Service Configuration**.

Paso 3 Cambie **Basic** a **All** y busque y establezca los siguientes parámetros:

Tabla 3-46 Parámetros de encriptación de datos

Parámetro	Valor	Descripción
fs.obs.server-side-encryption-type	SSE-KMS	● **SSE-KMS**: las claves de KMS se utilizan para encriptación y descifrado ● **NONE**: La función de encriptación está deshabilitada.

Parámetro	Valor	Descripción
fs.obs.server-side-encryption-key	-	ID de la clave de KMS utilizada para encriptación. Este parámetro es opcional. Si **fs.obs.server-side-encryption-type** se establece en **SSE-KMS** y este parámetro no se establece, OBS utiliza la clave KMS predeterminada para la encriptación.
fs.obs.connection.ssl.enabled	true	Si desea establecer una conexión segura con OBS. ● **true**: La conexión segura está habilitada. Para utilizar la encriptación y el descifrado de OBS, este parámetro debe establecerse en **true**. ● **false**: La conexión segura está deshabilitada.

Paso 4 Haga clic en **Save Configuration** y seleccione **Restart the affected services or instances**. Haga clic en **OK**.

Paso 5 Inicie sesión en el nodo de Master como usuario **root**. La contraseña es la contraseña del usuario **root** que establece al crear el clúster. Si el clúster tiene varios nodos de Master, inicie sesión en cada nodo de Master y repita **Paso 5** a **Paso 7**.

Paso 6 Ejecute el siguiente comando para cambiar al directorio del cliente, por ejemplo **/opt/Bigdata/client**:

cd /opt/Bigdata/client

Paso 7 Ejecute el siguiente comando para actualizar las configuraciones del cliente e introduzca el nombre de usuario y la contraseña. El nombre de usuario es **admin** y la contraseña es la contraseña del usuario **admin** que establece al crear el clúster.

./autoRefreshConfig.sh

----Fin

Método 2: Configuración a través del archivo de configuración del cliente

Agregue los siguientes parámetros al archivo de configuración del cliente, por ejemplo **/opt/Bigdata/client/Spark/spark/conf/core-site.xml**, en el nodo de Master. Si el clúster tiene varios nodos de Master, inicie sesión en cada nodo de Master y realice esta operación.

Tabla 3-47 Parámetros de encriptación de datos

Parámetro	Valor	Descripción
fs.obs.server-side-encryption-type	SSE-KMS	● **SSE-KMS**: las claves de KMS se utilizan para encriptación y descifrado ● **NONE**: La función de encriptación está deshabilitada.

Parámetro	Valor	Descripción
fs.obs.server-side-encryption-key	-	ID de la clave de KMS utilizada para encriptación. Este parámetro es opcional. Si **fs.obs.server-side-encryption-type** se establece en **SSE-KMS** y este parámetro no se establece, OBS utiliza la clave KMS predeterminada para la encriptación.
fs.obs.connection.ssl.enabled	true	Si desea establecer una conexión segura con OBS. ● **true**: La conexión segura está habilitada. Para utilizar la encriptación y el descifrado de OBS, este parámetro debe establecerse en **true**. ● **false**: La conexión segura está deshabilitada.

Configuración de Presto

Paso 1 Inicie sesión en la consola de gestión de MRS. En el árbol de navegación de la izquierda, elija **Clusters** > **Active Clusters** y haga clic en el nombre del clúster.

Paso 2 Elija **Components** >**Presto** >**Service Configuration**.

Paso 3 Cambie **Basic** a **All** y busque y establezca los siguientes parámetros:

Tabla 3-48 Parámetros de encriptación de datos

Parámetro	Valor	Descripción
fs.obs.server-side-encryption-type	SSE-KMS	● **SSE-KMS**: las claves de KMS se utilizan para encriptación y descifrado ● **NONE**: La función de encriptación está deshabilitada.
fs.obs.server-side-encryption-key	-	ID de la clave de KMS utilizada para encriptación. Este parámetro es opcional. Si **fs.obs.server-side-encryption-type** se establece en **SSE-KMS** y este parámetro no se establece, OBS utiliza la clave KMS predeterminada para la encriptación.

Parámetro	Valor	Descripción
fs.obs.connection.ssl.enabled	true	Si desea establecer una conexión segura con OBS. ● **true**: La conexión segura está habilitada. Para utilizar la encriptación y el descifrado de OBS, este parámetro debe establecerse en **true**. ● **false**: La conexión segura está deshabilitada.

Paso 4 Haga clic en **Save Configuration** y seleccione **Restart the affected services or instances**. Haga clic en **OK**.

----Fin

3.6.11 Configuración de reglas de notificación de trabajos

MRS utiliza SMN para ofrecer un modelo de publicación/suscripción para lograr suscripciones y notificaciones de uno a varios mensajes en una variedad de tipos de mensajes (SMS y correos electrónicos). Puede configurar reglas de notificación de trabajo para recibir notificaciones inmediatamente tras un éxito o falla de ejecución de trabajo.

Procedimiento

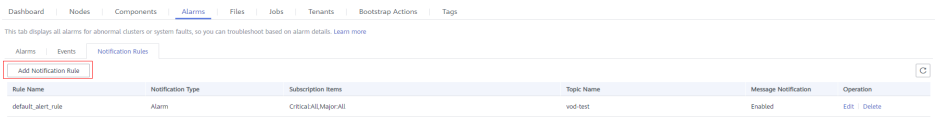
Paso 1 Inicie sesión en la consola de gestión.

Paso 2 Haga clic en **Service List**. En **Management & Governance**, haga clic en **Simple Message Notification**.

Paso 3 Cree un tema y agregue suscripciones al tema. Para obtener más información, consulte **Configuración de la notificación de mensaje**.

Paso 4 Vaya a la consola de gestión de MRS y haga clic en el nombre del clúster para ir a la página de detalles del clúster.

Paso 5 Haga clic en la pestaña **Alarms** y elija **Notification Rules** > **Add Notification Rule**.



Paso 6 Configure una regla de notificación para enviar resultados de ejecución de trabajos a los suscriptores.

Tabla 3-49 Parámetros para agregar una regla de notificación

Parámetro	Descripción
Rule Name	Nombre de regla de notificación definida por el usuario. Solo se permiten dígitos, letras, guiones (-) y guiones bajos (_).

Parámetro	Descripción
Message Notification	Si habilita esta función, los mensajes de suscripción se enviarán a los suscriptores.
Topic Name	Seleccione un tema existente o haga clic en **Create Topic** para crear un tema.
Notification Type	Seleccione **Event**.
Subscription Items	1. Haga clic en junto a **Suggestion**. 2. Haga clic en junto a **Manager**. 3. Seleccione **Job Running Succeeded** y **Job Running Failed**.

----Fin

3.7 Gestión de componentes

3.7.1 Gestión de objetos

MRS contiene diferentes tipos de objetos básicos. **Tabla 3-50** describe estos objetos.

Tabla 3-50 Descripción del objeto básico de MRS

Objeto	Descripción	Ejemplo
Servicio	Conjunto de funciones que puede completar un negocio específico.	Servicio de KrbServer y servicio de LdapServer
Instancia del servicio	Ejemplo específico de un servicio, generalmente llamado servicio.	Servicio de KrbServer
Rol de servicio	Entidad de función que forma un servicio completo, generalmente llamado rol.	KrbServer está compuesto por el rol KerberosAdmin y el rol KerberosServer.
Instancia de rol	Ejemplo específico de un rol de servicio que se ejecuta en un host.	KerberosAdmin que se ejecuta en Host2 y KerberosServer que se ejecuta en Host3
Host	Un ECS que ejecuta el sistema operativo de Linux.	Host1 a Host5
Rack	Entidad física que contiene varios hosts que se conectan al mismo switch.	Rack1 contiene Host1 a Host5.

Objeto	Descripción	Ejemplo
Clúster	Entidad lógica que consta de varios hosts y proporciona varios servicios.	El clúster de Cluster1 consta de cinco hosts (de Host1 a Host5) y proporciona servicios como KrbServer y LdapServer.

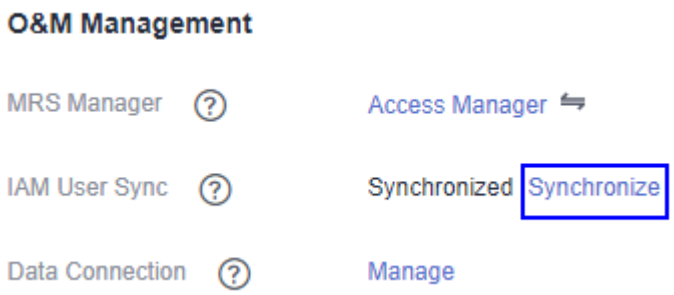
3.7.2 Ver configuraciones

En MRS, puede ver la configuración de los servicios (incluidos los roles) y las instancias de rol.

Prerrequisitos

Tiene usuarios de IAM sincronizados. (En la página **Dashboard**, haga clic en **Synchronize** en el lado derecho de **IAM User Sync** para sincronizar usuarios de IAM.)

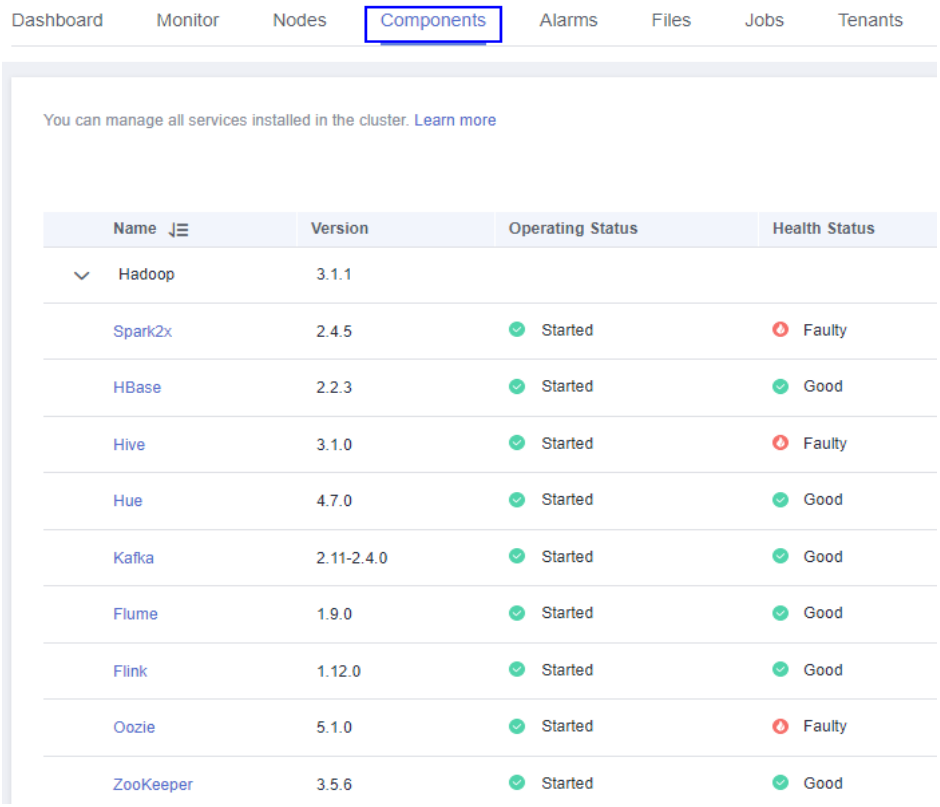
Figura 3-33 Sincronización de usuarios de IAM



Procedimiento

- Consultar configuración de servicio.
  a. En la página de detalles del clúster, haga clic en la pestaña **Components**.

Figura 3-34 Página de pestaña de componentes

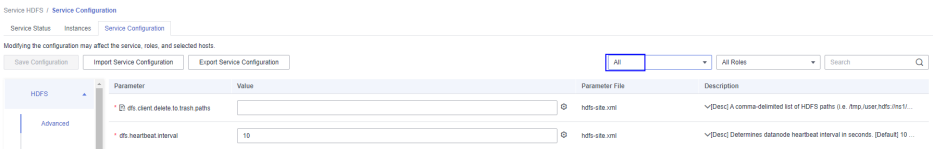


b. Seleccione el servicio de destino en la lista de servicios.

c. Haga clic en **Service Configuration**.

d. Cambie de **Basic** a **All**. Todos los parámetros de configuración del servicio se muestran en el árbol de navegación. El nombre del servicio y los nombres de rol se muestran de arriba a abajo en el árbol de navegación.

Figura 3-35 Todas las configuraciones.



e. En el árbol de navegación, seleccione un parámetro especificado y cambie su valor. También puede introducir el nombre del parámetro en el cuadro **Search** para buscar el parámetro y ver el resultado.

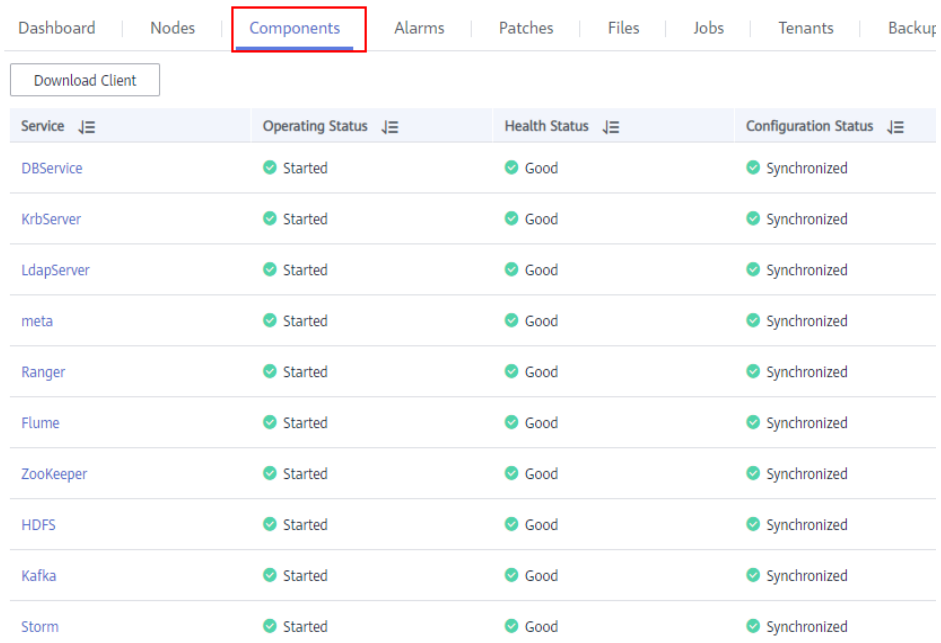
Los parámetros bajo los nodos de servicio y los nodos de rol son parámetros de configuración de servicio y parámetros de configuración de rol respectivamente.

f. Si selecciona **Non-default** en la lista desplegable **--Select--**, los parámetros cuyos valores no son los predeterminados se muestran en la página. (Esta opción de valor está disponible en versiones anteriores a MRS 3.*x*.)

- Consultar configuraciones de instancia de rol.

a. En la página de detalles del clúster de MRS, haga clic en **Components**.

Figura 3-36 Página de pestaña Componentes (usando MRS 1.9.2 como ejemplo)



b. Seleccione el servicio de destino en la lista de servicios.

c. Haga clic en la pestaña **Instances**.

d. Haga clic en la instancia de rol de destino en la lista de instancias de rol.

e. Haga clic en **Instance Configuration**.

f. Cambie **Basic** a **All** a la derecha de la página. Todos los parámetros de configuración de la instancia de rol se muestran en el árbol de navegación.

g. En el árbol de navegación, seleccione un parámetro especificado y cambie su valor. También puede introducir el nombre del parámetro en el cuadro **Search** para buscar el parámetro y ver el resultado.

h. Si selecciona **Non-default** en la lista desplegable **--Select--**, los parámetros cuyos valores no son los predeterminados se muestran en la página. (Esta opción de valor está disponible en versiones anteriores a MRS 3.*x*.)

3.7.3 Gestión de servicios

Puede realizar las siguientes operaciones en MRS:

- Agregar o eliminar servicios. Solo está disponible para clústeres personalizados de MRS 3.1.2 y versiones posteriores.
- Inicie el servicio en el estado **Stopped**, **Stop Failed** o **Failed to Start** para usar el servicio.
- Detener los servicios o detener los servicios anormales.
- Reinicie servicios anormales o configure servicios caducados para restaurar o habilitar los servicios.

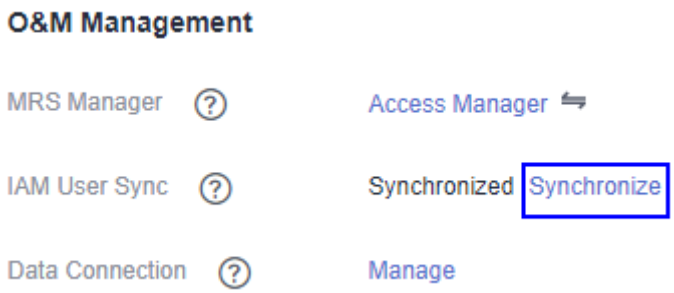
Prerrequisitos

- **Ha configurado permisos para el grupo de usuarios al que pertenecen los usuarios de IAM.**

Agregar o eliminar un servicio en un clúster es una operación de alto riesgo. Vincule la política de MRS FullAccess, MRS Administrator, Server Administrator, Tenant Guest, MRS Administrator, o Tenant Administrator al grupo de usuarios antes de realizar esta operación. Para obtener más información sobre los permisos, consulte **Sincronización de usuarios de IAM a MRS**.

- **Ha sincronizado usuarios de IAM.** (En la página de pestaña **Dashboard**, haga clic en **Synchronize** junto a **IAM User Sync** para sincronizar usuarios de IAM.)

Figura 3-37 Sincronización de usuarios de IAM



Impacto en el sistema

- El componente con estado no se puede agregar al grupo de nodos de tarea.

Adición de un servicio

NOTA

Los servicios se pueden agregar y eliminar en MRS 3.1.2-LTS.3 o posterior.

Paso 1 En la página de detalles del clúster, elija **Components** y haga clic en **Add Service**.

Paso 2 En la lista de servicios, seleccione los servicios que desea agregar y haga clic en **Next**.

NOTA

- Cuando se agrega un servicio, se seleccionan automáticamente los servicios subyacentes de los que depende el servicio. Puede agregar varios servicios al mismo tiempo.
- Puede agregar un servicio solo en un nodo en estado normal.
- Si agrega Hadoop a un clúster sin Hadoop antes, debe actualizar la página de detalles del clúster en la consola de MRS y sincronizar los usuarios de IAM para que los trabajos se puedan enviar correctamente.
- No se puede agregar un solo componente del servicio Hadoop al clúster. Solo se puede agregar el servicio Hadoop. El servicio Hadoop incluye MapReduce, Yarn, y HDFS.
- Después de agregar el componente de Spark2x, si necesita operar SparkSQL en la interfaz de usuario web de Hue, reinicie primero el servicio de Hue.

Paso 3 En la página **Topology Adjustment**, seleccione los nodos en los que se va a desplegar el servicio. Para obtener más información sobre el esquema de despliegue, consulte **Tabla 2-9**.

Paso 4 Haga clic en **OK**. Después de agregar el servicio, puede ver el servicio agregado en la página **Components**.

NOTA

Los servicios agregados en la consola se sincronizan automáticamente con Manager.

----Fin

Eliminación de un servicio

NOTA

Los servicios se pueden agregar y eliminar en MRS 3.1.2-LTS.3 o posterior.

Paso 1 En la página de detalles del clúster, haga clic en **Components**.

Paso 2 Busque la fila que contiene el servicio de destino y haga clic en **Delete**.

NOTA

- Si el servicio que se va a eliminar tiene dependencias de capa superior, el servicio no se puede eliminar. Solo se puede eliminar un servicio a la vez.
- Puede eliminar los servicios instalados excepto Hadoop (HDFS, Yarn y MapReduce), Ranger, DBService, KrbServer, LdapServer y meta servicios.

Paso 3 En el cuadro de diálogo que se muestra, haga clic en **Yes** para confirmar la eliminación.

ATENCIÓN

- Los servicios eliminados en la consola se sincronizan automáticamente con Manager.
- Antes de eliminar un servicio, realice una copia de respaldo de los datos del servicio para evitar la pérdida de datos.

----Fin

Inicio, detención y reinicio de un servicio

Paso 1 En la página de detalles del clúster de MRS, haga clic en **Components**.

Paso 2 Busque la fila que contiene el servicio de destino, **Start**, **Stop**, y **Restart** para iniciar, detener o reiniciar el servicio.

Los servicios están interrelacionados. Si se inicia, se detiene y se reinicia un servicio, los servicios que dependen de él se verán afectados.

Los servicios se verán afectados de las siguientes maneras:

- Si se va a iniciar un servicio, los servicios de capa inferior que dependen de él deben iniciarse primero.
- Si se detiene un servicio, los servicios de capa superior que dependen de él no estarán disponibles.
- Si se reinicia un servicio, los servicios de capa superior en ejecución que dependen de él deben reiniciarse.

----Fin

3.7.4 Configuración de parámetros de servicio

En la consola de MRS, puede ver y modificar las configuraciones de servicio predeterminadas según los requisitos del sitio y exportar o importar las configuraciones.

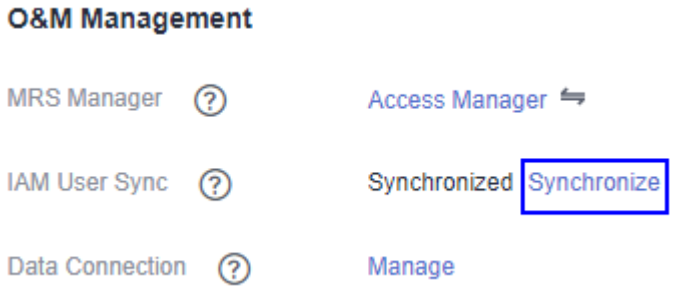
Impacto en el sistema

- Debe descargar y actualizar los archivos de configuración del cliente después de configurar las propiedades de servicio HBase, HDFS, Hive, Spark, Yarn y MapReduce.
- Los parámetros de DBService no se pueden modificar cuando solo existe una instancia de rol DBService en el clúster.

Prerrequisitos

Tiene usuarios de IAM sincronizados. (En la página **Dashboard**, haga clic en **Synchronize** en el lado derecho de **IAM User Sync** para sincronizar usuarios de IAM.)

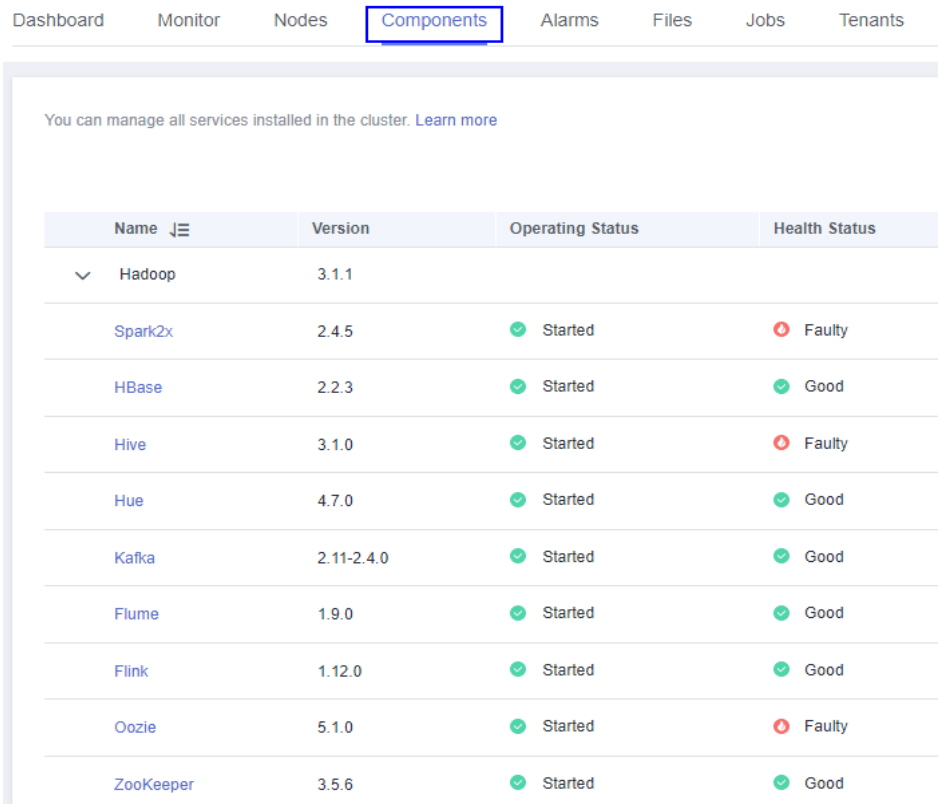
Figura 3-38 Sincronización de usuarios de IAM



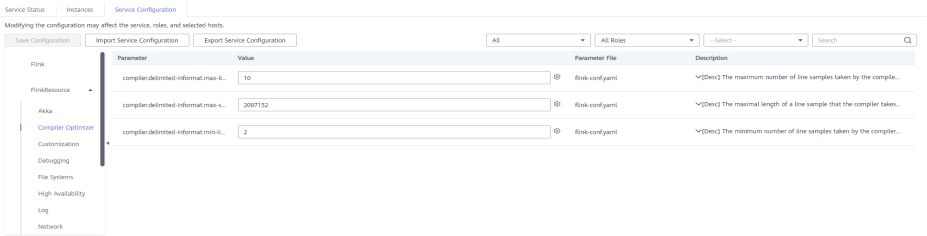
Modificación de parámetros de servicio

1. En la página de detalles del clúster de MRS, haga clic en **Components**.

Figura 3-39 Página de pestaña de componentes



2. Seleccione el servicio de destino en la lista de servicios.
3. Haga clic en **Service Configuration**.
4. Cambie de **Basic** a **All**. Todos los parámetros de configuración del servicio se muestran en el árbol de navegación. El nombre del servicio y los nombres de rol se muestran de arriba a abajo en el árbol de navegación.
5. En el árbol de navegación, seleccione un parámetro especificado y cambie su valor. También puede introducir el nombre del parámetro en el cuadro **Search** para buscar el parámetro y ver el resultado.



Si desea cancelar la modificación de un valor de parámetro, haga clic en para restaurarlo.

6. Haga clic en **Save Configuration**, guarde los parámetros y reinicie el servicio.

NOTA

En versiones anteriores a MRS 3.*x*, para actualizar la configuración de cola de YARN sin reiniciar el servicio, seleccione **More** > **Refresh Queue** en la página de pestaña **Service Status**.

3.7.5 Configuración de parámetros de servicio personalizados

Cada componente de MRS soporta todos los parámetros de código abierto. MRS admite la modificación de algunos parámetros para escenarios de aplicación clave. Algunos clientes de componentes pueden no incluir todos los parámetros con características de código abierto. Para modificar los parámetros de componentes que no son compatibles directamente con MRS, puede agregar nuevos parámetros para los componentes mediante la función de personalización de configuración en MRS. Los parámetros recién agregados se guardan en los archivos de configuración de componentes y entran en vigor después del reinicio.

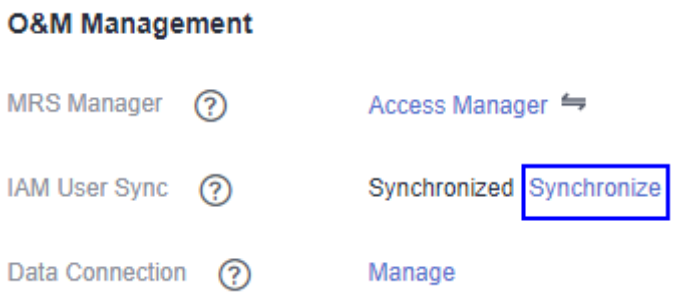
Impacto en el sistema

- Después de configurar los atributos de servicio, es necesario reiniciar el servicio. No se puede acceder al servicio durante el reinicio.
- Debe descargar y actualizar los archivos de configuración del cliente después de configurar las propiedades de servicio HBase, HDFS, Hive, Spark, Yarn y MapReduce.

Prerrequisitos

- Ha comprendido los significados de los parámetros a añadir, los archivos de configuración que han surtido efecto y el impacto en los componentes.
- Tiene usuarios de IAM sincronizados. (En la página **Dashboard**, haga clic en **Synchronize** en el lado derecho de **IAM User Sync** para sincronizar usuarios de IAM.)

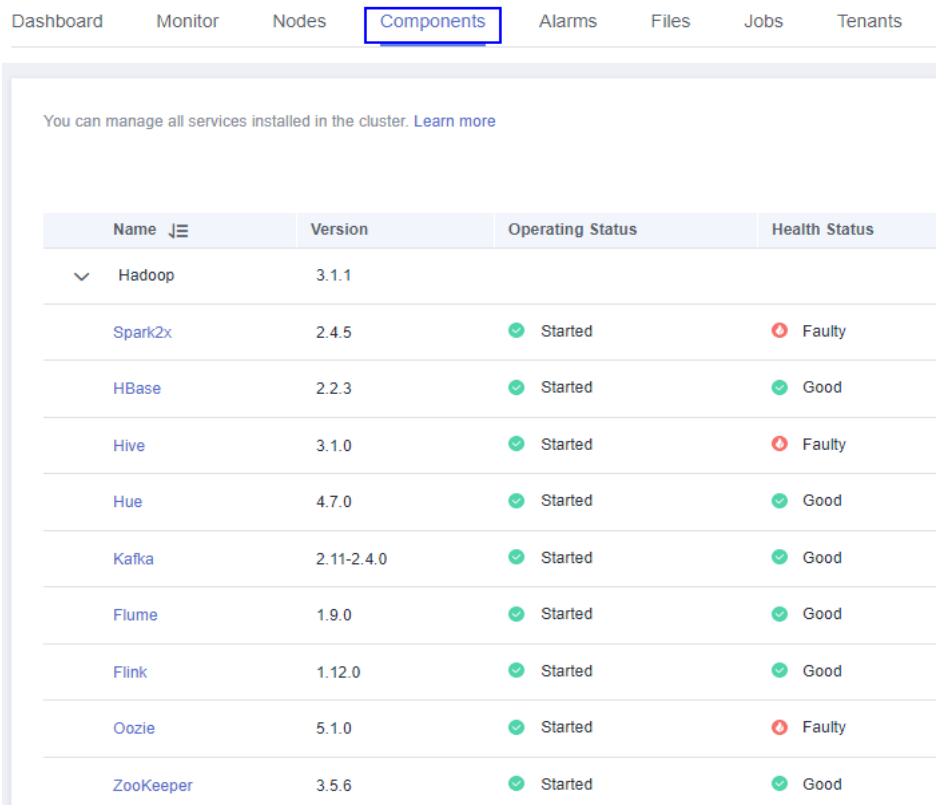
Figura 3-40 Sincronización de usuarios de IAM



Procedimiento

Paso 1 En la página de detalles del clúster de MRS, haga clic en **Components**.

Figura 3-41 Página de pestaña de componentes

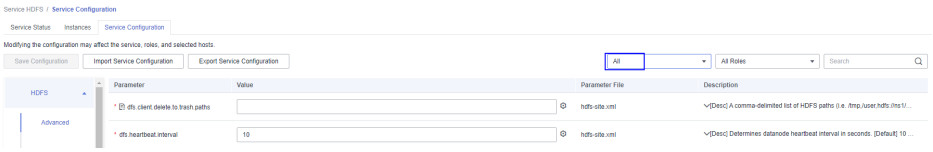


Paso 2 Seleccione el servicio de destino en la lista de servicios.

Paso 3 Haga clic en **Service Configuration**.

Paso 4 En el cuadro desplegable de tipo de configuración del lado derecho, cambie **Basic** a **All**.

Figura 3-42 Todas las configuraciones.



Paso 5 En el árbol de navegación, seleccione **Customization**. Los parámetros personalizados del componente actual se muestran en MRS.

Los archivos de configuración que guardan los parámetros personalizados recién agregados se muestran en la columna **Parameter File**. Diferentes archivos de configuración pueden tener los mismos parámetros de código abierto. Después de que los parámetros en diferentes archivos se establecen en valores diferentes, si la configuración tiene efecto depende de la secuencia de carga de los archivos de configuración por componentes. Puede personalizar los parámetros para los servicios y roles según sea necesario. No se admite la adición de parámetros personalizados para una instancia de rol única.

Paso 6 En función de los archivos de configuración y las funciones de parámetros, busque la fila donde reside un parámetro especificado, introduzca el nombre del parámetro admitido por el componente en la columna **Parameter** e introduzca el valor del parámetro en la columna **Value**.

- Puede hacer clic en o para agregar o eliminar un parámetro personalizado. You can delete a customized parameter only after you click for the first time.
- Si desea cancelar la modificación de un valor de parámetro, haga clic en para restaurarlo.

Paso 7 Haga clic en **Save Configuration**, seleccione **Restart the affected services or instances**, y haga clic en **OK**.

----Fin

Ejemplo de tarea

Configuración de parámetros de Hive personalizados

Hive depende de HDFS. De forma predeterminada, Hive accede al cliente HDFS. Los parámetros de configuración que tienen efecto son controlados por HDFS de una manera unificada. Por ejemplo, el parámetro HDFS **ipc.client.rpc.timeout** afecta al período de tiempo de espera de RPC para que todos los clientes se conecten al servidor HDFS. Si necesita modificar el período de tiempo de espera para que Hive se conecte a HDFS, puede utilizar la función de personalización de configuración. Después de agregar este parámetro al archivo **core-site.xml** de Hive, este parámetro puede ser identificado por el servicio Hive y su configuración sobrescribe la configuración del parámetro en HDFS.

Paso 1 En la página de detalles del clúster de MRS, haga clic en **Components**.

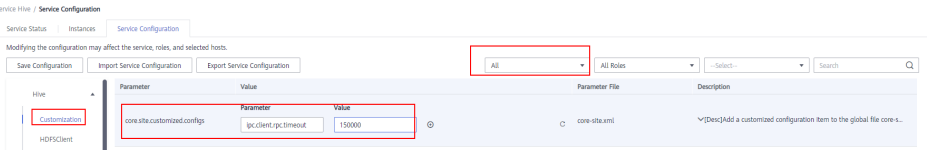
Paso 2 Elija **Hive** > **Service Configuration**.

Paso 3 En el cuadro desplegable de tipo de configuración del lado derecho, cambie **Basic** a **All**.

Paso 4 En el árbol de navegación de la izquierda, seleccione **Customization** para el servicio Hive. El sistema muestra los parámetros de servicio personalizados compatibles con Hive.

Paso 5 En **core-site.xml**, busque la fila que contiene el parámetro **core.site.customized.configs**, escriba **ipc.client.rpc.timeout** en la columna **Parameter** e introduzca un nuevo valor en la columna **Value**, por ejemplo, **150000**. La unidad es milisegundo.

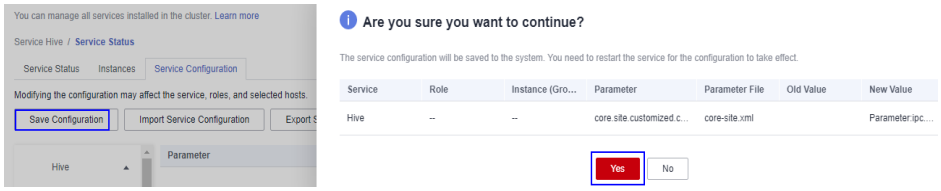
Figura 3-43 Configuración de parámetros personalizados (usando MRS 1.9.2 como ejemplo)



Paso 6 Haga clic en **Save Configuration**, seleccione **Restart the affected services or instances**, y haga clic en **OK**.

Se muestra **Operation successful**. Haga clic en **Finish**. El servicio se inicia correctamente.

Figura 3-44 Guardar configuraciones personalizadas



----Fin

3.7.6 Sincronización de la configuración del servicio

Escenario

Si **Configuration Status** de algunos servicios es **Configuration expired** o **Configuration failed**, sincronice la configuración del clúster o servicio para restaurar su estado de configuración. Si todos los servicios del clúster están en estado **Configuration failed**, sincronice la configuración del clúster con la configuración en segundo plano.

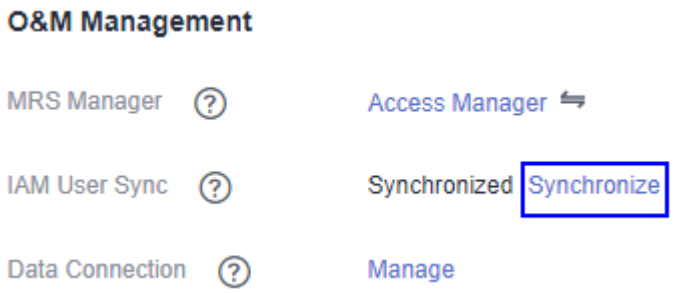
Impacto en el sistema

Después de sincronizar las configuraciones de servicio, debe reiniciar los servicios cuyas configuraciones han caducado. Estos servicios no están disponibles durante el reinicio.

Prerrequisitos

Tiene usuarios de IAM sincronizados. (En la página **Dashboard**, haga clic en **Synchronize** en el lado derecho de **IAM User Sync** para sincronizar usuarios de IAM.)

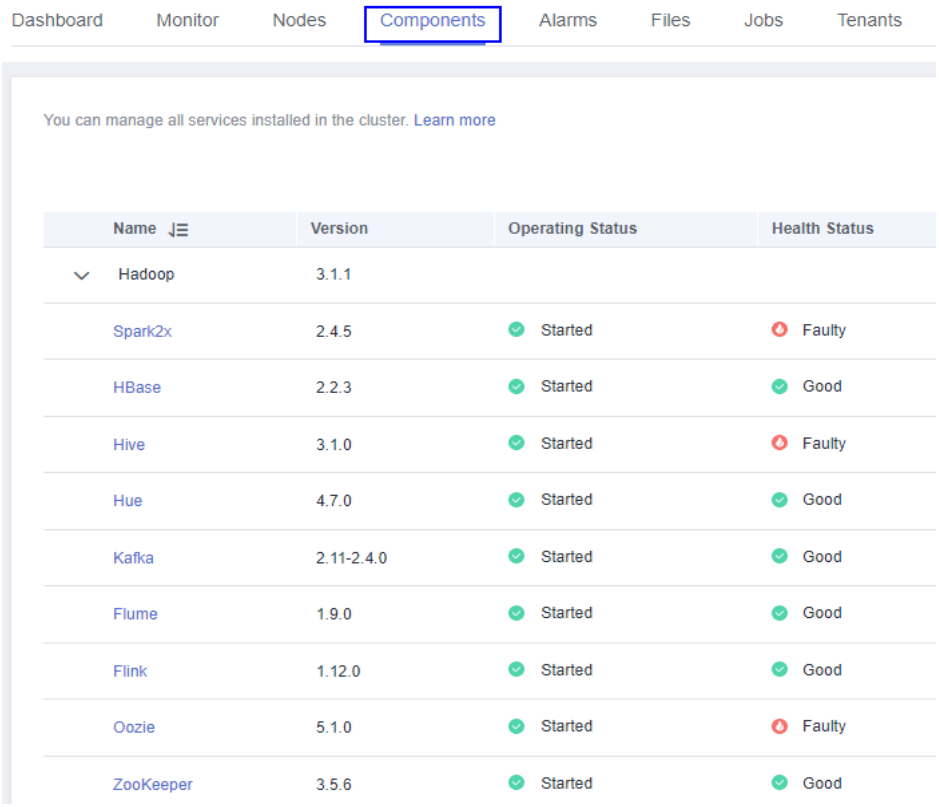
Figura 3-45 Sincronización de usuarios de IAM



Procedimiento

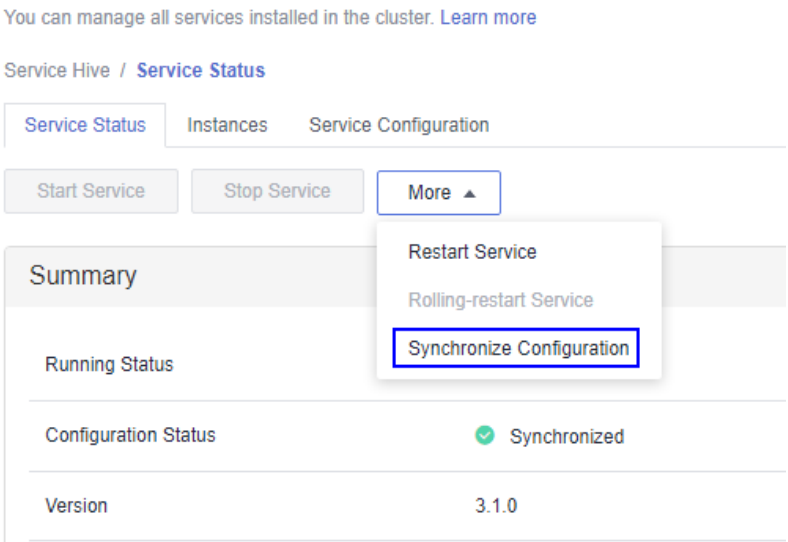
Paso 1 En la página de detalles del clúster de MRS, haga clic en **Components**.

Figura 3-46 Página de pestaña de componentes



Paso 2 Seleccione el servicio de destino en la lista de servicios.

Paso 3 En la página de la pestaña Service Status, elija **More** >**Synchronize Configuration**.



Paso 4 En el cuadro de diálogo que se muestra, seleccione **Restart the service or instances whose configurations have expired** y haga clic en **Yes** para reiniciar el servicio.

----Fin

3.7.7 Gestión de instancias de rol

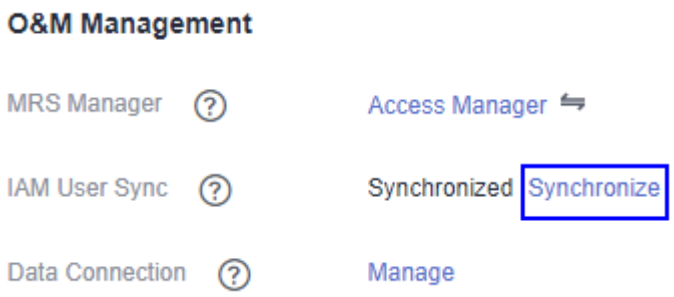
Escenario

Puede iniciar una instancia de rol que se encuentre en el estado **Stopped**, **Failed to stop** o **Failed to start**, detener una instancia de rol no utilizada o anormal o reiniciar una instancia de rol anormal para recuperar sus funciones.

Prerrequisitos

Tiene usuarios de IAM sincronizados. (En la página **Dashboard**, haga clic en **Synchronize** en el lado derecho de **IAM User Sync** para sincronizar usuarios de IAM.)

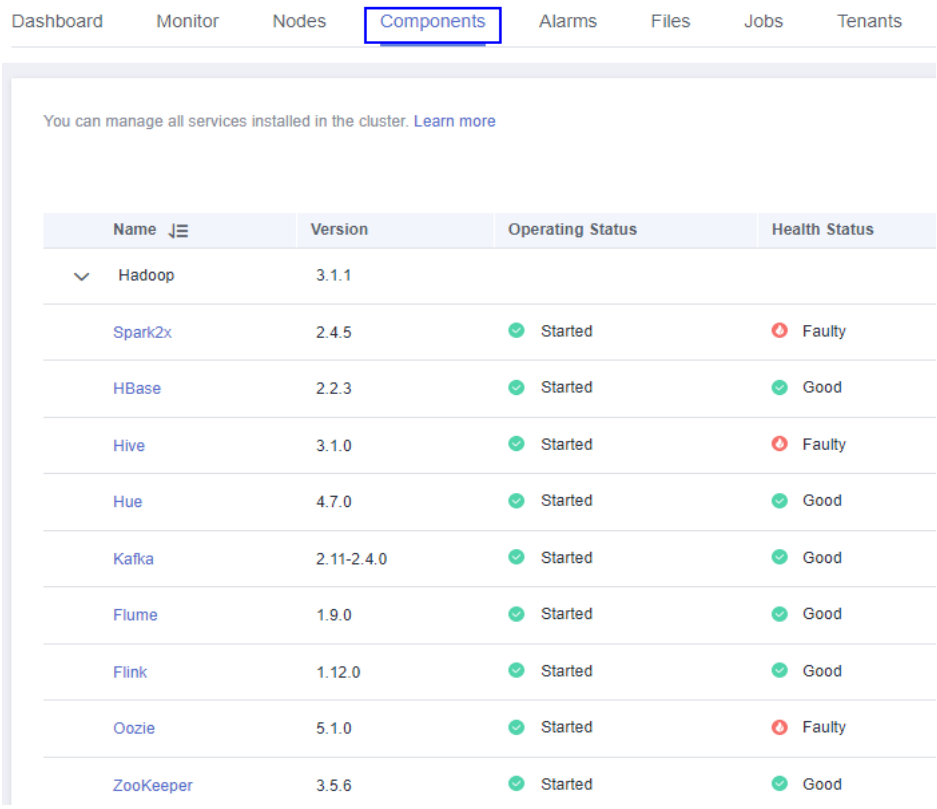
Figura 3-47 Sincronización de usuarios de IAM



Procedimiento

Paso 1 En la página de detalles del clúster, haga clic en la pestaña **Components**.

Figura 3-48 Página de pestaña de componentes

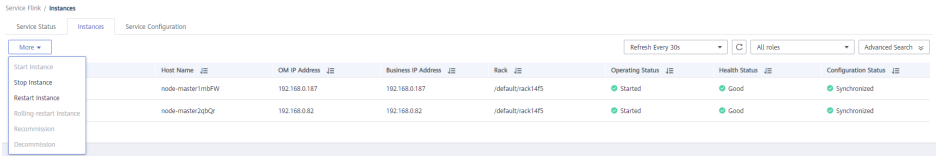


Paso 2 Seleccione el servicio de destino en la lista de servicios.

Paso 3 Haga clic en la pestaña **Instances**.

Paso 4 Seleccione la casilla de verificación situada a la izquierda de la instancia de rol de destino.

Paso 5 Haga clic en **More**, seleccione operaciones como **Start Instance**, **Stop Instance**, **Restart Instance**, **Rolling-restart Instance**, o **Delete Instance** según los requisitos del sitio.



----Fin

3.7.8 Configuración de parámetros de instancia de rol

Escenario

Puede ver y modificar la configuración de instancia de rol predeterminada en MRS según los requisitos del sitio. Las configuraciones se pueden importar y exportar.

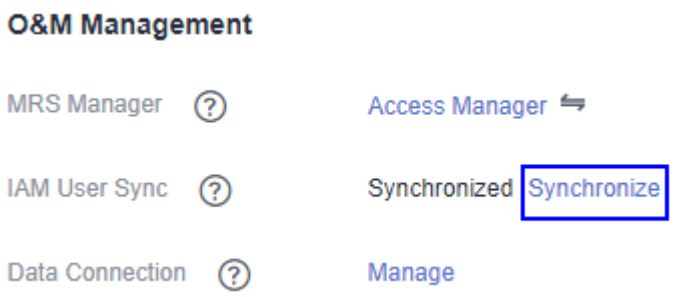
Impacto en el sistema

Debe descargar y actualizar los archivos de configuración del cliente después de configurar las propiedades de servicio HBase, HDFS, Hive, Spark, Yarn y MapReduce.

Prerrequisitos

Tiene usuarios de IAM sincronizados. (En la página **Dashboard**, haga clic en **Synchronize** en el lado derecho de **IAM User Sync** para sincronizar usuarios de IAM.)

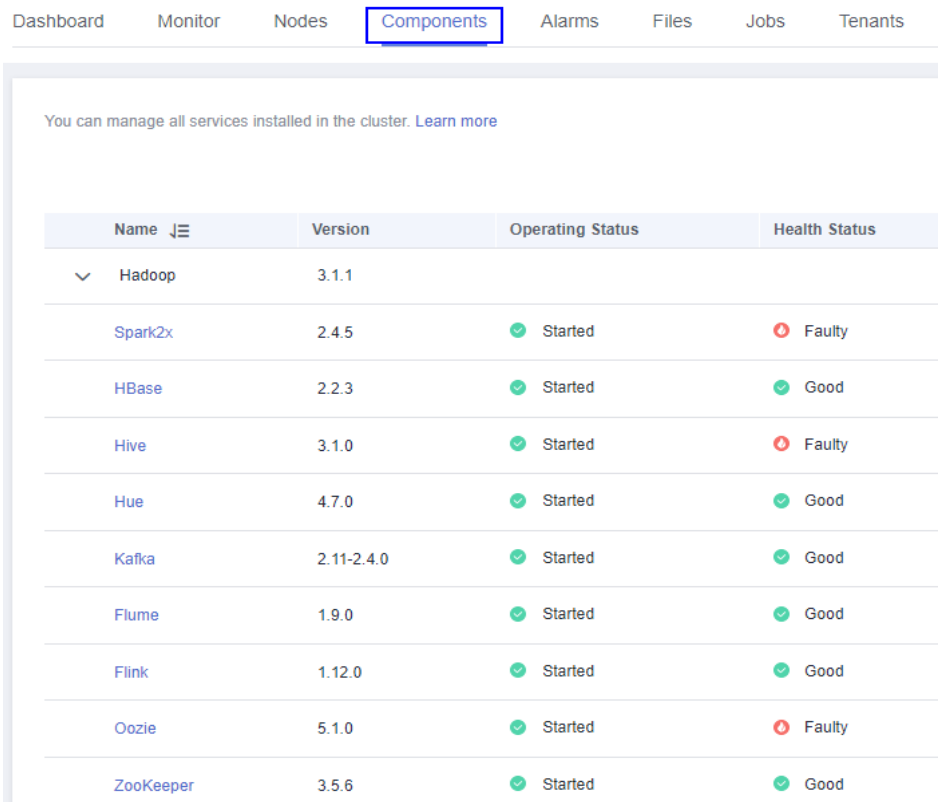
Figura 3-49 Sincronización de usuarios de IAM



Modificación de parámetros de instancia de rol

1. En la página de detalles del clúster, haga clic en la pestaña **Components**.

   Figura 3-50 Página de pestaña de componentes



2. Seleccione el servicio de destino en la lista de servicios.
3. Haga clic en la pestaña **Instances**.
4. Haga clic en la instancia de rol de destino en la lista de instancias de rol.
5. Haga clic en la pestaña **Instance Configuration**.

6. Cambie **Basic** a **All** desde la lista desplegable a la derecha de la página. Todos los parámetros de configuración de la instancia de rol se muestran en el árbol de navegación.
7. En el árbol de navegación, seleccione un parámetro especificado y cambie su valor. También puede introducir el nombre del parámetro en el cuadro **Search** para buscar el parámetro y ver el resultado.

   Si desea cancelar la modificación de un valor de parámetro, haga clic en para restaurarlo.
8. Haga clic en **Save Configuration**, seleccione **Restart the affected services or instances**, y haga clic en **OK**.

3.7.9 Sincronización de configuración de instancia de rol

Escenario

Cuando **Configuration Status** de una instancia de rol es **Configuration expired** o **Configuration failed**, puede sincronizar los datos de configuración de la instancia de rol con la configuración en segundo plano.

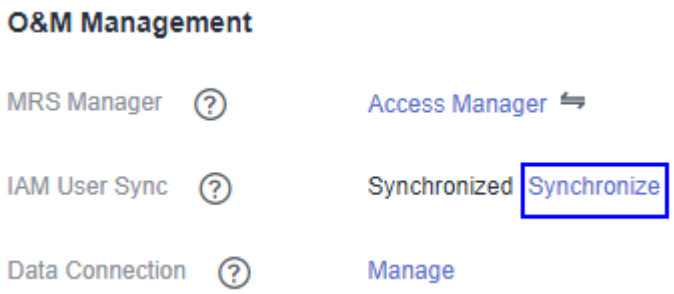
Impacto en el sistema

Después de sincronizar una configuración de instancia de rol, debe reiniciar la instancia de rol cuya configuración ha caducado. La instancia de rol no está disponible durante el reinicio.

Prerrequisitos

Tiene usuarios de IAM sincronizados. (En la página **Dashboard**, haga clic en **Synchronize** en el lado derecho de **IAM User Sync** para sincronizar usuarios de IAM.)

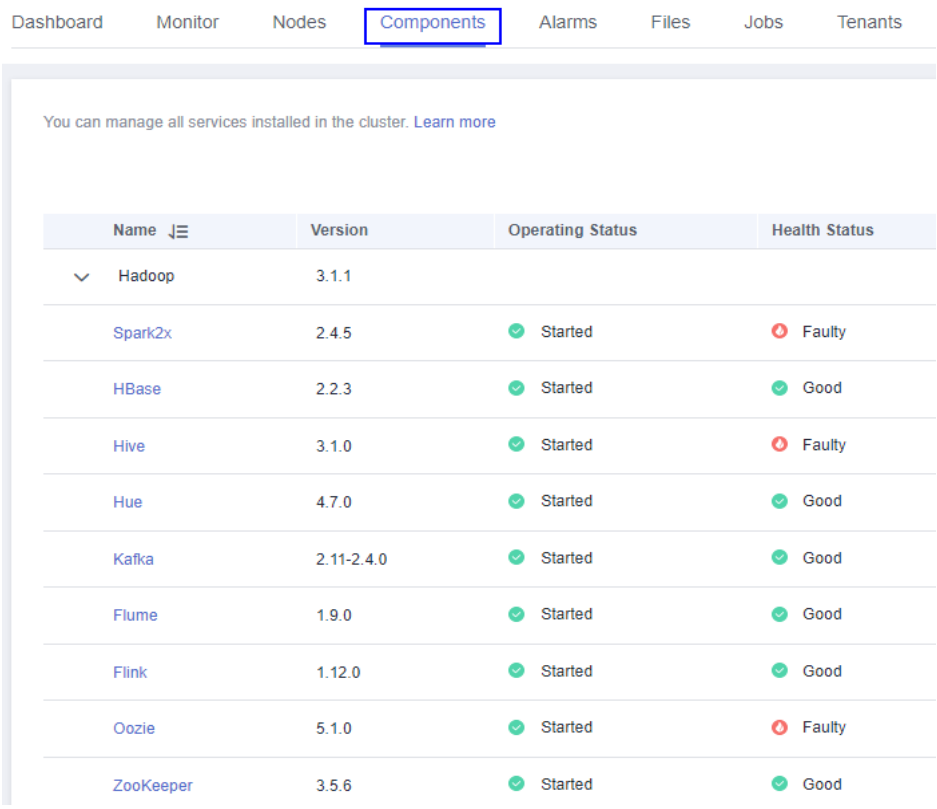
Figura 3-51 Sincronización de usuarios de IAM



Procedimiento

Paso 1 En la página de detalles del clúster, haga clic en la pestaña **Components**.

Figura 3-52 Página de pestaña de componentes

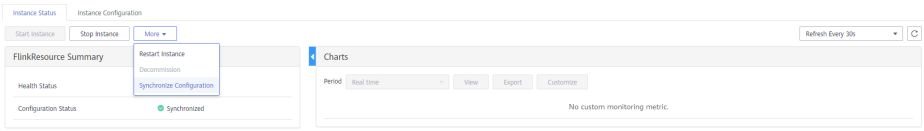


Paso 2 Seleccionar un nombre de servicio.

Paso 3 Haga clic en la pestaña **Instances**.

Paso 4 Haga clic en la instancia de rol de destino en la lista de instancias de rol.

Paso 5 Haga clic en **More** y seleccione **Synchronize Configuration** encima del estado de la instancia de rol y la información del indicador.



Paso 6 En el cuadro de diálogo que se muestra, seleccione **Restart the service or instances whose configurations have expired** y haga clic en **Yes** para reiniciar la instancia de rol.

----Fin

3.7.10 Desmantelar y volver a poner en servicio una instancia de rol

Escenario

Si un nodo Core o Task es defectuoso, el estado del clúster puede mostrarse como **Abnormal**. En un clúster de MRS, los datos se pueden almacenar en diferentes nodos de Core. Puede retirar la instancia de rol especificada en MRS para impedir que la instancia de rol

proporcione servicios. Después de la rectificación de errores, puede volver a poner en marcha la instancia de rol.

Las siguientes instancias de rol se pueden retirar o volver a poner en servicio:

- instancia de rol DataNode en HDFS
- instancia de rol de NodeManager en Yarn
- instancia de rol de RegionServer en HBase
- instancia de rol de ClickHouseServer en ClickHouse

  NOTA

  Las instancias de rol de ClickHouseServer solo se pueden desmantelar en MRS 3.1.2 o posterior.
- instancia de rol de broker en Kafka

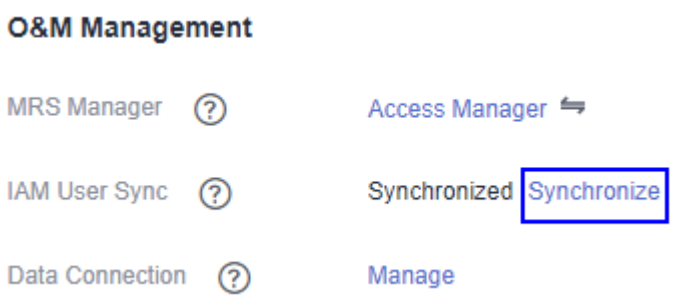
Restricciones:

- Si el número del DataNodes es menor o igual que el de las copias de HDFS, no se puede realizar el desmantelamiento. Si el número de copias de HDFS es tres y el número de DataNodes es inferior a cuatro en el sistema, no se puede realizar el desmantelamiento. En este caso, se informará de un error y obligará a MRS a salir del desmantelamiento 30 minutos después de que MRS intente realizar el desmantelamiento.
- Si el número de instancias de Kafka Broker es menor o igual que el de las copias de Kafka, no se puede realizar el desmantelamiento. Por ejemplo, si el número de copias de Kafka es dos y el número de nodos es inferior a tres en el sistema, no se puede realizar el desmantelamiento. El desmantelamiento de instancias fallará y saldrá. Si necesita equilibrar los datos después de cambiar los nodos Kafka, consulte **Instrucciones de herramienta de balanceo de Kafka**.
- Si una instancia de rol está fuera de servicio, debe volver a poner en servicio la instancia para iniciarla antes de volver a usarla.

Prerrequisitos

Tiene usuarios de IAM sincronizados. (En la página **Dashboard**, haga clic en **Synchronize** en el lado derecho de **IAM User Sync** para sincronizar usuarios de IAM.)

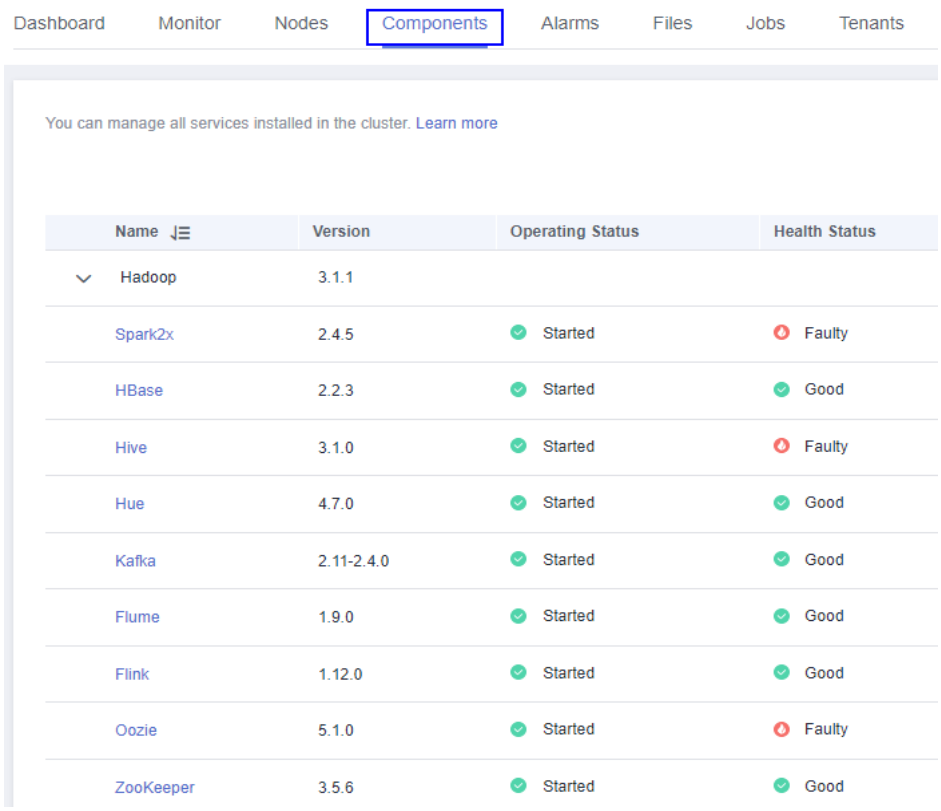
Figura 3-53 Sincronización de usuarios de IAM



Procedimiento

Paso 1 En la página de detalles del clúster, haga clic en la pestaña **Components**.

Figura 3-54 Página de pestaña de componentes

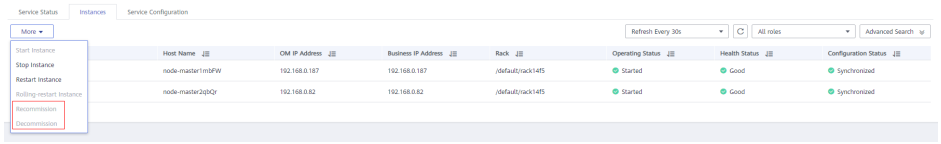


Paso 2 Haga clic en un servicio en la lista de servicios.

Paso 3 Haga clic en la pestaña **Instances**.

Paso 4 Seleccione una instancia.

Paso 5 Elija **More** > **Decommission** o **Recommission** para realizar la operación correspondiente.



NOTA

Durante la retirada de la instancia, si el servicio correspondiente a la instancia se reinicia en el clúster mediante otro navegador, MRS muestra un mensaje que indica que la retirada de la instancia se ha detenido, pero el **Operating Status** de la instancia se muestra como **Started**. En este caso, la instancia ha sido desmantelada en segundo plano. Para sincronizar el estado operativo, debe volver a desmantelar la instancia.

----Fin

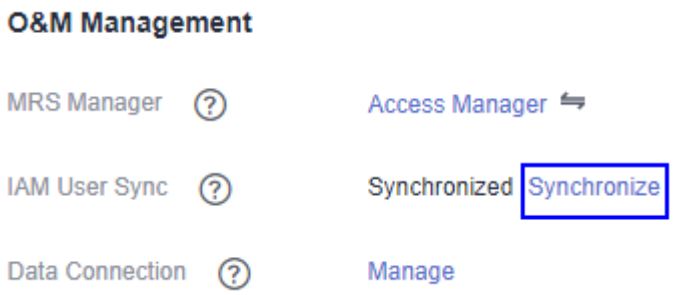
3.7.11 Inicio y detención de un clúster

Un clúster es una colección de componentes de servicio. Puede iniciar o detener todos los servicios de un clúster.

Prerrequisitos

Tiene usuarios de IAM sincronizados. (En la página **Dashboard**, haga clic en **Synchronize** en el lado derecho de **IAM User Sync** para sincronizar usuarios de IAM.)

Figura 3-55 Sincronización de usuarios de IAM



Procedimiento

En la página de detalles del clúster, elija **Management Operations** > **Start All Components** o **Stop All Components** en la esquina superior derecha para realizar la operación requerida.

3.7.12 Sincronización de la configuración del clúster

Escenario

Si **Configuration Status** de todos los servicios o de algunos servicios es **Configuration expired** or **Configuration failed**, sincronice la configuración del clúster o del servicio para restaurar su estado de configuración.

- Si todos los servicios del clúster están en estado **Configuration failed**, sincronice la configuración del clúster con la configuración en segundo plano.
- Si todos los servicios del clúster están en estado **Configuration failed**, sincronice la configuración del servicio con la configuración en segundo plano.

  NOTA

  En **MRS 3.x**, no puede realizar operaciones en esta sección de la consola de gestión.

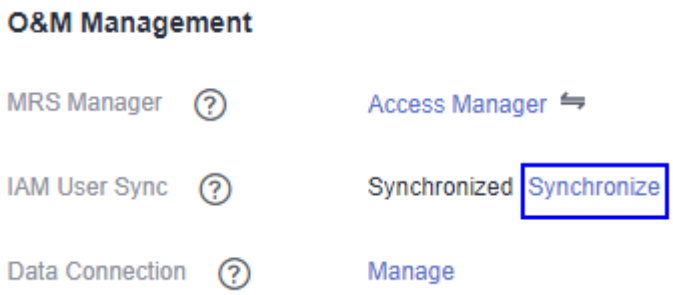
Impacto en el sistema

Después de sincronizar las configuraciones de clúster, debe reiniciar los servicios cuyas configuraciones han caducado. Estos servicios no están disponibles durante el reinicio.

Prerrequisitos

Tiene usuarios de IAM sincronizados. (En la página **Dashboard**, haga clic en **Synchronize** en el lado derecho de **IAM User Sync** para sincronizar usuarios de IAM.)

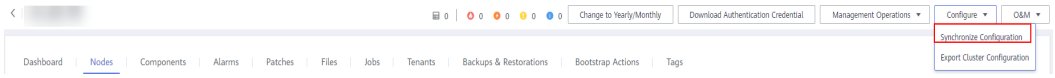
Figura 3-56 Sincronización de usuarios de IAM



Procedimiento

Paso 1 En la página de detalles del clúster, elija **Configuration** > **Synchronize Configuration** en la esquina superior derecha.

Figura 3-57 Sincronización de configuraciones (usando MRS 1.9.2 como ejemplo)



Paso 2 En el cuadro de diálogo mostrado, seleccione **Restart services and instances whose configuration have expired** y haga clic en **OK** para reiniciar el servicio cuya configuración ha caducado.

Cuando se muestre **Operation successful**, haga clic en **Finish**. El clúster se inicia correctamente.

----Fin

3.7.13 Exportación de configuración de clúster

Escenario

Puede exportar todos los datos de configuración de un clúster mediante MRS para cumplir con los requisitos del sitio. Los datos de configuración exportados se utilizan para actualizar rápidamente la configuración del servicio.

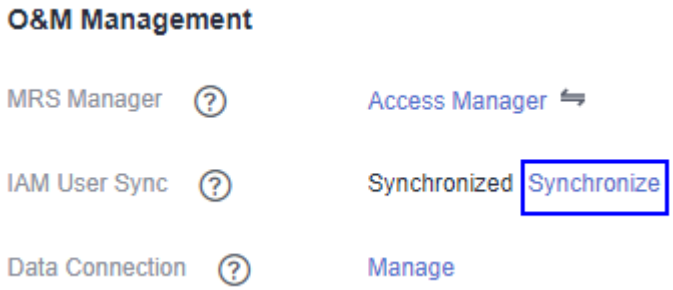
NOTA

En **MRS 3.x**, no puede realizar operaciones en esta sección de la consola de gestión.

Prerrequisitos

Tiene usuarios de IAM sincronizados. (En la página **Dashboard**, haga clic en **Synchronize** en el lado derecho de **IAM User Sync** para sincronizar usuarios de IAM.)

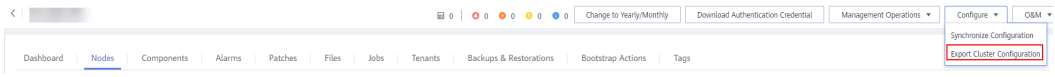
Figura 3-58 Sincronización de usuarios de IAM



Procedimiento

En la página de detalles del clúster, seleccione **Configuration** > **Export Cluster Configuration** en la esquina superior derecha.

Figura 3-59 Exportación de configuraciones de clúster (usando MRS 1.9.2 como ejemplo)



El archivo exportado se utiliza para actualizar las configuraciones de servicio. Para obtener más información, véase **Importación de parámetros de configuración de servicio** en la página web de **Configuración de parámetros de servicio**.

3.7.14 Realización de reinicio continuo

Después de modificar los elementos de configuración de un componente de big data, debe reiniciar el servicio correspondiente para que las nuevas configuraciones surtan efecto. Si utiliza un modo de reinicio normal, todos los servicios o instancias se reinician simultáneamente, lo que puede provocar una interrupción del servicio. Para asegurarse de que los servicios no se vean afectados durante el reinicio del servicio, puede reiniciar servicios o instancias en lotes mediante el reinicio continuo. Para las instancias en modo activo/en espera, una instancia en espera se reinicia primero y luego se reinicia una instancia activa. El reinicio continuo tarda más de lo normal.

Tabla 3-51 proporciona servicios e instancias que admiten o no admiten reinicio continuo en el clúster de MRS.

Tabla 3-51 Servicios e instancias que admiten o no admiten reinicio continuo

Servicio	Instancia	Si se admite el reinicio continuo
HDFS	NameNode	Sí
	Zkfc	
	JournalNode	
	HttpFS	

Servicio	Instancia	Si se admite el reinicio continuo
	DataNode	
Yarn	ResourceManager	Sí
	NodeManager	
Hive	MetaStore	Sí
	WebHCat	
	HiveServer	
Mapreduce	JobHistoryServer	Sí
HBase	HMaster	Sí
	RegionServer	
	ThriftServer	
	RESTServer	
Spark	JobHistory	Sí
	JDBCServer	
	SparkResource	No
Hue	Hue	No
Tez	TezUI	No
Loader	Sqoop	No
Zookeeper	Quorumpeer	Sí
Kafka	Broker	Sí
	MirrorMaker	No
Flume	Flume	Sí
	MonitorServer	
Storm	Nimbus	Sí
	UI	
	Supervisor	
	Logviewer	

Restricciones

- Realice un reinicio continuo durante las horas fuera de pico.

  - De lo contrario, puede producirse una falla de reinicio continuo. Por ejemplo, si el rendimiento de Kafka es alto (más de 100 MB/s) durante el reinicio de balanceo de Kafka, el reinicio de balanceo de Kafka puede fallar.
  - Por ejemplo, si las solicitudes por segundo de cada RegionServer en la interfaz nativa exceden 10,000 durante el reinicio continuo de HBase, debe aumentar el número de identificadores para evitar una falla de reinicio de RegionServer causado por cargas pesadas durante el reinicio.
- Antes del reinicio, compruebe el número de solicitudes actuales de HBase. Si el número de solicitudes de cada RegionServer en la interfaz nativa es superior a 10,000 aumente el número de identificadores para evitar un error.
- Si el número de nodos de Core en un clúster es inferior a seis, los servicios pueden verse afectados durante un corto período de tiempo.
- Preferentemente, realice un reinicio de instancia o servicio continuo y seleccione **Only restart instances whose configurations have expired**.

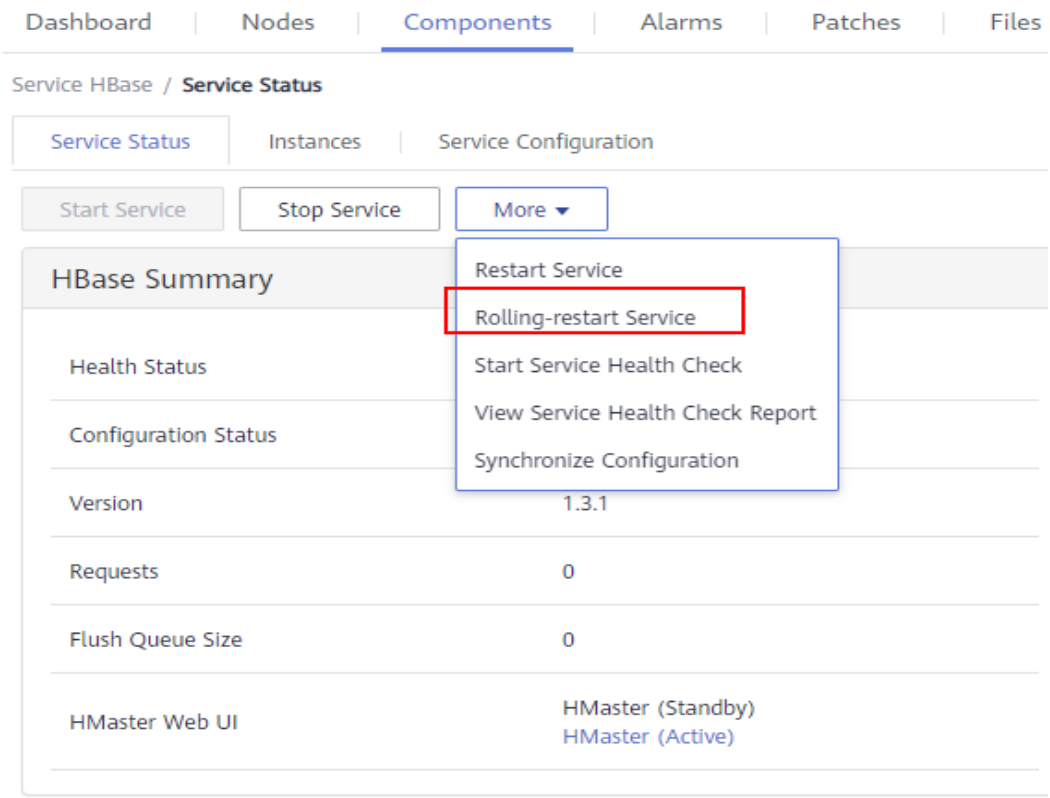
Realización de un reinicio de servicio continuo

Paso 1 Seleccione **Clusters** > **Active Clusters** y haga clic en un nombre de clúster para ir a la página de detalles del clúster.

Paso 2 Haga clic en **Components** y seleccione un servicio para el que desee realizar un reinicio continuo.

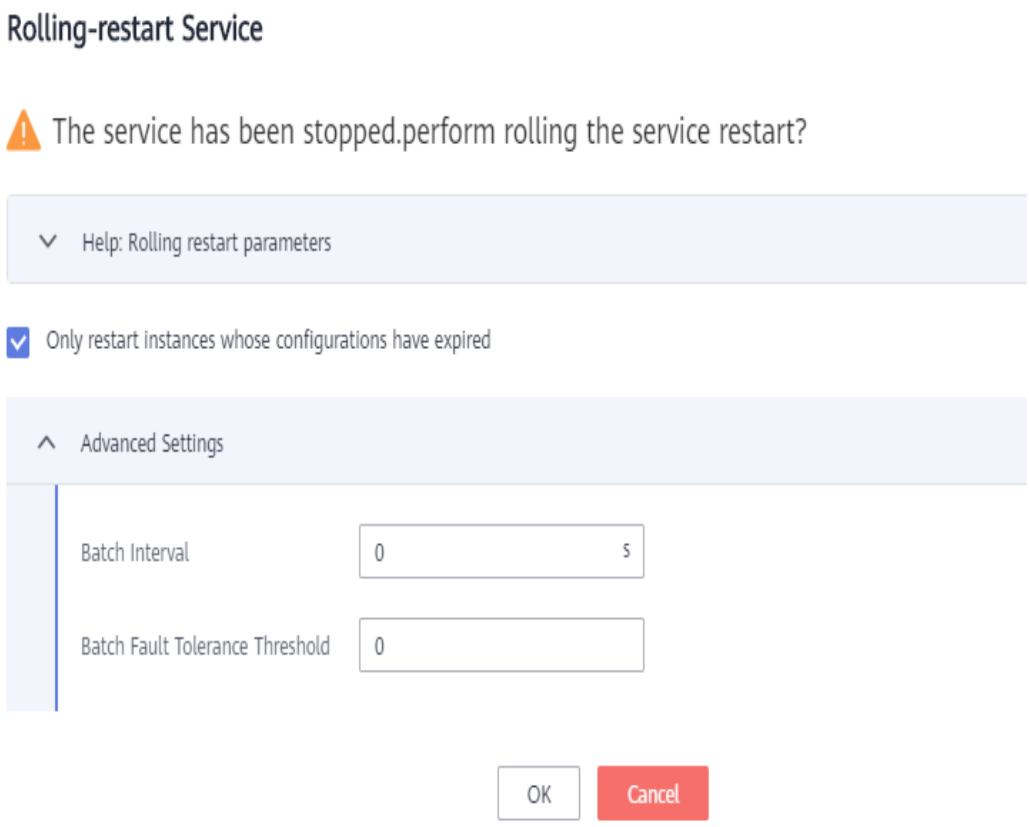
Paso 3 En la página de la pestaña **Service Status**, haga clic en **More** y seleccione **Rolling-restart Service**.

Figura 3-60 Estado del servicio (MRS 1.9.2 se usa como ejemplo)



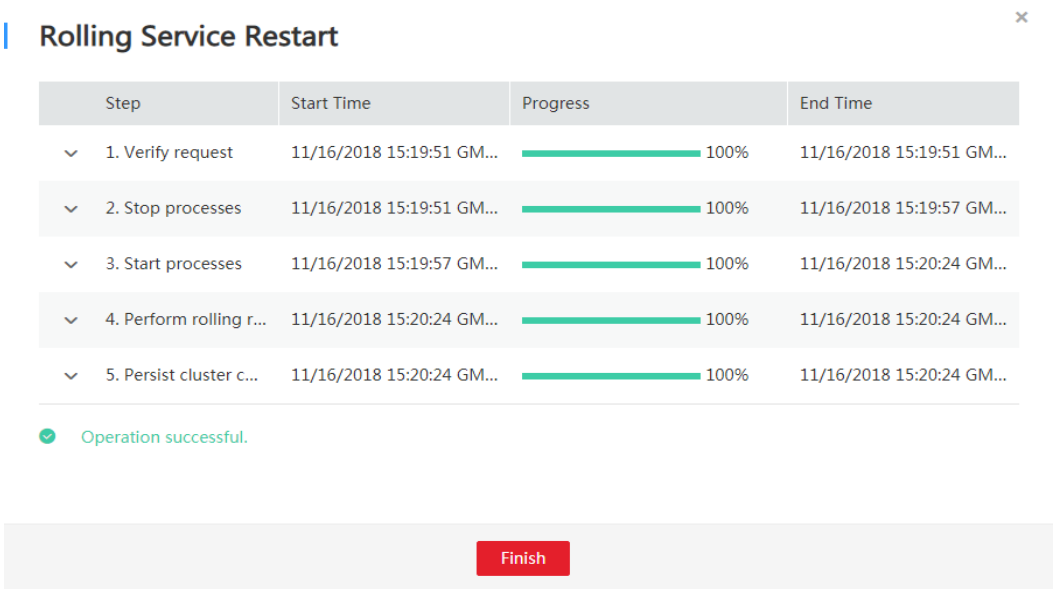
Paso 4 Se muestra la página **Rolling-restart Service**. Seleccione **Only restart instances whose configurations have expired** y haga clic en **OK** para realizar el reinicio continuo del servicio.

Figura 3-61 Realización de un reinicio de servicio continuo



Paso 5 Una vez completada la tarea de reinicio continuo, haga clic en **Finish**.

Figura 3-62 Finalización del reinicio del servicio continuo



----Fin

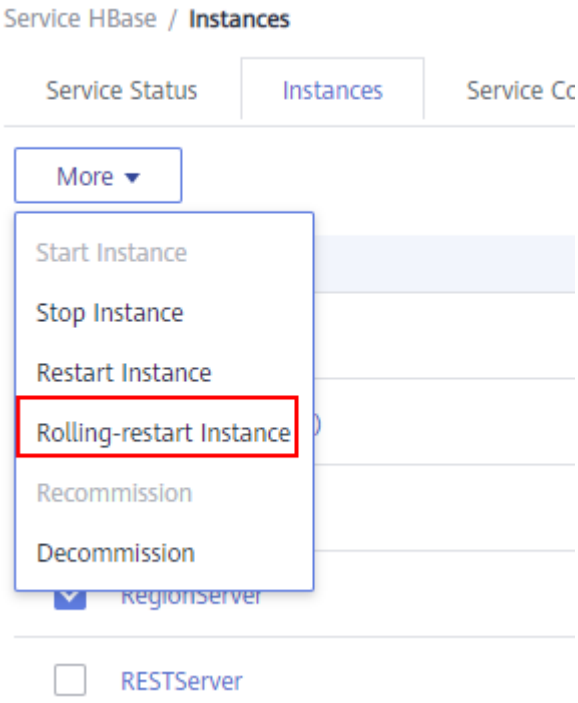
Realización de un reinicio continuo de instancia

Paso 1 Seleccione **Clusters** > **Active Clusters** y haga clic en un nombre de clúster para ir a la página de detalles del clúster.

Paso 2 Haga clic en **Components** y seleccione un servicio para el que desee realizar un reinicio continuo.

Paso 3 En la página de pestaña **Instance**, seleccione la instancia que desea reiniciar. Haga clic en **More** y seleccione **Rolling-restart Instance**.

Figura 3-63 Realización de un reinicio continuo de instancia



Paso 4 Después de introducir la contraseña de administrador, se muestra la página **Rolling-restart Instance**. Seleccione **Only restart instances whose configurations have expired** y haga clic en **OK** para realizar el reinicio continuo de la instancia.

Paso 5 Una vez completada la tarea de reinicio continuo, haga clic en **Finish**.

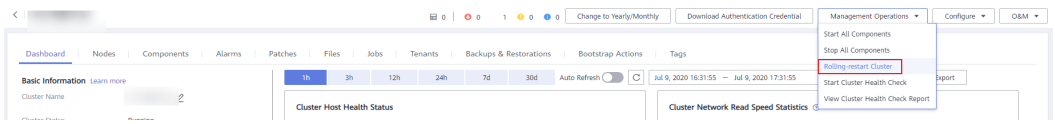
----Fin

Realizar un reinicio de clúster continuo

Paso 1 Seleccione **Clusters** > **Active Clusters** y haga clic en un nombre de clúster para ir a la página de detalles del clúster.

Paso 2 En la esquina superior derecha de la página, elija **Management Operations** >**Perform Rolling Cluster Restart**.

Figura 3-64 Realización de un reinicio continuo de un clúster (Uso de MRS 1.9.2 como ejemplo)



Paso 3 Se muestra la página **Rolling-restart Cluster**. Seleccione **Only restart instances whose configurations have expired** y haga clic en **OK** para realizar el reinicio continuo del clúster.

Paso 4 Una vez completada la tarea de reinicio continuo, haga clic en **Finish**.

----Fin

Descripción del parámetro de reinicio continuo

Tabla 3-52 describe los parámetros de reinicio continuo.

Tabla 3-52 Descripción del parámetro de reinicio de balanceo

Parámetro	Descripción
Only restart instances whose configurations have expired	Especifica si se deben reiniciar solo las instancias de un clúster que se hayan modificado.
Enable rack strategy	Si se debe habilitar la estrategia de reinicio continuo de rack simultáneos. Este parámetro solo tiene efecto para los roles que cumplen con la estrategia de reinicio continuo de rack. (Los roles admiten el reconocimiento de rack y las instancias de los roles pertenecen a dos o más racks.) **NOTA** Este parámetro es configurable solo cuando se realiza un reinicio continuo en HDFS y YARN en MRS 3.*x* o posterior.
Data Node Instances to Be Batch Restarted	Especifica la cantidad de instancias que se reinician en cada lote cuando se utiliza la estrategia de reinicio secuencial por lotes. El valor predeterminado es **1**. El valor varía de 1 a 20. Este parámetro solo es válido para nodos de datos.
Batch Interval	Especifica el intervalo entre dos lotes de instancias para el reinicio continuo. El valor predeterminado es **0**. El valor oscila entre 0 y 2147483647. La unidad es segunda. Nota: Establecer el parámetro de intervalo por lotes puede aumentar la estabilidad del proceso de componente de big data durante el reinicio continuo. Se recomienda establecer este parámetro en un valor no predeterminado, por ejemplo, 10.
Decommissioning Timeout Interval	Intervalo de desmantelamiento para instancias de rol durante un reinicio continuo.
Batch Fault Tolerance Threshold	Especifica los tiempos de tolerancia cuando el reinicio continuo de instancias no se ejecuta en lotes. El valor predeterminado es **0**, que indica que la tarea de reinicio continuo finaliza después de que no se reinicie ningún lote de instancias. El valor oscila entre 0 y 2147483647.

Procedimiento en un escenario típico

Paso 1 Seleccione **Clusters** > **Active Clusters** y haga clic en un nombre de clúster para ir a la página de detalles del clúster.

Paso 2 Haga clic en **Components** y seleccione **HBase**. Se muestra la página del servicio **HBase**.

Paso 3 Haga clic en la pestaña **Service Configuration**, modifique un parámetro HBase y guarde la configuración como se le solicite.

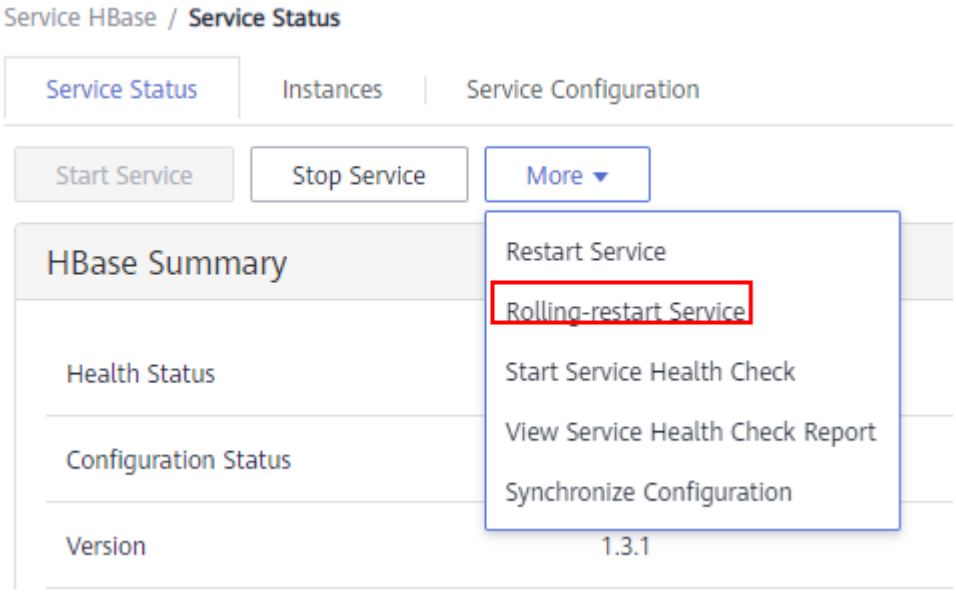
> **NOTA**
>
> En versiones anteriores a MRS 3.*x* no seleccione **Restart the affected services or instances**. Esta opción indica un reinicio normal. Si selecciona esta opción, se reiniciarán todos los servicios o instancias, lo que puede provocar una interrupción del servicio.

Paso 4 Después de guardar las configuraciones, haga clic en **Finish**.

Paso 5 Haga clic en la pestaña **Service Status**.

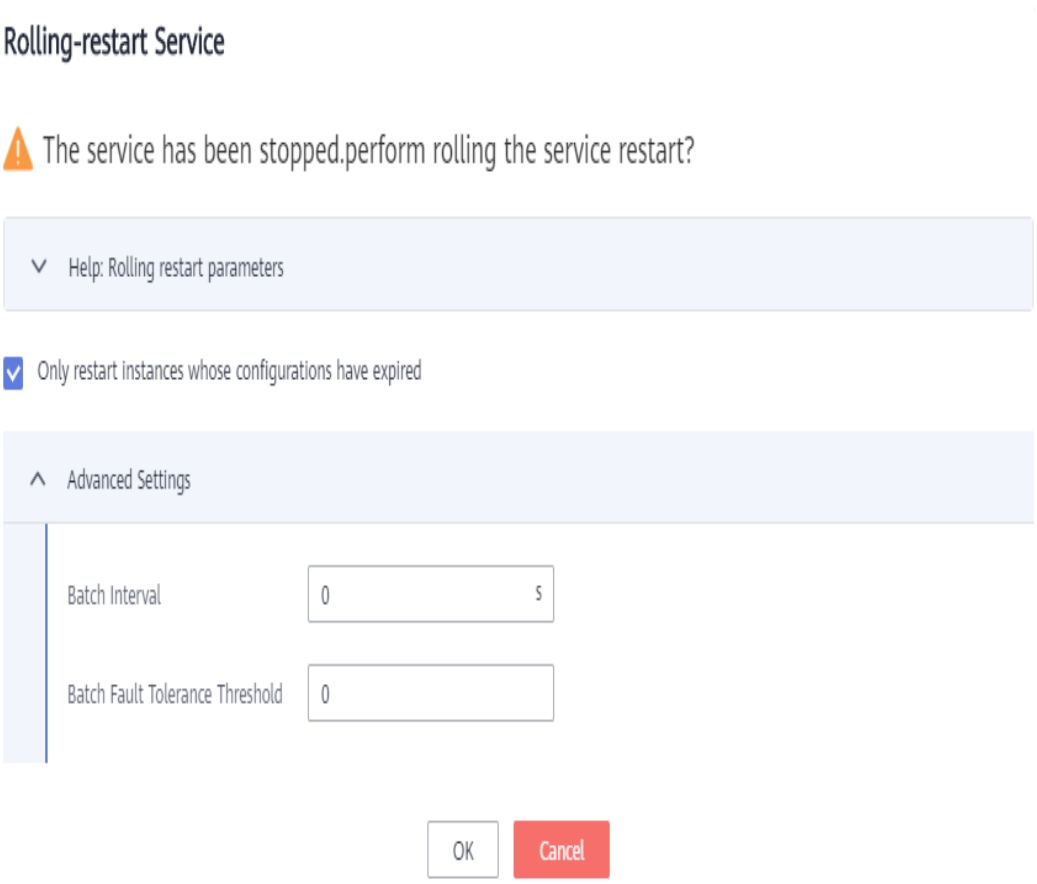
Paso 6 En la página de la pestaña **Service Status**, haga clic en **More** y seleccione **Rolling-restart Service**.

Figura 3-65 Estado del servicio - reinicio continuo (usando MRS 1.9.2 como ejemplo)



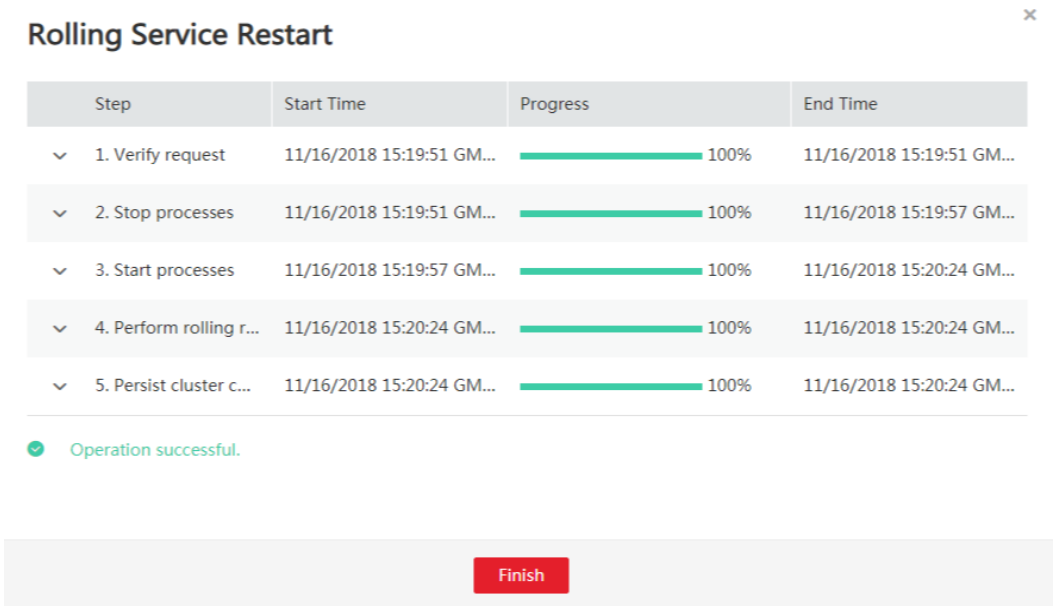
Paso 7 Después de introducir la contraseña de administrador, se muestra la página **Rolling-restart Service**. Seleccione **Only restart instances whose configurations have expired** y haga clic en **OK** para realizar el reinicio continuo.

Figura 3-66 Configuración del reinicio continuo del servicio



Paso 8 Una vez completada la tarea de reinicio continuo, haga clic en **Finish**.

Figura 3-67 Finalización del reinicio del servicio continuo



----Fin

3.8 Gestión de alarma

3.8.1 Visualización de la lista de alarmas

La lista de alarmas muestra todas las alarmas en el clúster de MRS. La página MRS muestra las alarmas que necesitan ser manejadas de manera oportuna y los eventos.

En la consola de gestión de MRS, solo puede consultar información básica sobre las alarmas de MRS no claras en la página de pestaña **Alarms**. Para obtener más información acerca de cómo ver los detalles de las alarmas o cómo gestionarlas, consulte **Consulta y eliminación manual de una alarma**.

Las alarmas se enumeran en orden cronológico por defecto en la lista de alarmas, con las alarmas más recientes mostradas en la parte superior.

Tabla 3-53 describe varios campos en una alarma.

Tabla 3-53 Descripción de la alarma

Parámetro	Descripción
Alarm ID	ID de una alarma.
Alarm Name	Nombre de una alarma.

Parámetro	Descripción
Severity	Severidad de alarma. En versiones anteriores a MRS 3.x, la gravedad de la alarma del clúster es la siguiente: ● Crítica Indica alarmas que informan errores que afectan a la ejecución del clúster, como servicios de clúster no disponibles, errores de nodo, incoherencia de datos entre las bases de datos de GaussDB activas y en espera y sincronización de datos de LdapServer anormal. Es necesario comprobar el estado del clúster basado en las alarmas y rectificar las fallas de manera oportuna. ● Grave Indica alarmas que informan de errores que afectan a algunas funciones del clúster, incluidos los errores de proceso, los errores periódicos de tareas de copia de respaldo y los permisos de archivos clave anormales. Compruebe los objetos para los que se generan las alarmas basándose en las alarmas y borre las alarmas de manera oportuna. ● Menor Indica alarmas que informan de errores que no afectan a las funciones principales del clúster actual, incluidas las alarmas que indican que el archivo de certificado está a punto de caducar, los registros de auditoría no se pueden volcar y el archivo de licencia está a punto de caducar. ● Advertencia Indica una alarma de la gravedad más baja. Se utiliza para mostrar información o solicitar información e indica que se produce un evento en los escenarios cuando se detiene un servicio, se elimina un servicio, se detiene una instancia, se elimina una instancia, se elimina un nodo, se reinicia un servicio, se reinicia una instancia, se realiza una conmutación activa/en espera para MRS Manager, escalar en un host o restaurar una instancia. Además, este tipo de alarmas también se produce cuando una instancia está defectuosa, un trabajo ejecutado correctamente o un trabajo no se puede ejecutar. En MRS 3.x o posterior, la gravedad de la alarma de un clúster es la siguiente: ● Crítica Indica alarmas que informan errores que afectan a la ejecución del clúster, como servicios de clúster no disponibles, errores de nodo, incoherencia de datos entre las bases de datos de GaussDB activas y en espera y sincronización de datos de LdapServer anormal. Es necesario comprobar el estado del clúster basado en las alarmas y rectificar las fallas de manera oportuna. ● Grave Indica alarmas que informan de errores que afectan a algunas funciones del clúster, incluidos los errores de proceso, los errores periódicos de tareas de copia de respaldo y los permisos de archivos clave anormales. Compruebe los objetos para los que se generan las

Parámetro	Descripción
	alarmas basándose en las alarmas y borre las alarmas de manera oportuna. ● Menor Indica alarmas que informan de errores que no afectan a las funciones principales del clúster actual, incluidas las alarmas que indican que el archivo de certificado está a punto de caducar, los registros de auditoría no se pueden volcar y el archivo de licencia está a punto de caducar. ● Sugerencia Indica una alarma de la gravedad más baja. Se utiliza para mostrar información o solicitar información e indica que se produce un evento en los escenarios cuando se detiene un servicio, se elimina un servicio, se detiene una instancia, se elimina una instancia, se elimina un nodo, se reinicia un servicio, se reinicia una instancia, se realiza una conmutación activa/en espera para MRS Manager, escalar en un host o restaurar una instancia. Además, este tipo de alarmas también se produce cuando una instancia está defectuosa, un trabajo ejecutado correctamente o un trabajo no se puede ejecutar.
Generated	Hora en que se genera la alarma.
Location	Detalles sobre la alarma.
Operation	Si la alarma se puede borrar manualmente, haga clic en **Clear Alarm**. Para ver detalles sobre una alarma, haga clic en **View Help**. (Esta función está disponible en MRS 3.*x* o posterior).

Tabla 3-54 Descripción de botones

Botón	Descripción
	Seleccione un intervalo para actualizar la lista de alarmas de la lista desplegable. ● Actualizar cada 30s ● Actualizar cada 60s ● Dejar de actualizar
	Seleccione una gravedad de alarma en el cuadro de lista desplegable para filtrar las alarmas. Para versiones anteriores a MRS 3.x, se pueden filtrar las siguientes alarmas: Todas, Crítica, Mayor, Menor y Advertencia. (Para MRS 3.x o posterior) Puede filtrar las siguientes alarmas: Todas, Crítica, Mayor, Menor y Advertencia.
	Haga clic en  y actualice manualmente la lista de alarmas.

Botón	Descripción
Advanced Search	Haga clic en **Advanced Search**. En el área de búsqueda de alarmas mostrada, establezca criterios de búsqueda y haga clic en **Search** para ver la información sobre las alarmas especificadas. Puede hacer clic en **Reset** para borrar los criterios de búsqueda.

3.8.2 Consulta de la lista de eventos

La lista de eventos muestra información acerca de todos los eventos de un clúster, como el reinicio del servicio y la terminación del servicio.

Los eventos se enumeran en la lista de eventos en orden cronológico de forma predeterminada, con los eventos más recientes mostrados en la parte superior.

NOTA

Solo MRS 2.x y versiones posteriores soportan esta función. Debe asegurarse de que se ha completado la sincronización del usuario de IAM.

Tabla 3-55 describe varios campos para un evento.

Tabla 3-55 Descripción del evento

Parámetro	Descripción
Event ID	Especifica el ID de un evento.
Event Severity	Especifica la gravedad del evento. En versiones anteriores a MRS 3.x, el nivel de evento de clúster es el siguiente: ● Crítica ● Grave ● Menor ● Sugerencia En MRS 3.x o posterior, el nivel de evento de un clúster es el siguiente: ● Crítica ● Grave ● Menor ● Sugerencia
Event Name	Nombre del evento generado.
Generated	Hora en la que se genera el evento.
Location	Especifica la información detallada para localizar el evento,

Tabla 3-56 Descripción de íconos

Ícono	Descripción
	Seleccione un intervalo para actualizar la lista de eventos de la lista desplegable. ● Actualizar cada 30s ● Actualizar cada 60s ● Dejar de actualizar
	Haga clic en para actualizar manualmente la lista de eventos.
Búsqueda avanzada	Haga clic en **Advanced Search**. En el área de búsqueda de eventos que se muestra, establezca criterios de búsqueda y haga clic en **Search** para ver la información sobre los eventos especificados. Haga clic en **Reset** para borrar los criterios de búsqueda.

Exportación de eventos

Paso 1 Elija **Clusters > Active Clusters** y haga clic en un nombre de clúster para ir a la página de detalles del clúster.

Paso 2 Haga clic en **Alarm Management** > **Events**.

Paso 3 Haga clic en **Export All**.

Paso 4 En el cuadro de diálogo que aparece, seleccione el tipo y haga clic en **OK**.

----Fin

Eventos Comunes

Tabla 3-57 Eventos comunes

ID del evento	Nombre del evento
12019	Stop Service
12020	Delete Service
12021	Stop RoleInstance
12022	Delete RoleInstance
12023	Delete Node
12024	Restart Service
12025	Restart RoleInstance
12026	Manager Switchover

ID del evento	Nombre del evento
12065	Restart Process
12070	Job Running Succeeded
12071	Job Running Failed
12072	Job Killed
12086	Restart Agent
12152	Start Periodic Replication
12153	Periodic Replication Completed
12154	Start Streaming Replication
12155	Restart Streaming Replication
12156	Stop Streaming Replication
12157	Skip Periodic Synchronization
14005	NameNode Switchover
14028	HDFS DiskBalancer Task
14029	Active NameNode Entered Security Mode and Generated New Fsimage
17001	Oozie Workflow Execution Failure
17002	Oozie Scheduled Job Execution Failure
18001	ResourceManager Switchover
18004	JobHistoryServer Switchover
19001	HMaster Failover
20003	Hue Failover
24002	Flume Channel Overflow
25001	LdapServer Failover
27000	DBServer Switchover
29001	Impala HaProxy Active/Standby Switchover
29002	Impala StateStoreCatalog Active/Standby Switchover
38003	Adjust Topic Data Storage Period
43014	Spark2x Data Skew
43015	Spark2x SQL Large Query Results
43016	Spark2x SQL Execution Timeout

ID del evento	Nombre del evento
43024	Start JDBCServer
43025	Stop JDBCServer
43026	ZooKeeper Connection Succeeded
43027	Zookeeper Connection Failed
44003	Coordinator Switchover

3.8.3 Consulta y eliminación manual de una alarma

Escenario

Puede ver y borrar las alarmas en MRS.

Generalmente, el sistema borra automáticamente una alarma cuando se rectifica la falla. Si la falla ha sido rectificado y la alarma no se puede borrar automáticamente, puede borrar la alarma manualmente.

Puede ver las últimas 100,000 alarmas (incluidas las alarmas borradas, borradas manualmente y borradas automáticamente) en MRS. Si el número de alarmas borradas supera los 100,000 y está a punto de alcanzar los 110,000, el sistema descarga automáticamente las primeras 10,000 alarmas borradas al recorrido de volcado.

3. En versiones anteriores a x, el valor es el mismo que el de ${BIGDATA_HOME}/OMSV100R001C00x8664/workspace/data para el nodo de gestión activo.

(Para las versiones 3.x y posteriores) La ruta es **${BIGDATA_HOME}/om-server/OMS/workspace/data** del nodo de gestión activo.

Un directorio se genera automáticamente cuando las alarmas se descargan por primera vez.

NOTA

Establezca un intervalo de actualización automática o haga clic en  para una actualización inmediata.

Se admiten las siguientes opciones de intervalo de actualización:

- Refrescar cada 30 segundos
- Refrescar cada 60 segundos
- Dejar de actualizar

Procedimiento

Paso 1 Elija **Clusters > Active Clusters** y haga clic en un nombre de clúster para ir a la página de detalles del clúster.

Paso 2 Haga clic en **Alarms** y vea la información de alarma en la lista de alarmas.

- De forma predeterminada, la página de lista de alarmas muestra las últimas 10 alarmas.
- De forma predeterminada, los datos se ordenan en orden descendente según el tiempo de generación. Para MRS 3.x o anterior, puede hacer clic en el ID de alarma, la gravedad y

el tiempo de generación para modificar el modo de ordenación. Para los clústeres de MRS 3.x o posterior, puede hacer clic en la gravedad y el tiempo de generación para modificar el modo de ordenación.

- Puede filtrar todas las alarmas de la misma gravedad. Los resultados incluyen alarmas despejadas y no claras.
- Para clústeres de MRS 3.x y versiones anteriores, puede hacer clic en  ,  , o  en la esquina superior derecha de la página para filtrar rápidamente las alarmas **Critical**, **Major**, **Minor** o **Suggestion** que no estén claras.
- Para clústeres de MRS 3.x o posterior: Puede hacer clic en  ,  , o  en la esquina superior derecha de la página para filtrar rápidamente las alarmas no claras **Critical**, **Major**, **Minor** o **Warning**.

Paso 3 Haga clic en **Advanced Search**. En el área de búsqueda de alarmas mostrada, establezca criterios de búsqueda y haga clic en **Search** para ver la información sobre las alarmas especificadas. Puede hacer clic en **Reset** para borrar los criterios de búsqueda.

NOTA

La hora de inicio y la hora de finalización se especifican en **Time Range**. Puede buscar las alarmas generadas dentro del rango de tiempo.

Manejar la alarma haciendo referencia a **Alarm Reference**. Si las alarmas en algunos escenarios se generan debido a otros servicios en la nube de los que depende MRS, debe ponerse en contacto con el personal de mantenimiento de los servicios en la nube correspondientes.

Paso 4 Si la alarma necesita ser borrada manualmente después de corregir los errores, haga clic en **Clear Alarm**.

NOTA

Si se han manejado varias alarmas, puede seleccionar una o más alarmas para borrarlas y hacer clic en **Clear Alarm** para borrar las alarmas por lotes. Se puede eliminar un máximo de 300 alarmas en cada lote.

----Fin

Exportación de alarmas

Paso 1 Elija **Clusters > Active Clusters** y haga clic en un nombre de clúster para ir a la página de detalles del clúster.

Paso 2 Haga clic en **Alarm Management** > **Alarms**.

Paso 3 Haga clic en **Export All**.

Paso 4 En el cuadro de diálogo que aparece, seleccione el tipo y haga clic en **OK**.

----Fin

3.9 Gestión de parches

3.9.1 Patch Operation Guide for MRS 3.1.5

Install the cluster version patch as required if you obtain patch information from:

- The message center service
- The **Patches** > **Cluster Component Patches** tab page

Preparing for Patch Installation

ATENCIÓN

- For details about how to check the cluster status, see section **Realización de una comprobación de estado**. Exceptions such as cluster node faults and hard disk faults may cause patch installation and uninstallation failures. Before you install or uninstall the patch, ensure that the cluster is healthy.
- Click **Patches** then **Cluster Component Patches**, click **Learn more** in the **Patch Description** column of the target patch, read the patch description carefully, and understand the patch installation procedure and impact.

Installing a Patch

Paso 1 Log in to the MRS management console.

Paso 2 Choose **Clusters** > **Active Clusters** and click the name of the desired cluster.

Paso 3 Click **Patches** then **Cluster Component Patches**, find the target patch in the patch list, and click **Install** in the **Operation** column. Wait until the patch is successfully installed.

Paso 4 Restart the component and install the client patch according to the patch description.

NOTA

If there is an isolated host in the cluster, the patch will not be installed on the isolated host. In this case, when the installation completes, the patch is partially installed. After the isolated node is restored and the isolation is canceled, you can install the patch again. In this case, the patch is installed only on the node whose isolation is canceled.

----Fin

Uninstalling a Patch

Paso 1 Log in to the MRS management console.

Paso 2 Choose **Clusters** > **Active Clusters** and click the name of the desired cluster.

Paso 3 Click **Patches** then **Cluster Component Patches**, find the target patch in the patch list, and click **Uninstall** in the **Operation** column.

Paso 4 Restart the component and uninstall the client patch according to the patch description.

NOTA

If there is an isolated host in the cluster, the patch will not be uninstalled on the isolated host. In this case, when the uninstallation completes, the patch is partially uninstalled. After the isolated node is restored and the isolation is canceled, you can uninstall the patch again. In this case, the patch is uninstalled only on the node whose isolation is canceled.

----Fin

3.9.2 Parches rodantes

La función de parche rodante indica que los parches se instalan o desinstalan para uno o más servicios en un clúster realizando un reinicio de servicio rodante (reiniciar servicios o instancias en lotes), sin interrumpir los servicios o dentro de un intervalo de interrupción de servicio minimizado. Los servicios de un clúster se dividen en los tres tipos siguientes en función de si admiten parches rodantes:

- Servicios que admiten la instalación o desinstalación de parches rodantes: Todas las empresas o parte de ellas (variando en función de los diferentes servicios) de los servicios no se interrumpen durante la instalación o desinstalación de parches.
- Servicios que no admiten la instalación o desinstalación de parches rodantes: los negocios de los servicios se interrumpen durante la instalación o desinstalación de parches.
- Servicios con algunas funciones que admiten la instalación o desinstalación de parches rodantes: Algunas empresas de los servicios no se interrumpen durante la instalación o desinstalación de parches.

NOTA

En **MRS 3.x**, no puede realizar operaciones en esta sección de la consola de gestión.

Tabla 3-58 proporciona servicios e instancias que admiten o no admiten reinicio rodante en el clúster MRS.

Tabla 3-58 Servicios e instancias que admiten o no admiten reinicio rodante

Servicio	Instancia	Si se admite el reinicio rodante
HDFS	NameNode	Sí
	Zkfc	
	JournalNode	
	HttpFS	
	DataNode	
Yarn	ResourceManager	Sí
	NodeManager	
Hive	MetaStore	Sí
	WebHCat	

Servicio	Instancia	Si se admite el reinicio rodante
	HiveServer	
MapReduce	JobHistoryServer	Sí
HBase	HMaster	Sí
	RegionServer	
	ThriftServer	
	RESTServer	
Spark	JobHistory	Sí
	JDBCServer	
	SparkResource	No
Hue	Hue	No
Tez	TezUI	No
Loader	Sqoop	No
Zookeeper	Quorumpeer	Sí
Kafka	Broker	Sí
	MirrorMaker	No
Flume	Flume	Sí
	MonitorServer	
Storm	Nimbus	Sí
	UI	
	Supervisor	
	LogViewer	

Instalación de un parche

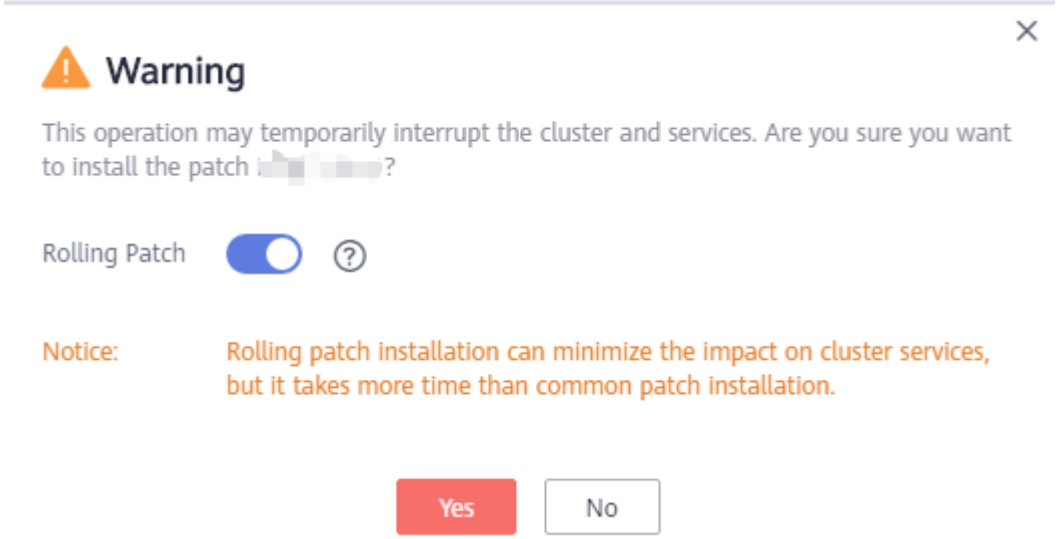
Paso 1 Inicie sesión en la consola de MRS.

Paso 2 Seleccione **Clusters** > **Active Clusters** y haga clic en el nombre del clúster que se va a consultar para entrar en la página que muestra la información básica del clúster.

Paso 3 En la página **Patches**, haga clic en **Install** en la columna **Operation**.

Paso 4 En la página **Warning**, active o desactive **Rolling Patch**.

Figura 3-68 Instalación de parches rodantes



NOTA

- Activación de la función de instalación de parches continuos: los servicios no se detienen antes de la instalación del parche y el reinicio del servicio continuo se realiza después de la instalación del parche. Esto minimiza el impacto en los servicios de clúster, pero lleva más tiempo que la instalación de parches común.
- Desactivación de la función de desinstalación continua de parches: Todos los servicios se detienen antes de la desinstalación de parches y todos los servicios se reinician después de la desinstalación de parches. Esto interrumpe temporalmente el clúster y los servicios, pero toma menos tiempo que la desinstalación continua de parches.
- La función de instalación de parches continuos no está disponible en clústeres con menos de dos nodos de Master y tres nodos de Core.

Paso 5 Haga clic en **Yes** para instalar el parche de destino.

Paso 6 Vea el progreso de la instalación del parche.

1. Acceda a MRS Manager. Para obtener más información, consulte **Acceso a MRS Manager (MRS 2.x o anterior)**.
2. Elija **System** > **Manage Patch**. En la página **Manage Patch**, puede ver el progreso de la instalación del parche.

NOTA

Para los nodos host aislados del clúster, siga las instrucciones en **Restauración de parches para los hosts aislados** para restaurar el parche.

----Fin

Desinstalación de un parche

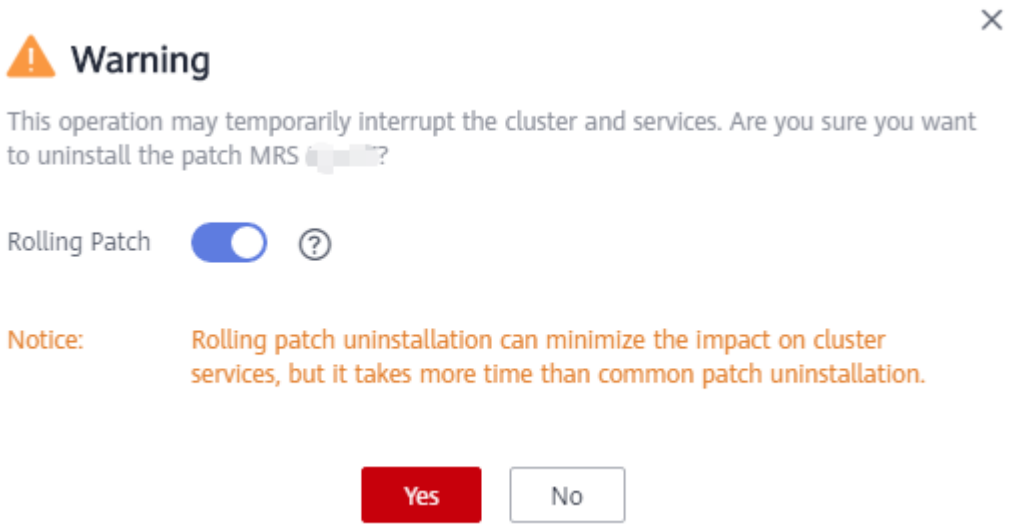
Paso 1 Inicie sesión en la consola de MRS.

Paso 2 Seleccione **Clusters** > **Active Clusters** y haga clic en el nombre del clúster que se va a consultar para entrar en la página que muestra la información básica del clúster.

Paso 3 En la página **Patches**, haga clic en **Uninstall** en la columna **Operation**.

Paso 4 En la página **Warning**, active o desactive **Rolling Patch**.

Figura 3-69 Desinstalación de parche rodante



NOTA

- Activación de la función de desinstalación de parches continuos: los servicios no se detienen antes de la desinstalación de parches y el reinicio de servicio continuo se realiza después de la desinstalación de parches. Esto minimiza el impacto en los servicios de clúster, pero lleva más tiempo que la desinstalación de parches común.
- Desactivación de la función de desinstalación continua de parches: Todos los servicios se detienen antes de la desinstalación de parches y todos los servicios se reinician después de la desinstalación de parches. Esto interrumpe temporalmente el clúster y los servicios, pero toma menos tiempo que la desinstalación continua de parches.
- Sólo los parches que se instalan en modo rodante se pueden desinstalar en el mismo modo.

Paso 5 Haga clic en **Yes** para desinstalar el parche de destino.

Paso 6 Vea el progreso de la desinstalación del parche.

1. Acceda a MRS Manager. Para obtener más información, consulte **Acceso a MRS Manager (MRS 2.x o anterior)**.
2. Elija **System** > **Manage Patch**. En la página **Manage Patch**, puede ver el progreso de la desinstalación del parche.

NOTA

Para los nodos host aislados del clúster, siga las instrucciones en **Restauración de parches para los hosts aislados** para restaurar el parche.

----Fin

3.9.3 Restauración de parches para los hosts aislados

Si algunos hosts están aislados en un clúster, realice las siguientes operaciones para restaurar los parches para estos hosts aislados después de la instalación de parches en otros hosts del

clúster. Después de la restauración de parches, las versiones de los nodos host aislados son consistentes con aquellos no están aislados.

NOTA

En **MRS 3.x**, no puede realizar operaciones en esta sección de la consola de gestión.

Paso 1 Acceda a MRS Manager. Para obtener más información, consulte **Acceso a MRS Manager (MRS 2.x o anterior)**.

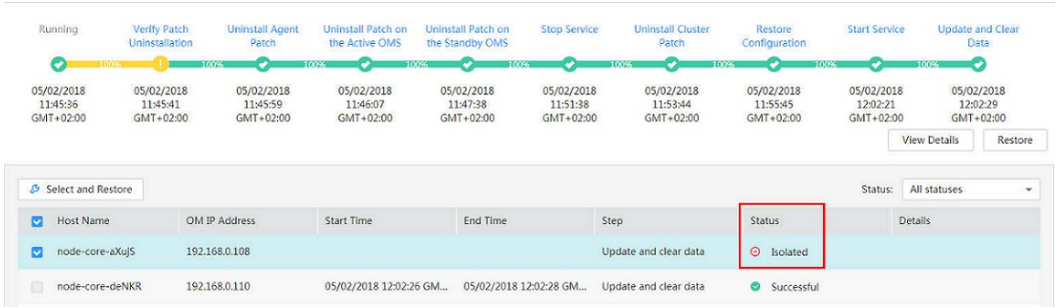
Paso 2 Elija **System > Manage Patch**. Se muestra la página **Manage Patch**.

Paso 3 En la columna **Operation**, haga clic en **View Details**.

Paso 4 En la página de detalles del parche, seleccione los nodos de host cuyo **Status** sea **Isolated**.

Paso 5 Haga clic en **Select and Restore** para restaurar los nodos de host aislados.

Figura 3-70 Restauración de parches para los hosts aislados



----Fin

3.9.4 Descripción de parche de MRS

3.9.4.1 Corregida la vulnerabilidad de escalada de privilegios del usuario omm

Versión aplicable

Todas las versiones de MRS

Problema resuelto

Rectifique el problema de que el usuario **omm** puede usar el script **installSudoExecute.sh** para obtener el permiso del usuario **root**.

Estructura del paquete de parches

- **install.sh**: script de instalación de parches.
- **ips.ini**: almacena las direcciones IP de todos los nodos del clúster. Modifique este archivo basándose en las direcciones IP reales de los nodos del clúster. Cada dirección IP ocupa una línea. No se permite ninguna línea en blanco entre direcciones IP. Deje una línea en blanco al final del archivo.
- **scp-util.exp**: script de herramienta SCP.

- **ssh-util.exp**: script de herramienta SSH.
- **Sudo_Vulnerability_20210330**: directorio para almacenar el script **sudo_repair.sh**. Puede copiar el directorio a la carpeta para ejecutar el script en cada nodo.
- **sudo_repair.sh**: script para corregir la vulnerabilidad.
- **README.md**: describe cómo utilizar la herramienta de parche.

Instalación del parche

Paso 1 Haga clic en la dirección del área correspondiente del clúster para descargar el paquete de parches.

- **CN-Hong Kong**: **https://mrs-container1-patch-ap-southeast-1.obs.ap-southeast-1.myhuaweicloud.com/MRS_Common_Script/MRS_All_Sudo_Vulnerability_20210330.tar.gz**
- **AP-Bangkok**: **https://mrs-container1-patch-ap-southeast-2.obs.ap-southeast-2.myhuaweicloud.com/MRS_Common_Script/MRS_All_Sudo_Vulnerability_20210330.tar.gz**
- **AP-Singapore**: **https://mrs-container1-patch-ap-southeast-3.obs.ap-southeast-3.myhuaweicloud.com/MRS_Common_Script/MRS_All_Sudo_Vulnerability_20210330.tar.gz**

Paso 2 Inicie sesión en el nodo maestro activo del clúster como usuario **root**.

Paso 3 Cargue el paquete de parches a **/root/**.

Paso 4 Ejecute el siguiente comando para descomprimir el paquete de la herramienta de parche **MRS_All_Sudo_Vulnerability_20210330.tar.gz** en el directorio actual (**/root**).

tar -zxf MRS_All_Sudo_Vulnerability_20210330.tar.gz

Paso 5 Ejecute el siguiente comando para ir al directorio donde se encuentra el archivo **ips.ini**.

cd /root/MRS_All_Sudo_Vulnerability_20210330/

Paso 6 Configure las direcciones IP de todos los nodos del clúster en el archivo **ips.ini**. Cada dirección IP ocupa una línea. No se permite ninguna línea en blanco entre direcciones IP. Deje una línea en blanco al final del archivo.

Paso 7 Ejecute el siguiente script para instalar el parche.

Después de ejecutar el script, debe introducir la contraseña correcta del usuario **root**. Si la contraseña es incorrecta, la cuenta puede estar bloqueada durante 5 minutos.

cd /root/MRS_All_Sudo_Vulnerability_20210330/

dos2unix ./*

chmod +x ./* -R

sh install.sh "install"

----Fin

Desinstalación de un parche

Ejecute el siguiente script para desinstalar el parche. Después de ejecutar el script, debe introducir la contraseña correcta del usuario **root**. Si la contraseña es incorrecta, la cuenta puede estar bloqueada durante 5 minutos durante el proceso SSH del script.

cd /root/MRS_All_Sudo_Vulnerability_20210330/

sh install.sh "uninstall"

3.9.4.2 Descripción del parche MRS 2.1.0.11

Información básica:

Tabla 3-59 Información básica

Versión del parche	MRS 2.1.0.11
Fecha de lanzamiento	2020-12-30
Problemas resueltos	**Lista de problemas resueltos en MRS 2.1.0.11:** **MRS Manager** Los registros de Ejecutor, KNOX y OS se pueden revertir. Ahora se agregan registros de Executor GC. Se resuelve el error de reinicio de Knox. Resuelva el problema de que los trabajos no se pueden enviar cuando un nodo está defectuoso. Se admite el monitoreo de enlace completo. El estado del trabajo se puede actualizar al cambiar los nodos de ResourceManager activo y en espera. Se resuelven errores de copia de respaldo y restauración en algunos escenarios. Se resuelve la alarma de falla de proceso que se genera con frecuencia en el HMaster. **Componentes de Big data** Se ha resuelto el problema de la pérdida de memoria de JobHistory. Se ha resuelto el problema de la tabla de Hive truncate se agota y no se puede truncar. Se ha resuelto el problema de que el archivo de datos de tabla no existía después de que una tarea Hive incremental fallara. La sentencia Hive SQL no se está ejecutando correctamente. Después de crear una tabla Carbon en un clúster de seguridad y el grupo hive no tiene permiso para crear la tabla Carbon, otros usuarios pueden crear la tabla Carbon. Se ha resuelto el problema de que el proceso spark JDBCServer es anormal.

	Lista de problemas resueltos en MRS 2.1.0.10: **MRS Manager** Las nuevas configuraciones de cola en el archivo **capacity-schedule.xml** no se perderán durante el escalamiento horizontal del clúster después de instalar el parche. El monitoreo de enlace completo se puede revertir. **Componentes de Big data** Se ha resuelto la falla de asignación de permisos de Hive en Spark. Si no se especifica ninguna cola, las tareas se envían a la cola de launcher-job de forma predeterminada. La tarea que se ejecuta no se verá afectada.
	Lista de problemas resueltos en MRS 2.1.0.9: **MRS Manager** Se resuelve el desbordamiento de memoria del MRS Executor. El proceso de escalamiento horizontal del clúster está optimizado. Se resuelve el problema de que la sentencia SQL se combina incorrectamente cuando el valor de SparkSQL contiene espacios. Se resuelve el problema de que los trabajos de HiveSQL no se envían ocasionalmente. El control de permisos para descargar el archivo keytab está optimizado. **Componentes de Big data** Cuando el nombre del rol Presto contiene letras mayúsculas, el modelo de permisos puede tener efecto. Se resuelve el problema de que las particiones Hive se eliminan lentamente. Se resuelve el problema de que el token caduca después de que Spark se ejecute durante mucho tiempo.
	Lista de problemas resueltos en MRS 2.1.0.8: **MRS Manager** Se ha resuelto el problema de que el tráfico de la API de ECS está limitado cuando se accede a OBS a través de una delegación. Varios usuarios pueden iniciar sesión en MRS Manager al mismo tiempo. Se admite el monitoreo de enlace completo. **Componentes de big data de MRS** Se ha actualizado Carbon 2.0. Se ha resuelto el problema HBASE-18484.
	Lista de problemas resueltos en MRS 2.1.0.7: **MRS Manager** Se ha resuelto el problema de que los datos y los archivos se muestran incorrectamente si un campo contiene un carácter de nueva línea en la consulta DLF+Presto. El resultado de la consulta Presto se puede guardar como un archivo.

	Lista de problemas resueltos en MRS 2.1.0.6: **MRS Manager** Se ha resuelto el problema de que el uso de E/S de disco de los datos de monitoreo es inexacto. Se ha resuelto el problema de que el estado del trabajo de Spark no se actualiza ocasionalmente. El problema de que se ha solucionado el error en la ejecución del trabajo. El mecanismo de parche se ha optimizado. **Componentes de big data de MRS** Se rectifican las excepciones de HBase. Se ha resuelto el problema de que el sistema responde lentamente cuando los roles de Hive están vinculados a permisos.
	Lista de problemas resueltos en MRS 2.1.0.5: **Componentes de big data de MRS** Impala soporta la función de ObsFileSystem. Se puede configurar el período de tiempo de espera de la página MRS Manager y las páginas nativas de los componentes. Se ha resuelto el problema de congelación de la unión de privilegios de Hive. Se ha solucionado el error de conexión de datos.
	Lista de problemas resueltos en MRS 2.1.0.3: **MRS Manager** Se han resuelto los problemas de la alta entrega de trabajos simultáneos de Manager executor. **Componentes de big data de MRS** Se ha corregido el error de inserción de datos en hive on tez.

	Lista de problemas resueltos en MRS 2.1.0.2: **MRS Manager** No se muestra ninguna información de monitoreo después de reiniciar NodeAgent. Cuando un trabajo está bajo envío durante mucho tiempo, se produce un desbordamiento de memoria en el proceso **manager executor**. Se admite la presentación de trabajos. **manager executor** se puede utilizar para configurar una alta simultaneidad. Los nuevos topics de Kafka no se muestran en el plano de gestión de MRS Manager. Cuando invoca a las API del clúster de seguridad para enviar el trabajo **Spark Submit** y realizar operaciones en una tabla HBase, el control de permisos en la tabla HBase no tiene efecto. Se ha optimizado el mecanismo de parche de MRS Manager. **Componentes de big data de MRS** Se ha optimizado el funcionamiento lento del comando **load data inpath** ejecutado por Spark. Los nombres de columna que contienen el signo de dólar ($) se pueden utilizar en la creación de tablas de Spark. Los problemas relacionados con la OBS han sido resueltos.
	Lista de problemas resueltos en MRS 2.1.0.1: **MRS Manager** Se han optimizado los resultados de retorno de las sentencias de Hive SQL enviadas por los trabajos V2 y se ha resuelto el problema de que los trabajos V2 no se envíen con un token de delegación. **Componentes de big data de MRS** HiveServer fuera de memoria (OOM) se ha resuelto para MRS Hive: HIVE-10970 y HIVE-22275.
Compatibilidad con otros parches	El paquete de parches MRS 2.1.0.11 contiene todos los parches publicados para MRS 2.1.0.
Divulgación de vulnerabilidades	Se ha corregido la vulnerabilidad de ejecución remota de código de Spark. Para obtener más información acerca de la vulnerabilidad, consulte **CVE-2020-9480**

Impacto de la instalación de parches

- Durante la instalación del parche MRS 2.1.0.11, MRS Manager se reiniciará, y los componentes como Hive, Impala, Spark, HDFS, Yarn, MapReduce, Presto, HBase, Tez, y los servicios dependientes relacionados se reiniciarán en modo rodante. Durante el reinicio de MRS Manager, los servicios no están disponibles temporalmente, pero los servicios no se interrumpen durante el reinicio rodante.

- Una vez instalado el parche MRS 2.1.0.11, inicie sesión en **standby Master node** (Iniciar sesión en MRS Manager. El nodo Master con un pentágono hueco en la página **Host Management** es el nodo Master en espera), cambia a usuario **omm** y ejecuta el comando **sh /opt/knox/bin/restart-knox.sh** para reiniciar el proceso Knox. Esta operación no es necesaria para un clúster con un solo nodo Master.

  Puede ejecutar el comando **ps -ef |grep knox** para comprobar si se ha iniciado el proceso knox. Si se muestra el ID de proceso knox, el proceso knox se inicia correctamente.
- (Opcional) Después de instalar el parche MRS 2.1.0.11, debe descargar e instalar de nuevo todos los clientes, incluidos los clientes originales de los nodos Master y los clientes utilizados por otros nodos de VPC (es decir, los clientes que ha configurado).
  - Para obtener más información acerca de cómo actualizar completamente el cliente original del nodo maestro activo, consulte **Actualización completa del cliente original del nodo de Master activo**.
  - Para obtener más información acerca de cómo actualizar completamente el cliente original del nodo Master en espera, consulte **Actualización completa del cliente original del nodo de Master en espera**.
  - Para obtener más información acerca de cómo instalar completamente los clientes que configuró, consulte **Instalación de un cliente (Versiones anteriores a 3.x)**.

  NOTA

  - Se le aconseja hacer una copia de respaldo de los clientes antiguos antes de volver a instalar los nuevos.
  - Si ha modificado las configuraciones de cliente según el escenario del servicio, vuelva a modificarlas después de reinstalar los clientes.
- (Opcional) Se puede configurar el intervalo de tiempo de espera de la página MRS Manager y la página nativa del componente. Es necesario modificar manualmente la siguiente configuración:

  a. Cambie el intervalo de tiempo de espera de sesión de los servicios web y CAS en todos los nodos de Master.

     i. Cambie el valor de **<session-timeout>20</session-timeout>** en **/opt/Bigdata/tomcat/webapps/cas/WEB-INF/web.xml**. La unidad es un minuto.

     ii. Cambie el valor de **<session-timeout>20</session-timeout>** en **/opt/Bigdata/tomcat/webapps/web/WEB-INF/web.xml**. La unidad es un minuto.

  b. Cambie el período de validez de TGT del CAS en todos los nodos de Master.

     Cambie **1200** de **p:maxTimeToLiveInSeconds="${tgt.maxTimeToLiveInSeconds:1200}** y **p:timeToKillInSeconds="${tgt.timeToKillInSeconds:1200}"** de **/opt/Bigdata/tomcat/webapps/cas/WEB-INF/spring-configuration/ticketExpirationPolicies.xml** al intervalo de tiempo de espera correspondiente, en segundos.

  c. Reinicie el servicio Tomcat en el nodo de Master activo.

     i. En el nodo de Master activo, ejecute el comando **netstat -anp |grep 28443 | grep LISTEN** como usuario **omm** para consultar el ID de proceso de Tomcat.

     ii. Ejecute el comando **kill -9** *{pid}*, en el que *{pid}* indica el ID de proceso obtenido en el paso anterior.

     iii. Espere a que el proceso se reinicie automáticamente. Puede ejecutar el comando **netstat -anp |grep 28443 |grep LISTEN** para comprobar si se ha iniciado el proceso. Si se muestra la salida del comando, el proceso se inicia correctamente.

d. Agregar o modificar elementos de configuración para cada componente. Los valores de los elementos de configuración son los mismos que el intervalo de tiempo de espera, en segundos.
   - HDFS/MapReduce/Yarn: Agregue el elemento de configuración personalizado **http.server.session.timeout.secs**.
   - Spark: Cambie el valor de **spark.session.maxAge**.
   - Hive: Agregue el elemento de configuración personalizado **http.server.session.timeout.secs**.

   Al guardar los elementos de configuración, puede elegir no reiniciar los servicios o instancias afectados. Reinicie los servicios o instancias cuando el servicio no esté ocupado.

3.9.4.3 Descripción del parche MRS 3.0.5.1

Información básica:

Tabla 3-60 Información básica:

Versión del parche	MRS 3.0.5.1
Fecha de lanzamiento	2021-08-14

Problemas resueltos	**Lista de problemas resueltos en MRS 3.0.5.1:** **MRS Manager** ● Resuelto el error al enviar trabajos de SparkSQL en la página de gestión de trabajos debido a sentencias SQL largas. ● Resuelto el error al ejecutar sentencias SQL con comentarios. **Componentes de Big data** ● Resuelto el error al sincronizar los usuarios de IAM con los clústeres de ClickHouse. ● Resuelto el problema de que el cliente de Flume en el clúster no podía usar una delegación para acceder a OBS. ● Resuelto el problema de que el valor de **% of Queue** no se muestra para un trabajo especificado en la interfaz de usuario web de Yarn nativa. ● Resuelto el problema de que los registros de trabajo no se muestran completamente en la interfaz de usuario web nativa de Yarn. ● Resuelto el problema de que los archivos temporales residieran en HDFS después de la ejecución de trabajos de Hive. ● Resuelta la incompatibilidad en la interconexión entre Sqoop 1.4.7 de código abierto y MRS Hive. ● Resuelto el error al consultar tablas Avro a través de Hive en MR. ● Resuelto el problema de pérdida de memoria causado cuando HiveServer cargaba funciones definidas por el usuario (UDF). ● Resuelto el problema de que los resultados de ejecución de las funciones de tiempo de Hive y SparkSQL son incoherentes. ● Resuelto el problema (HIVE-20187) por el que el resultado es incorrecto cuando Hive on Tez utiliza MapJoin para lograr el ajuste del rendimiento. ● Resuelto el problema de que se produce un error al ejecutar el comando **beeline -p**. ● Resuelto el problema por el que Hue falla al formatear sentencias SQL. ● Resuelto la falla al enviar trabajos de Oozie debido a la incompatibilidad entre las zonas horarias de Hue y Oozie. ● Resuelta la falta de disponibilidad de la lista desplegable de variables cuando se ejecuta una sentencia SQL de Hive declarada como variable en la interfaz de usuario web de Hue. ● Resuelta la falla de consulta causado por sesiones cerradas incorrectamente cuando Hue se conecta a Hive para realizar consultas. ● Resueltas las respuestas lentas a las consultas de servidores Kunpeng de tablas Kudu utilizando Impala. ● Resuelta la falla de instalación del cliente Kudu. ● Resuelto los reinicios inesperados de la instancia de KuduMaster en los servidores de Kunpeng. ● Resueltas las excepciones de búsqueda en la interfaz web de Ranger. ● Se ha resuelto el error al redirigir a los usuarios a la página de inicio de sesión después de cerrar sesión de la interfaz de usuario web de Ranger.

Compatibilidad con otros parches	El parche MRS 3.0.5.1 puede resolver todos los problemas detectados en MRS 3.0.5.

Impacto de la instalación de parches

- Durante la instalación de MRS 3.0.5.1, los procesos del Executor y del Controller se reinician automáticamente y las funciones del clúster en el plano de gestión, como el envío de trabajos y el escalado del clúster, se verán afectadas. Por lo tanto, instale el parche en el momento adecuado.
- Después de instalar el parche, reinicie los componentes Spark2x, Hive, Yarn, Impala, Kudu y Hue en FusionInsight Manager para que el parche surta efecto. Durante el reinicio, es posible que algunos servicios no estén disponibles durante un corto período de tiempo. Para minimizar el impacto en la continuidad del servicio, realice el reinicio en el momento adecuado.
- Para instalar el parche MRS 3.0.5.1, debe descargar manualmente el archivo de parche e instalarlo en cualquier nodo master del clúster. Para obtener más información, consulte el archivo **README.md** en el paquete de parches.
- Este parche también debe instalarse para cualquier nodo nuevo que se agregue posteriormente al clúster. Para instalar el parche para este nuevo nodo, instale el parche en el nodo master y reinicie el servicio correspondiente.

Direcciones de descarga de parches

- **CN-Hong Kong**: **https://mrs-container1-patch-ap-southeast-1.obs.ap-southeast-1.myhuaweicloud.com/MRS_Common_Script/MRS_3.0.5.1_Patch_All_20210724.tar.gz**
- **AP-Singapore**: **https://mrs-container1-patch-ap-southeast-3.obs.ap-southeast-3.myhuaweicloud.com/MRS_Common_Script/MRS_3.0.5.1_Patch_All_20210724.tar.gz**
- **AP-Bangkok**: **https://mrs-container1-patch-ap-southeast-2.obs.ap-southeast-2.myhuaweicloud.com/MRS_Common_Script/MRS_3.0.5.1_Patch_All_20210724.tar.gz**

3.9.4.4 Descripción del parche MRS 2.1.0.10

Información básica:

Tabla 3-61 Información básica

Versión del parche	MRS 2.1.0.10
Fecha de lanzamiento	2020-09-21

Problemas resueltos	**Lista de problemas resueltos en MRS 2.1.0.10:** **MRS Manager** Las nuevas configuraciones de cola en el archivo **capacity-schedule.xml** no se perderán durante el escalamiento horizontal del clúster después de instalar el parche. El monitoreo de enlace completo se puede revertir. **Componentes de Big data** Se ha resuelto la falla de asignación de permisos de Hive en Spark. Si no se especifica ninguna cola, las tareas se envían a la cola de launcher-job de forma predeterminada. La tarea que se ejecuta no se verá afectada.
	Lista de problemas resueltos en MRS 2.1.0.9: **MRS Manager** Se resuelve el desbordamiento de memoria del MRS Executor. Proceso de escalamiento horizontal del clúster optimizado. Se resuelve el problema de que la sentencia SQL se combina incorrectamente cuando el valor de SparkSQL contiene espacios. Se resuelve el problema de que los trabajos de HiveSQL no se envían ocasionalmente. El control de permisos para descargar el archivo keytab está optimizado. **Componentes de Big data** Cuando el nombre del rol Presto contiene letras mayúsculas, el modelo de permisos puede tener efecto. Se resuelve el problema de que las particiones Hive se eliminan lentamente. Se resuelve el problema de que el token caduca después de que Spark se ejecute durante mucho tiempo.
	Lista de problemas resueltos en MRS 2.1.0.8: **MRS Manager** Se ha resuelto el problema de que el tráfico de la API de ECS está limitado cuando se accede a OBS a través de una delegación. Varios usuarios pueden iniciar sesión en MRS Manager al mismo tiempo. Se admite el monitoreo de enlace completo. **Componentes de big data de MRS** Se ha actualizado Carbon 2.0. Se ha resuelto el problema HBASE-18484.
	Lista de problemas resueltos en MRS 2.1.0.7: **MRS Manager** Se ha resuelto el problema de que los datos y los archivos se muestran incorrectamente si un campo contiene un carácter de nueva línea en la consulta DLF+Presto. El resultado de la consulta Presto se puede guardar como un archivo.

	Lista de problemas resueltos en MRS 2.1.0.6: **MRS Manager** Se ha resuelto el problema de que el uso de E/S de disco de los datos de monitoreo es inexacto. Se ha resuelto el problema de que el estado del trabajo de Spark no se actualiza ocasionalmente. El problema de que se ha solucionado el error en la ejecución del trabajo. El mecanismo de parche se ha optimizado. **Componentes de big data de MRS** Se rectifican las excepciones de HBase. Se ha resuelto el problema de que el sistema responde lentamente cuando los roles de Hive están vinculados a permisos.
	Lista de problemas resueltos en MRS 2.1.0.5: **Componentes de big data de MRS** Impala soporta la función de ObsFileSystem. Se puede configurar el período de tiempo de espera de la página MRS Manager y las páginas nativas de los componentes. Se ha resuelto el problema de congelación de la unión de privilegios de Hive. Se ha solucionado el error de conexión de datos.
	Lista de problemas resueltos en MRS 2.1.0.3: **MRS Manager** Se han resuelto los problemas de la alta entrega de trabajos simultáneos de Manager executor. **Componentes de big data de MRS** Se ha corregido el error de inserción de datos en **hive on tez**.

	Lista de problemas resueltos en MRS 2.1.0.2: **MRS Manager** No se muestra ninguna información de monitoreo después de reiniciar NodeAgent. Cuando un trabajo está bajo envío durante mucho tiempo, se produce un desbordamiento de memoria en el proceso **manager executor**. Se admite la presentación de trabajos. **manager executor** se puede utilizar para configurar una alta simultaneidad. Los nuevos topics de Kafka no se muestran en el plano de gestión de MRS Manager. Cuando invoca a las API del clúster de seguridad para enviar el trabajo **Spark Submit** y realizar operaciones en una tabla HBase, el control de permisos en la tabla HBase no tiene efecto. Se ha optimizado el mecanismo de parche de MRS Manager. **Componentes de big data de MRS** Se ha optimizado el funcionamiento lento del comando **load data inpath** ejecutado por Spark. Los nombres de columna que contienen el signo de dólar ($) se pueden utilizar en la creación de tablas de Spark. Los problemas relacionados con la OBS han sido resueltos.
	Lista de problemas resueltos en MRS 2.1.0.1: **MRS Manager** Se han optimizado los resultados de retorno de las sentencias de Hive SQL enviadas por los trabajos V2 y se ha resuelto el problema de que los trabajos V2 no se envíen con un token de delegación. **Componentes de big data de MRS** HiveServer fuera de memoria (OOM) se ha resuelto para MRS Hive: HIVE-10970 y HIVE-22275.
Compatibilidad con otros parches	El paquete de parches MRS 2.1.0.10 contiene todos los parches publicados para MRS 2.1.0.
Divulgación de vulnerabilidades	Se ha corregido la vulnerabilidad de ejecución remota de código de Spark. Para obtener más información acerca de la vulnerabilidad, consulte **CVE-2020-9480**

Impacto de la instalación de parches

- Durante la instalación del parche MRS 2.1.0.10, MRS Manager se reiniciará, y los componentes como Hive, Impala, Spark, HDFS, Yarn, MapReduce, Presto, HBase, Tez, y los servicios dependientes relacionados se reiniciarán en modo rodante. Durante el reinicio de MRS Manager, los servicios no están disponibles temporalmente, pero los servicios no se interrumpen durante el reinicio rodante.

- Después de instalar el parche MRS 2.1.0.10, debe descargar e instalar de nuevo todos los clientes, incluidos los clientes originales de los nodos de Master y los clientes utilizados por otros nodos de VPC (es decir, los clientes que ha configurado).
  - Para obtener más información acerca de cómo actualizar completamente el cliente original del nodo maestro activo, consulte **Actualización completa del cliente original del nodo de Master activo**.
  - Para obtener más información acerca de cómo actualizar completamente el cliente original del nodo Master en espera, consulte **Actualización completa del cliente original del nodo de Master en espera**.
  - Para obtener más información acerca de cómo instalar completamente los clientes que configuró, consulte **Instalación de un cliente (Versiones anteriores a 3.x)**.

  NOTA

  - Se le aconseja hacer una copia de respaldo de los clientes antiguos antes de volver a instalar los nuevos.
  - Si ha modificado las configuraciones de cliente según el escenario del servicio, vuelva a modificarlas después de reinstalar los clientes.
- (Opcional) Se puede configurar el intervalo de tiempo de espera de la página MRS Manager y la página nativa del componente. Es necesario modificar manualmente la siguiente configuración:

  a. Cambie el intervalo de tiempo de espera de sesión de los servicios web y CAS en todos los nodos de Master.

     i. Cambie el valor de **<session-timeout>20</session-timeout>** en **/opt/Bigdata/tomcat/webapps/cas/WEB-INF/web.xml**. La unidad es un minuto.

     ii. Cambie el valor de **<session-timeout>20</session-timeout>** en **/opt/Bigdata/tomcat/webapps/web/WEB-INF/web.xml**. La unidad es un minuto.

  b. Cambie el período de validez de TGT del CAS en todos los nodos de Master.

     Cambie **1200** de **p:maxTimeToLiveInSeconds="${tgt.maxTimeToLiveInSeconds:1200}** y **p:timeToKillInSeconds="${tgt.timeToKillInSeconds:1200}"** de **/opt/Bigdata/tomcat/webapps/cas/WEB-INF/spring-configuration/ticketExpirationPolicies.xml** al intervalo de tiempo de espera correspondiente, en segundos.

  c. Reinicie el servicio Tomcat en el nodo de Master activo.

     i. En el nodo de Master activo, ejecute el comando **netstat -anp |grep 28443 | grep LISTEN** como usuario **omm** para consultar el ID de proceso de Tomcat.

     ii. Ejecute el comando **kill -9** *{pid}*, en el que *{pid}* indica el ID de proceso obtenido en el paso anterior.

     iii. Espere a que el proceso se reinicie automáticamente. Puede ejecutar el comando **netstat -anp |grep 28443 |grep LISTEN** para comprobar si se ha iniciado el proceso. Si se muestra la salida del comando, el proceso se inicia correctamente.

  d. Agregar o modificar elementos de configuración para cada componente. Los valores de los elementos de configuración son los mismos que el intervalo de tiempo de espera, en segundos.

     - HDFS/MapReduce/Yarn: Agregue el elemento de configuración personalizado **http.server.session.timeout.secs**.
     - Spark: Cambie el valor de **spark.session.maxAge**.

- Hive: Agregue el elemento de configuración personalizado **http.server.session.timeout.secs**.

Al guardar los elementos de configuración, puede elegir no reiniciar los servicios o instancias afectados. Reinicie los servicios o instancias cuando el servicio no esté ocupado.

3.9.4.5 Descripción del parche MRS 2.1.0.9

Información básica:

Tabla 3-62 Información básica

Versión del parche	MRS 2.1.0.9
Fecha de lanzamiento	2020-08-21
Problemas resueltos	**Lista de problemas resueltos en MRS 2.1.0.9:** **MRS Manager** Se resuelve el desbordamiento de memoria del MRS Executor. Optimización del proceso de escalamiento horizontal del disco. Se resuelve el problema de que la sentencia SQL se combina incorrectamente cuando el valor de SparkSQL contiene espacios. Se resuelve el problema de que los trabajos de HiveSQL no se envían ocasionalmente. El control de permisos para descargar el archivo keytab está optimizado. **Componentes de Big data** Cuando el nombre del rol Presto contiene letras mayúsculas, el modelo de permisos puede tener efecto. Las particiones se eliminan lentamente en Hive. Se resuelve el problema de que el token caduca después de que Spark se ejecute durante mucho tiempo.
	Lista de problemas resueltos en MRS 2.1.0.8: **MRS Manager** Se ha resuelto el problema de que el tráfico de la API de ECS está limitado cuando se accede a OBS a través de una delegación. Varios usuarios pueden iniciar sesión en MRS Manager al mismo tiempo. Se admite el monitoreo de enlace completo. **Componentes de big data de MRS** Se ha actualizado Carbon 2.0. Se ha resuelto el problema HBASE-18484.

	Lista de problemas resueltos en MRS 2.1.0.7: **MRS Manager** Se ha resuelto el problema de que los datos y los archivos se muestran incorrectamente si un campo contiene un carácter de nueva línea en la consulta DLF+Presto. El resultado de la consulta Presto se puede guardar como un archivo.
	Lista de problemas resueltos en MRS 2.1.0.6: **MRS Manager** Se ha resuelto el problema de que el uso de E/S de disco de los datos de monitoreo es inexacto. Se ha resuelto el problema de que el estado del trabajo de Spark no se actualiza ocasionalmente. El problema de que se ha solucionado el error en la ejecución del trabajo. El mecanismo de parche se ha optimizado. **Componentes de big data de MRS** Se rectifican las excepciones de HBase. Se ha resuelto el problema de que el sistema responde lentamente cuando los roles de Hive están vinculados a permisos.
	Lista de problemas resueltos en MRS 2.1.0.5: **Componentes de big data de MRS** Impala soporta la función de ObsFileSystem. Se puede configurar el período de tiempo de espera de la página MRS Manager y las páginas nativas de los componentes. Se ha resuelto el problema de congelación de la unión de privilegios de Hive. Se ha solucionado el error de conexión de datos.
	Lista de problemas resueltos en MRS 2.1.0.3: **MRS Manager** Se han resuelto los problemas de la alta entrega de trabajos simultáneos de Manager executor. **Componentes de big data de MRS** Se ha corregido el error de inserción de datos en **hive on tez**.

	Lista de problemas resueltos en MRS 2.1.0.2: **MRS Manager** No se muestra ninguna información de monitoreo después de reiniciar NodeAgent. Cuando un trabajo está bajo envío durante mucho tiempo, se produce un desbordamiento de memoria en el proceso **manager executor**. Se admite la presentación de trabajos. **manager executor** se puede utilizar para configurar una alta simultaneidad. Los nuevos topics de Kafka no se muestran en el plano de gestión de MRS Manager. Cuando invoca a las API del clúster de seguridad para enviar el trabajo **Spark Submit** y realizar operaciones en una tabla HBase, el control de permisos en la tabla HBase no tiene efecto. Se ha optimizado el mecanismo de parche de MRS Manager. **Componentes de big data de MRS** Se ha optimizado el funcionamiento lento del comando **load data inpath** ejecutado por Spark. Los nombres de columna que contienen el signo de dólar ($) se pueden utilizar en la creación de tablas de Spark. Los problemas relacionados con la OBS han sido resueltos.
	Lista de problemas resueltos en MRS 2.1.0.1: **MRS Manager** Se han optimizado los resultados de retorno de las sentencias de Hive SQL enviadas por los trabajos V2 y se ha resuelto el problema de que los trabajos V2 no se envíen con un token de delegación. **Componentes de big data de MRS** HiveServer fuera de memoria (OOM) se ha resuelto para MRS Hive: HIVE-10970 y HIVE-22275.
Compatibilidad con otros parches	El paquete de parches MRS 2.1.0.9 contiene todos los parches publicados para MRS 2.1.0.
Divulgación de vulnerabilidades	Se ha corregido la vulnerabilidad de ejecución remota de código de Spark. Para obtener más información acerca de la vulnerabilidad, consulte **CVE-2020-9480**

Impacto de la instalación de parches

- Durante la instalación del parche MRS 2.1.0.9, MRS Manager se reiniciará, y los componentes como Hive, Impala, Spark, HDFS, Yarn, MapReduce, Presto, HBase, Tez, y los servicios dependientes relacionados se reiniciarán en modo rodante. Durante el reinicio de MRS Manager, los servicios no están disponibles temporalmente, pero los servicios no se interrumpen durante el reinicio rodante.

- Después de instalar el parche MRS 2.1.0.9, debe descargar e instalar de nuevo todos los clientes, incluidos los clientes originales de los nodos maestros y los clientes utilizados por otros nodos de VPC (es decir, los clientes que ha configurado).
  - Para obtener más información acerca de cómo actualizar completamente el cliente original del nodo maestro activo, consulte **Actualización completa del cliente original del nodo de Master activo**.
  - Para obtener más información acerca de cómo actualizar completamente el cliente original del nodo Master en espera, consulte **Actualización completa del cliente original del nodo de Master en espera**.
  - Para obtener más información acerca de cómo instalar completamente los clientes que configuró, consulte **Instalación de un cliente (Versiones anteriores a 3.x)**.

  NOTA

  - Se le aconseja hacer una copia de respaldo de los clientes antiguos antes de volver a instalar los nuevos.
  - Si ha modificado las configuraciones de cliente según el escenario del servicio, vuelva a modificarlas después de reinstalar los clientes.
- (Opcional) Se puede configurar el intervalo de tiempo de espera de la página MRS Manager y la página nativa del componente. Es necesario modificar manualmente la siguiente configuración:

  a. Cambie el intervalo de tiempo de espera de sesión de los servicios web y CAS en todos los nodos de Master.

     i. Cambie el valor de **<session-timeout>20</session-timeout>** en **/opt/Bigdata/tomcat/webapps/cas/WEB-INF/web.xml**. La unidad es un minuto.

     ii. Cambie el valor de **<session-timeout>20</session-timeout>** en **/opt/Bigdata/tomcat/webapps/web/WEB-INF/web.xml**. La unidad es un minuto.

  b. Cambie el período de validez de TGT del CAS en todos los nodos de Master.

     Cambie **1200** de **p:maxTimeToLiveInSeconds="${tgt.maxTimeToLiveInSeconds:1200}** y **p:timeToKillInSeconds="${tgt.timeToKillInSeconds:1200}"** de **/opt/Bigdata/tomcat/webapps/cas/WEB-INF/spring-configuration/ticketExpirationPolicies.xml** al intervalo de tiempo de espera correspondiente, en segundos.

  c. Reinicie el servicio Tomcat en el nodo de Master activo.

     i. En el nodo de Master activo, ejecute el comando **netstat -anp |grep 28443 | grep LISTEN** como usuario **omm** para consultar el ID de proceso de Tomcat.

     ii. Ejecute el comando **kill -9** *{pid}*, en el que *{pid}* indica el ID de proceso obtenido en el paso anterior.

     iii. Espere a que el proceso se reinicie automáticamente. Puede ejecutar el comando **netstat -anp |grep 28443 |grep LISTEN** para comprobar si se ha iniciado el proceso. Si se muestra la salida del comando, el proceso se inicia correctamente.

  d. Agregar o modificar elementos de configuración para cada componente. Los valores de los elementos de configuración son los mismos que el intervalo de tiempo de espera, en segundos.

     - HDFS/MapReduce/Yarn: Agregue el elemento de configuración personalizado **http.server.session.timeout.secs**.
     - Spark: Cambie el valor de **spark.session.maxAge**.

- Hive: Agregue el elemento de configuración personalizado **http.server.session.timeout.secs**.

Al guardar los elementos de configuración, puede elegir no reiniciar los servicios o instancias afectados. Reinicie los servicios o instancias cuando el servicio no esté ocupado.

3.9.4.6 Descripción del parche MRS 2.1.0.8

Información básica

Tabla 3-63 Información básica

Versión del parche	MRS 2.1.0.8
Fecha de lanzamiento	2020-08-04
Problemas resueltos	**Lista de problemas resueltos en MRS 2.1.0.8:** **MRS Manager** Se ha resuelto el problema de que el tráfico de la API de ECS está limitado cuando se accede a OBS a través de una delegación. Varios usuarios pueden iniciar sesión en MRS Manager al mismo tiempo. Se admite el monitoreo de enlace completo. **Componentes de big data de MRS** Se ha actualizado Carbon 2.0. Se ha resuelto el problema HBASE-18484.
	Lista de problemas resueltos en MRS 2.1.0.7: **MRS Manager** Se ha resuelto el problema de que los datos y los archivos se muestran incorrectamente si un campo contiene un carácter de nueva línea en la consulta DLF+Presto. El resultado de la consulta Presto se puede guardar como un archivo.

	Lista de problemas resueltos en MRS 2.1.0.6: **MRS Manager** Se ha resuelto el problema de que el uso de E/S de disco de los datos de monitoreo es inexacto. Se ha resuelto el problema de que el estado del trabajo de Spark no se actualiza ocasionalmente. El problema de que se ha solucionado el error en la ejecución del trabajo. El mecanismo de parche se ha optimizado. **Componentes de big data de MRS** Se rectifican las excepciones de HBase. Se ha resuelto el problema de que el sistema responde lentamente cuando los roles de Hive están vinculados a permisos.
	Lista de problemas resueltos en MRS 2.1.0.5: **Componentes de big data de MRS** Impala soporta la función de ObsFileSystem. Se puede configurar el período de tiempo de espera de la página MRS Manager y las páginas nativas de los componentes. Se ha resuelto el problema de congelación de la unión de privilegios de Hive. Se ha solucionado el error de conexión de datos.
	Lista de problemas resueltos en MRS 2.1.0.3: **MRS Manager** Se han resuelto los problemas de la alta entrega de trabajos simultáneos de Manager executor. **Componentes de big data de MRS** Se ha corregido el error de inserción de datos en hive on tez.

	Lista de problemas resueltos en MRS 2.1.0.2: **MRS Manager** No se muestra ninguna información de monitoreo después de reiniciar NodeAgent. Cuando un trabajo está bajo envío durante mucho tiempo, se produce un desbordamiento de memoria en el proceso **manager executor**. Se admite la presentación de trabajos. **manager executor** se puede utilizar para configurar una alta simultaneidad. Los nuevos topics de Kafka no se muestran en el plano de gestión de MRS Manager. Cuando invoca a las API del clúster de seguridad para enviar el trabajo **Spark Submit** y realizar operaciones en una tabla HBase, el control de permisos en la tabla HBase no tiene efecto. Se ha optimizado el mecanismo de parche de MRS Manager. **Componentes de big data de MRS** Se ha optimizado el funcionamiento lento del comando **load data inpath** ejecutado por Spark. Los nombres de columna que contienen el signo de dólar ($) se pueden utilizar en la creación de tablas de Spark. Los problemas relacionados con la OBS han sido resueltos.
	Lista de problemas resueltos en MRS 2.1.0.1: **MRS Manager** Se han optimizado los resultados de retorno de las sentencias de Hive SQL enviadas por los trabajos V2 y se ha resuelto el problema de que los trabajos V2 no se envíen con un token de delegación. **Componentes de big data de MRS** HiveServer fuera de memoria (OOM) se ha resuelto para MRS Hive: HIVE-10970 y HIVE-22275.
Compatibilidad con otros parches	El paquete de parches MRS 2.1.0.8 contiene todos los parches publicados para MRS 2.1.0.
Divulgación de vulnerabilidades	Se ha corregido la vulnerabilidad de ejecución remota de código de Spark. Para obtener más información acerca de la vulnerabilidad, consulte **CVE-2020-9480**

Impacto de la instalación de parches

- Durante la instalación del parche MRS 2.1.0.8, MRS Manager se reiniciará, y los componentes como Hive, Impala, Spark, HDFS, Yarn, MapReduce, Presto, HBase, Tez, y los servicios dependientes relacionados se reiniciarán en modo continuo. Durante el reinicio de MRS Manager, los servicios no están disponibles temporalmente, pero los servicios no se interrumpen durante el reinicio rodante.

- Después de instalar el parche MRS 2.1.0.8, debe descargar e instalar de nuevo todos los clientes, incluidos los clientes originales de los nodos maestros y los clientes utilizados por otros nodos de VPC (es decir, los clientes que ha configurado).
  - Para obtener más información acerca de cómo actualizar completamente el cliente original del nodo maestro activo, consulte **Actualización completa del cliente original del nodo de Master activo**.
  - Para obtener más información acerca de cómo actualizar completamente el cliente original del nodo Master en espera, consulte **Actualización completa del cliente original del nodo de Master en espera**.
  - Para obtener más información acerca de cómo instalar completamente los clientes que configuró, consulte **Instalación de un cliente (Versiones anteriores a 3.x)**.

  NOTA

  - Se le aconseja hacer una copia de respaldo de los clientes antiguos antes de volver a instalar los nuevos.
  - Si ha modificado las configuraciones de cliente según el escenario del servicio, vuelva a modificarlas después de reinstalar los clientes.
- (Opcional) Se puede configurar el intervalo de tiempo de espera de la página MRS Manager y la página nativa del componente. Es necesario modificar manualmente la siguiente configuración:

  a. Cambie el intervalo de tiempo de espera de sesión de los servicios web y CAS en todos los nodos de Master.

     i. Cambie el valor de **<session-timeout>20</session-timeout>** en **/opt/Bigdata/tomcat/webapps/cas/WEB-INF/web.xml**. La unidad es un minuto.

     ii. Cambie el valor de **<session-timeout>20</session-timeout>** en **/opt/Bigdata/tomcat/webapps/web/WEB-INF/web.xml**. La unidad es un minuto.

  b. Cambie el período de validez de TGT del CAS en todos los nodos de Master.

     Cambie **1200** de **p:maxTimeToLiveInSeconds="${tgt.maxTimeToLiveInSeconds:1200}** y **p:timeToKillInSeconds="${tgt.timeToKillInSeconds:1200}"** de **/opt/Bigdata/tomcat/webapps/cas/WEB-INF/spring-configuration/ticketExpirationPolicies.xml** al intervalo de tiempo de espera correspondiente, en segundos.

  c. Reinicie el servicio Tomcat en el nodo de Master activo.

     i. En el nodo de Master activo, ejecute el comando **netstat -anp |grep 28443 | grep LISTEN** como usuario **omm** para consultar el ID de proceso de Tomcat.

     ii. Ejecute el comando **kill -9** *{pid}*, en el que *{pid}* indica el ID de proceso obtenido en el paso anterior.

     iii. Espere a que el proceso se reinicie automáticamente. Puede ejecutar el comando **netstat -anp |grep 28443 |grep LISTEN** para comprobar si se ha iniciado el proceso. Si se muestra la salida del comando, el proceso se inicia correctamente.

  d. Agregar o modificar elementos de configuración para cada componente. Los valores de los elementos de configuración son los mismos que el intervalo de tiempo de espera, en segundos.

     - HDFS/MapReduce/Yarn: Agregue el elemento de configuración personalizado **http.server.session.timeout.secs**.
     - Spark: Cambie el valor de **spark.session.maxAge**.

- Hive: Agregue el elemento de configuración personalizado **http.server.session.timeout.secs**.

Al guardar los elementos de configuración, puede elegir no reiniciar los servicios o instancias afectados. Reinicie los servicios o instancias cuando el servicio no esté ocupado.

3.9.4.7 Descripción del parche de MRS 2.1.0.7

Información básica

Tabla 3-64 Información básica

Versión del parche	MRS 2.1.0.7
Fecha de lanzamiento	2020-07-15
Problemas resueltos	**Lista de problemas resueltos en MRS 2.1.0.7**: **MRS Manager** Se ha resuelto el problema de que los datos y los archivos se muestran incorrectamente si un campo contiene un carácter de nueva línea en la consulta DLF+Presto. El resultado de la consulta Presto se puede guardar como un archivo.
	Lista de problemas resueltos en MRS 2.1.0.6: **MRS Manager** Se ha resuelto el problema de que el uso de E/S de disco de los datos de monitoreo es inexacto. Se ha resuelto el problema de que el estado del trabajo de Spark no se actualiza ocasionalmente. El problema de que se ha solucionado el error en la ejecución del trabajo. El mecanismo de parche se ha optimizado. **Componentes de big data de MRS** Se rectifican las excepciones de HBase. Se ha resuelto el problema de que el sistema responde lentamente cuando los roles de Hive están vinculados a permisos.
	Lista de problemas resueltos en MRS 2.1.0.5: **Componentes de big data de MRS** Impala soporta la función de ObsFileSystem. Se puede configurar el período de tiempo de espera de la página MRS Manager y las páginas nativas de los componentes. Se ha resuelto el problema de congelación de la unión de privilegios de Hive. Se ha solucionado el error de conexión de datos.

	Lista de problemas resueltos en MRS 2.1.0.3: **MRS Manager** Se han resuelto los problemas de la alta entrega de trabajos simultáneos de Manager executor. **Componentes de big data de MRS** Se ha corregido el error de inserción de datos en hive on tez.
	Lista de problemas resueltos en MRS 2.1.0.2: **MRS Manager** No se muestra ninguna información de monitoreo después de reiniciar NodeAgent. Cuando un trabajo está bajo envío durante mucho tiempo, se produce un desbordamiento de memoria en el proceso **manager executor**. Se admite la presentación de trabajos. **manager executor** se puede utilizar para configurar una alta simultaneidad. Los nuevos temas de Kafka no se muestran en el plano de gestión de MRS Manager. Cuando invoca a las API del clúster de seguridad para enviar el trabajo **Spark Submit** y realizar operaciones en una tabla HBase, el control de permisos en la tabla HBase no tiene efecto. Se ha optimizado el mecanismo de parche de MRS Manager. **Componentes de big data de MRS** Se ha optimizado el funcionamiento lento del comando **load data inpath** ejecutado por Spark. Los nombres de columna que contienen el signo de dólar ($) se pueden utilizar en la creación de tablas de Spark. Los problemas relacionados con la OBS han sido resueltos.
	Lista de problemas resueltos en MRS 2.1.0.1: **MRS Manager** Se han optimizado los resultados de retorno de las sentencias de Hive SQL enviadas por los trabajos V2 y se ha resuelto el problema de que los trabajos V2 no se envíen con un token de agencia. **Componentes de big data de MRS** HiveServer fuera de memoria (OOM) se ha resuelto para MRS Hive: HIVE-10970 y HIVE-22275.
Compatibilidad con otros parches	El paquete de parches de MRS 2.1.0.7 contiene todos los parches publicados para MRS 2.1.0.

Impacto de la instalación de parches

- Durante la instalación del parche MRS 2.1.0.7, MRS Manager se reiniciará, y los componentes como Hive, Impala, Spark, HDFS, Yarn, MapReduce, Presto, HBase, Tez,

y los servicios dependientes relacionados se reiniciarán en modo continuo. Durante el reinicio de MRS Manager, los servicios no están disponibles temporalmente, pero los servicios no se interrumpen durante el reinicio continuo.

- Después de instalar el parche MRS 2.1.0.7, debe descargar e instalar de nuevo todos los clientes, incluidos los clientes originales de los nodos de Master y los clientes utilizados por otros nodos de VPC (es decir, los clientes que ha configurado).
  - Para obtener más información acerca de cómo actualizar completamente el cliente original del nodo maestro activo, consulte **Actualización completa del cliente original del nodo de Master activo**.
  - Para obtener más información acerca de cómo actualizar completamente el cliente original del nodo maestro en espera, consulte **Actualización completa del cliente original del nodo de Master en espera**.
  - Para obtener más información acerca de cómo instalar completamente los clientes que configuró, consulte **Instalación de un cliente (Versiones anteriores a 3.x)**.

  NOTA

  - Se le aconseja hacer una copia de respaldo de los clientes antiguos antes de volver a instalar los nuevos.
  - Si ha modificado las configuraciones de cliente según el escenario del servicio, vuelva a modificarlas después de reinstalar los clientes.
- (Opcional) Se puede configurar el intervalo de tiempo de espera de la página MRS Manager y la página nativa del componente. Es necesario modificar manualmente la siguiente configuración:

  a. Cambie el intervalo de tiempo de espera de sesión de los servicios web y CAS en todos los nodos de Master.

     i. Cambia el valor de **<session-timeout>20</session-timeout>** en **/opt/Bigdata/tomcat/webapps/cas/WEB-INF/web.xml**. La unidad es un minuto.

     ii. Cambie el valor de **<session-timeout>20</session-timeout>** en **/opt/Bigdata/tomcat/webapps/web/WEB-INF/web.xml**. La unidad es un minuto.

  b. Cambie el período de validez de TGT del CAS en todos los nodos de Master.

     Cambie **1200** de **p:maxTimeToLiveInSeconds="${tgt.maxTimeToLiveInSeconds:1200}** y **p:timeToKillInSeconds="${tgt.timeToKillInSeconds:1200}"** de **/opt/Bigdata/tomcat/webapps/cas/WEB-INF/spring-configuration/ticketExpirationPolicies.xml** al intervalo de tiempo de espera correspondiente, en segundos.

  c. Reinicie el servicio Tomcat en el nodo de Master activo.

     i. En el nodo de Master activo, ejecute el comando **netstat -anp |grep 28443 | grep LISTEN** como usuario **omm** para consultar el ID de proceso de Tomcat.

     ii. Ejecute el comando **kill -9** *{pid}*, en el que *{pid}* indica el ID de proceso obtenido en el paso anterior.

     iii. Espere a que el proceso se reinicie automáticamente. Puede ejecutar el comando **netstat -anp |grep 28443 |grep LISTEN** para comprobar si se ha iniciado el proceso. Si se muestra la salida del comando, el proceso se inicia correctamente.

  d. Agregar o modificar elementos de configuración para cada componente. Los valores de los elementos de configuración son los mismos que el intervalo de tiempo de espera, en segundos.

- HDFS/MapReduce/Yarn: Agregue el elemento de configuración personalizado **http.server.session.timeout.secs**.
- Spark: Cambie el valor de **spark.session.maxAge**.
- Hive: Agregue el elemento de configuración personalizado **http.server.session.timeout.secs**.

Al guardar los elementos de configuración, puede elegir no reiniciar los servicios o instancias afectados. Reinicie los servicios o instancias cuando el servicio no esté ocupado.

3.9.4.8 Descripción de parche de MRS 2.1.0.6

Información básica

Tabla 3-65 Información básica

Versión del parche	MRS 2.1.0.6
Fecha de lanzamiento	2020-06-10
Problemas resueltos	**Lista de problemas resueltos en MRS 2.1.0.6:** **MRS Manager** Se ha resuelto el problema de que el uso de E/S de disco de los datos de monitoreo es inexacto. Se ha resuelto el problema de que el estado del trabajo de Spark no se actualiza ocasionalmente. El problema de que se ha solucionado el error en la ejecución del trabajo. El mecanismo de parche se ha optimizado. **Componentes de big data de MRS** Se rectifican las excepciones de HBase. Se ha resuelto el problema de que el sistema responde lentamente cuando los roles de Hive están vinculados a permisos.
	Lista de problemas resueltos en MRS 2.1.0.5: **Componentes de big data de MRS** Impala soporta la función de ObsFileSystem. Se puede configurar el período de tiempo de espera de la página MRS Manager y las páginas nativas de los componentes. Se ha resuelto el problema de congelación de la unión de privilegios de Hive. Se ha solucionado el error de conexión de datos.

	Lista de problemas resueltos en MRS 2.1.0.3: **MRS Manager** Se han resuelto los problemas de la alta entrega de trabajos simultáneos de Manager executor. **Componentes de big data de MRS** Se ha corregido el error de inserción de datos en hive on tez.
	Lista de problemas resueltos en MRS 2.1.0.2: **MRS Manager** No se muestra ninguna información de monitoreo después de reiniciar NodeAgent. Cuando un trabajo está bajo envío durante mucho tiempo, se produce un desbordamiento de memoria en el proceso **manager executor**. Se admite la presentación de trabajos. **manager executor** se puede utilizar para configurar una alta simultaneidad. Los nuevos temas de Kafka no se muestran en el plano de gestión de MRS Manager. Cuando invoca a las API del clúster de seguridad para enviar el trabajo **Spark Submit** y realizar operaciones en una tabla HBase, el control de permisos en la tabla HBase no tiene efecto. Se ha optimizado el mecanismo de parche de MRS Manager. **Componentes de big data de MRS** Se ha optimizado el funcionamiento lento del comando **load data inpath** ejecutado por Spark. Los nombres de columna que contienen el signo de dólar ($) se pueden utilizar en la creación de tablas de Spark. Los problemas relacionados con la OBS han sido resueltos.
	Lista de problemas resueltos en MRS 2.1.0.1: **MRS Manager** Se han optimizado los resultados de retorno de las sentencias de Hive SQL enviadas por los trabajos V2 y se ha resuelto el problema de que los trabajos V2 no se envíen con un token de agencia. **Componentes de big data de MRS** HiveServer fuera de memoria (OOM) se ha resuelto para MRS Hive: HIVE-10970 y HIVE-22275.
Compatibilidad con otros parches	El paquete de parches MRS 2.1.0.6 contiene todos los parches publicados para MRS 2.1.0.

Impacto de la instalación de parches

- Durante la instalación del parche MRS 2.1.0.6, MRS Manager se reiniciará, y los componentes como Hive, Impala, Spark, HDFS, Yarn, MapReduce, Presto, HBase, Tez,

y los servicios dependientes relacionados se reiniciarán en modo continuo. Durante el reinicio de MRS Manager, los servicios no están disponibles temporalmente, pero los servicios no se interrumpen durante el reinicio continuo.

- Después de instalar el parche MRS 2.1.0.6, debe descargar e instalar de nuevo todos los clientes, incluidos los clientes originales de los nodos de Master y los clientes utilizados por otros nodos de VPC (es decir, los clientes que ha configurado).
  - Para obtener más información acerca de cómo actualizar completamente el cliente original del nodo maestro activo, consulte **Actualización completa del cliente original del nodo de Master activo**.
  - Para obtener más información acerca de cómo actualizar completamente el cliente original del nodo Master en espera, consulte **Actualización completa del cliente original del nodo de Master en espera**.
  - Para obtener más información acerca de cómo instalar completamente los clientes que configuró, consulte **Instalación de un cliente (Versiones anteriores a 3.x)**.

  NOTA

  - Se le aconseja hacer una copia de respaldo de los clientes antiguos antes de volver a instalar los nuevos.
  - Si ha modificado las configuraciones de cliente según el escenario del servicio, vuelva a modificarlas después de reinstalar los clientes.
- (Opcional) Se puede configurar el intervalo de tiempo de espera de la página MRS Manager y la página nativa del componente. Es necesario modificar manualmente la siguiente configuración:

  a. Cambie el intervalo de tiempo de espera de sesión de los servicios web y CAS en todos los nodos de Master.

     i. Cambia el valor de **<session-timeout>20</session-timeout>** en **/opt/Bigdata/tomcat/webapps/cas/WEB-INF/web.xml**. La unidad es un minuto.

     ii. Cambia el valor de **<session-timeout>20</session-timeout>** en **/opt/Bigdata/tomcat/webapps/web/WEB-INF/web.xml**. La unidad es un minuto.

  b. Cambie el período de validez de TGT del CAS en todos los nodos de Master.

     Cambie **1200** de **p:maxTimeToLiveInSeconds="${tgt.maxTimeToLiveInSeconds:1200}** y **p:timeToKillInSeconds="${tgt.timeToKillInSeconds:1200}"** de **/opt/Bigdata/tomcat/webapps/cas/WEB-INF/spring-configuration/ticketExpirationPolicies.xml** al intervalo de tiempo de espera correspondiente, en segundos.

  c. Reinicie el servicio Tomcat en el nodo de Master activo.

     i. En el nodo de Master activo, ejecute el comando **netstat -anp |grep 28443 | grep LISTEN** como usuario **omm** para consultar el ID de proceso de Tomcat.

     ii. Ejecute el comando **kill -9** *{pid}*, en el que *{pid}* indica el ID de proceso obtenido en el paso anterior.

     iii. Espere a que el proceso se reinicie automáticamente. Puede ejecutar el comando **netstat -anp |grep 28443 |grep LISTEN** para comprobar si se ha iniciado el proceso. Si se muestra la salida del comando, el proceso se inicia correctamente.

  d. Agregar o modificar elementos de configuración para cada componente. Los valores de los elementos de configuración son los mismos que el intervalo de tiempo de espera, en segundos.

- HDFS/MapReduce/Yarn: Agregue el elemento de configuración personalizado **http.server.session.timeout.secs**.
- Spark: Cambie el valor de **spark.session.maxAge**.
- Hive: Agregue el elemento de configuración personalizado **http.server.session.timeout.secs**.

Al guardar los elementos de configuración, puede elegir no reiniciar los servicios o instancias afectados. Reinicie los servicios o instancias cuando el servicio no esté ocupado.

3.9.4.9 Descripción del parche de MRS 2.1.0.3

Información básica

Tabla 3-66 Información básica

Versión del parche	MRS 2.1.0.3
Fecha de lanzamiento	2020-04-29
Problemas resueltos	**Lista de problemas resueltos en MRS 2.1.0.3:** **MRS Manager** Se han resuelto los problemas de la alta entrega de trabajos simultáneos de Manager executor. **Componentes de big data de MRS** Se ha corregido el error de inserción de datos en hive on tez.

	Lista de problemas resueltos en MRS 2.1.0.2: **MRS Manager** No se muestra ninguna información de monitoreo después de reiniciar NodeAgent. Cuando un trabajo está bajo envío durante mucho tiempo, se produce un desbordamiento de memoria en el proceso **manager executor**. Se admite la presentación de trabajos. **manager executor** se puede utilizar para configurar una alta simultaneidad. Los nuevos temas de Kafka no se muestran en el plano de gestión de MRS Manager. Cuando invoca a las API del clúster de seguridad para enviar el trabajo **Spark Submit** y realizar operaciones en una tabla HBase, el control de permisos en la tabla HBase no tiene efecto. Se ha optimizado el mecanismo de parche de MRS Manager. **Componentes de big data de MRS** Se ha optimizado el funcionamiento lento del comando **load data inpath** ejecutado por Spark. Los nombres de columna que contienen el signo de dólar ($) se pueden utilizar en la creación de tablas de Spark. Los problemas relacionados con la OBS han sido resueltos.
	Lista de problemas resueltos en MRS 2.1.0.1: **MRS Manager** Se han optimizado los resultados de retorno de las sentencias de Hive SQL enviadas por los trabajos V2 y se ha resuelto el problema de que los trabajos V2 no se envíen con un token de agencia. **Componentes de big data de MRS** HiveServer fuera de memoria (OOM) se ha resuelto para MRS Hive: HIVE-10970 y HIVE-22275.
Compatibilidad con otros parches	El paquete de parches MRS 2.1.0.3 contiene todos los parches publicados para MRS 2.1.0.

Impacto de la instalación de parches

- Durante la instalación del parche MRS 2.1.0.3, MRS Manager se reiniciará y los componentes como Hive, Spark, HDFS, Yarn, MapReduce, Presto, HBase, y los servicios dependientes relacionados se reiniciarán en modo continuo. Durante el reinicio de MRS Manager, los servicios no están disponibles temporalmente, pero los servicios no se interrumpen durante el reinicio continuo.
- Después de instalar el parche MRS 2.1.0.3, debe descargar e instalar de nuevo todos los clientes, incluidos los clientes originales de los nodos de Master y los clientes utilizados por otros nodos de VPC (es decir, los clientes que ha configurado).

- Para obtener más información acerca de cómo actualizar completamente el cliente original del nodo maestro activo, consulte **Actualización completa del cliente original del nodo de Master activo**.
- Para obtener más información acerca de cómo actualizar completamente el cliente original del nodo maestro en espera, consulte **Actualización completa del cliente original del nodo de Master en espera**.
- Para obtener más información acerca de cómo instalar completamente los clientes que configuró, consulte **Instalación de un cliente (Versiones anteriores a 3.x)**.

NOTA

- Se le aconseja hacer una copia de respaldo de los clientes antiguos antes de volver a instalar los nuevos.
- Si ha modificado las configuraciones de cliente según el escenario del servicio, vuelva a modificarlas después de reinstalar los clientes.

3.9.4.10 Descripción del parche de MRS 2.1.0.2

Información básica

Tabla 3-67 Información básica

Versión del parche	MRS 2.1.0.2
Fecha de lanzamiento	2020-04-22
Problemas resueltos	**Lista de problemas resueltos en MRS 2.1.0.2**: **MRS Manager** No se muestra ninguna información de monitoreo después de reiniciar NodeAgent. Cuando un trabajo está bajo envío durante mucho tiempo, se produce un desbordamiento de memoria en el proceso **manager executor**. Se admite la presentación de trabajos. Puede configurar la simultaneidad para **manager executor**. Los nuevos temas de Kafka no se muestran en el plano de gestión de MRS Manager. Cuando invoca a las API del clúster de seguridad para enviar el trabajo **Spark Submit** y realizar operaciones en una tabla HBase, el control de permisos en la tabla HBase no tiene efecto. Se ha optimizado el mecanismo de parche de MRS Manager. **Componentes de big data de MRS** Se ha optimizado el funcionamiento lento del comando **load data inpath** ejecutado por Spark. Los nombres de columna que contienen el signo de dólar ($) se pueden utilizar en la creación de tablas de Spark. Los problemas relacionados con la OBS han sido resueltos.

	Lista de problemas resueltos en MRS 2.1.0.1: **MRS Manager** Se han optimizado los resultados de retorno de las sentencias de Hive SQL enviadas por los trabajos V2 y se ha resuelto el problema de que los trabajos V2 no se envíen con un token de agencia. **Componentes de big data de MRS** HiveServer fuera de memoria (OOM) se ha resuelto para MRS Hive: HIVE-10970 y HIVE-22275
Compatibilidad con otros parches	El paquete de parches de MRS 2.1.0.2 contiene todo el contenido del paquete de parches de MRS 2.1.0.1.

Impacto de la instalación de parches

- Durante la instalación del parche MRS 2.1.0.2, MRS Manager se reiniciará y los componentes como Hive, Spark, HDFS, Yarn, MapReduce, Presto, HBase y los servicios dependientes relacionados se reiniciarán en modo continuo. Durante el reinicio de MRS Manager, los servicios no están disponibles temporalmente y los servicios no se interrumpen durante el reinicio continuo.
- Después de instalar el parche de MRS 2.1.0.2, debe descargar e instalar de nuevo todos los clientes, incluidos los clientes originales de los nodos de Master y los clientes utilizados por otros nodos de VPC (es decir, los clientes que ha configurado).
  - Para obtener más información acerca de cómo actualizar completamente el cliente original del nodo maestro activo, consulte **Actualización completa del cliente original del nodo de Master activo**.
  - Para obtener más información acerca de cómo actualizar completamente el cliente original del nodo Master en espera, consulte **Actualización completa del cliente original del nodo de Master en espera**.
  - Para obtener más información acerca de cómo instalar completamente los clientes que configuró, consulte **Instalación de un cliente (Versiones anteriores a 3.x)**.

  NOTA

  - Se le aconseja hacer una copia de respaldo de los clientes antiguos antes de volver a instalar los nuevos.
  - Si ha modificado las configuraciones de cliente según el escenario del servicio, vuelva a modificarlas después de reinstalar los clientes.

3.9.4.11 Descripción del parche de MRS 2.1.0.1

Información básica

Tabla 3-68 Información básica

Versión del parche	MRS 2.1.0.1

Fecha de lanzamiento	2020-02-12
Problemas resueltos	**Lista de problemas resueltos en MRS 2.1.0.1**: **MRS Manager** Se han optimizado los resultados de retorno de las sentencias de Hive SQL enviadas por los trabajos V2 y se ha resuelto el problema de que los trabajos V2 no se envíen con un token de agencia. **Componentes de big data de MRS** HiveServer fuera de memoria (OOM) se ha resuelto para MRS Hive: HIVE-10970 y HIVE-22275
Compatibilidad con otros parches	Ninguna

Impacto de la instalación de parches

Durante la instalación de los parches MRS 2.1.0.1, MRS Manager y Hive se reinician. Durante el reinicio, los servicios no están disponibles temporalmente.

Después de instalar los parches MRS 2.1.0.1, inicie sesión en el nodo de Master1 del clúster de MRS y elimine el directorio de trabajo en HDFS.

- Para un clúster con autenticación de Kerberos deshabilitada, ejecute el siguiente comando para eliminar el directorio de trabajo en HDFS:

  hdfs dfs -rm -r /mrs/mrsjob/hive

- Para un clúster con autenticación Kerberos habilitada, realice las siguientes operaciones para eliminar el directorio de trabajos en HDFS:

  a. Ejecute el siguiente comando e introduzca la contraseña para realizar la autenticación.

     kinit hdfs

  b. Ejecute el siguiente comando para eliminar el directorio de trabajos en HDFS:

     hdfs dfs -rm -r /mrs/mrsjob/hive

NOTA

Este paso no es necesario para un nuevo clúster de MRS porque el directorio no existe en HDFS.

3.9.4.12 Descripción del parche de MRS 2.0.6.1

Información básica

Tabla 3-69 Información básica

Versión del parche	MRS 2.0.6.1
Fecha de lanzamiento	2020-07-06
Problemas resueltos	**Lista de problemas resueltos en MRS 2.1.0.1:** **MRS Manager** Mecanismo de parche Las métricas de monitorización están vacías ocasionalmente. En la consulta DLF+Presto, si un campo contiene un carácter de nueva línea, los datos y los archivos se muestran incorrectamente.
Compatibilidad con otros parches	Ninguna

Impacto de la instalación de parches

Durante la instalación del parche MRS 2.0.6.1, MRS Manager se reiniciará, y los componentes como Hive y los servicios con dependencia se reiniciarán en modo continuo. Durante el reinicio de MRS Manager, los servicios no están disponibles temporalmente y los servicios no se interrumpen durante el reinicio continuo.

3.9.4.13 Descripción del parche MRS 2.0.1.3

Información básica

Tabla 3-70 Información básica

Versión del parche	MRS 2.0.1.3
Fecha de lanzamiento	2019-12-25

Problemas resueltos	**Lista de problemas resueltos en MRS 2.0.1.3**: **MRS Manager** Se ha optimizado la lógica de escalado del clúster y se han resuelto los problemas de fuga de conexiones TCP en el fondo de las API de gestión de trabajos de la V1. **Componentes de big data de MRS** Se han resuelto los siguientes problemas para MRS Hive: HiveServer falta de memoria (OOM); fase **MergeFile** lenta si existe un gran número de archivos pequeños; archivos no encontrados en la fase **load partition** de **insert overwrite** y error de fusión de archivos durante la reutilización de **HIVE-22373:Container**.
	Lista de problemas resueltos en MRS 2.0.1.2: **MRS Manager** Se solucionó el siguiente problema: La escalabilidad hacia fuera falla ocasionalmente debido al tiempo de espera que se produce cuando ResourceManager ejecuta **refreshNodes**.
	Lista de problemas resueltos en MRS 2.0.1.1: **MRS Manager** Se ha solucionado el siguiente problema: OOM ocurre en el executor de los nodos de MRS Master debido a la ampliación y reducción de nodos. **Componentes de big data de MRS** Se ha agregado la siguiente nueva función: MRS Presto soporta OBSFileSystem. Se han resuelto los siguientes problemas para MRS Presto: El jstack se imprime con frecuencia y los archivos de registro son demasiado grandes para desplazarse.
Compatibilidad con otros parches	El paquete de parches MRS 2.0.1.3 contiene todo el contenido de los paquetes de parches MRS 2.0.1.2 y MRS 2.0.1.1.

Impacto de la instalación de parches

Durante la instalación de los parches MRS 2.0.1.3, MRS Manager y Presto se reinician. Durante el reinicio, los servicios no están disponibles temporalmente.

3.9.4.14 Descripción del parche de MRS 2.0.1.2

Información básica

Tabla 3-71 Información básica

Versión del parche	MRS 2.0.1.2

Fecha de lanzamiento	2019-09-30
Problemas resueltos	**Lista de problemas resueltos en MRS 2.0.1.2**: **MRS Manager** Se solucionó el siguiente problema: La escalabilidad hacia fuera falla ocasionalmente debido al tiempo de espera que se produce cuando ResourceManager ejecuta **refreshNodes**.
	Lista de problemas resueltos en MRS 2.0.1.1: **MRS Manager** Se ha solucionado el siguiente problema: Fuera de memoria (OOM) se produce en el ejecutor de los nodos de Master de MRS debido a la reducción o expansión horizontal de nodos repetidos. **Componentes de big data de MRS** Se ha agregado la siguiente nueva función: MRS Presto soporta OBSFileSystem. Se han resuelto los siguientes problemas para MRS Presto: El jstack se imprime con frecuencia y los archivos de registro son demasiado grandes para desplazarse.
Compatibilidad con otros parches	El paquete de parches de MRS 2.0.1.2 contiene todo el contenido del paquete de parches de MRS 2.0.1.1.

Impacto de la instalación de parches

Durante la instalación de los parches de MRS 2.0.1.2, MRS Manager y Presto se reinician. Durante el reinicio, los servicios no están disponibles temporalmente.

3.9.4.15 Descripción del parche MRS 2.0.1.1

Información básica

Tabla 3-72 Información básica

Versión del parche	MRS 2.0.1.1
Fecha de lanzamiento	2019-09-30

Problemas resueltos	**MRS Manager** Se ha solucionado el siguiente problema: Fuera de memoria (OOM) se produce en el ejecutor de los nodos de Master de MRS debido a expansión horizontal y reducción horizontal de nodos repetidos. **Componentes de big data de MRS** Se ha agregado la siguiente nueva función: MRS Presto soporta OBSFileSystem. Se han resuelto los siguientes problemas para MRS Presto: El jstack se imprime con frecuencia y los archivos de registro son demasiado grandes para desplazarse.
Compatibilidad con otros parches	Ninguna

Impacto de la instalación de parches

Durante la instalación de los parches MRS 2.0.1.1, MRS Manager y Presto se reinician. Durante el reinicio, los servicios no están disponibles temporalmente.

3.9.4.16 Descripción del parche MRS 1.9.3.3

Información básica:

Tabla 3-73 Información básica:

Versión del parche	MRS 1.9.3.3
Fecha de lanzamiento	2021-01-04
Problemas resueltos	**Lista de problemas resueltos en MRS 1.9.3.3:** **MRS Manager** Se ha resuelto el problema de aislamiento del nodo. **Componentes de big data de MRS** Resuelto el problema de fuga de memoria cuando Hive carga hooks.
	Lista de problemas resueltos en MRS 1.9.3.2: **Componentes de big data de MRS** Cuando se realiza la operación de sobrescritura de inserción utilizando Spark SQL y Beeline, los archivos antiguos no se pueden borrar.

	Lista de problemas resueltos en MRS 1.9.3.1: **MRS Manager** Se solucionó el problema de que los nodos de tarea no se podían quitar de un clúster personalizado. **Componentes de big data de MRS** Se solucionó el problema de que la versión del paquete **adapter-hadoop-wrapper-file-system** en las rutas Hive y Spark era incorrecta. Se solucionó el problema de que varios espacios de nombres guardados en FusionInsight Manager de HBase no surten efecto en segundo plano. Agregó HDFSWrapper para soportar AbstractFileSystem.
Compatibilidad con otros parches	El paquete de parches MRS 1.9.3.3 contiene todos los parches publicados para MRS 1.9.3.

Impacto de la instalación de parches

- Durante la instalación de la revisión MRS 1.9.3.3, MRS Manager se reinicia y Hadoop, HDFS, Hive, Spark y los servicios dependientes relacionados se reinician en modo rodante. Durante el reinicio de MRS Manager, los servicios no están disponibles temporalmente, pero los servicios no se interrumpen durante el reinicio rodante.
- Después de instalar el parche MRS 1.9.3.3, debe descargar e instalar de nuevo todos los clientes, incluidos los clientes originales de los nodos de Master y los clientes utilizados por otros nodos de VPC (es decir, los clientes que ha configurado).
  - Para obtener más información acerca de cómo actualizar completamente el cliente original del nodo maestro activo, consulte **Actualización completa del cliente original del nodo de Master activo**.
  - Para obtener más información acerca de cómo actualizar completamente el cliente original del nodo maestro en espera, consulte **Actualización completa del cliente original del nodo de Master en espera**.
  - Para obtener más información acerca de cómo instalar completamente los clientes que configuró, consulte **Instalación de un cliente (Versiones anteriores a 3.x)**.

    NOTA

    - Se le aconseja hacer una copia de respaldo de los clientes antiguos antes de volver a instalar los nuevos.
    - Si ha modificado las configuraciones de cliente según el escenario del servicio, vuelva a modificarlas después de reinstalar los clientes.

3.9.4.17 Descripción del parche MRS 1.9.3.1

Información básica

Tabla 3-74 Información básica

Versión del parche	MRS 1.9.3.1
Fecha de lanzamiento	2020-09-04
Problemas resueltos	**MRS Manager** Se solucionó el problema de que los nodos de tarea no se podían quitar de un clúster personalizado. **Componentes de big data de MRS** Se solucionó el problema de que la versión del paquete **adapter-hadoop-wrapper-file-system** en las rutas Hive y Spark era incorrecta. Se solucionó el problema de que varios espacios de nombres guardados en FusionInsight Manager de HBase no surten efecto en segundo plano. Agregó HDFSWrapper para soportar AbstractFileSystem.
Compatibilidad con otros parches	Ninguna

Impacto de la instalación de parches

- Durante la instalación del parche MRS 1.9.3.1, MRS Manager se reinicia y Hadoop, HDFS, Hive, Spark y los servicios dependientes relacionados se reinician en modo continuo. Durante el reinicio de MRS Manager, los servicios no están disponibles temporalmente, pero los servicios no se interrumpen durante el reinicio rodante.
- Después de instalar el parche MRS 1.9.3.1, es necesario volver a descargar e instalar todos los clientes, incluidos los clientes originales del nodo Master y los clientes utilizados por otros nodos de VPC (es decir, los clientes que ha configurado).
  - Para obtener más información acerca de cómo actualizar completamente el cliente original del nodo maestro activo, consulte **Actualización completa del cliente original del nodo de Master activo**.
  - Para obtener más información acerca de cómo actualizar completamente el cliente original del nodo Master en espera, consulte **Actualización completa del cliente original del nodo de Master en espera**.
  - Para obtener más información acerca de cómo instalar completamente los clientes que configuró, consulte **Instalación de un cliente (Versiones anteriores a 3.x)**.

NOTA

- Se le aconseja hacer una copia de respaldo de los clientes antiguos antes de volver a instalar los nuevos.
- Si ha modificado las configuraciones de cliente según el escenario del servicio, vuelva a modificarlas después de reinstalar los clientes.

3.9.4.18 MRS 1.9.2.2 Descripción del parche

Información básica:

Tabla 3-75 Información básica:

Versión del parche	MRS 1.9.2.2
Fecha de lanzamiento	2021-05-18
Problemas resueltos	**MRS Manager** Resuelta la vulnerabilidad de escalada de privilegios sudo. Resuelto el problema de pérdida de información de cola debido a la actualización de cola durante la expansión de la capacidad. **Componentes de big data de MRS** Resuelto el problema de que la tarea Hive on Spark estaba suspendida porque el block ID se mostraba con caracteres confusos. Las API autodesarrolladas se agregan a Hive. Resuelto el problema de que el archivo **map.xml** no se podía leer. Optimizada la función Hive Har. Resuelto el problema de que Yarn no estaba disponible debido a los datos sucios de ZooKeeper. Actualizados los paquetes de OBS. Actualizado la versión de JDK. Resuelto el problema de la pérdida de memoria de ResourceManager. Agregado el monitoreo en la excepción que se produce cuando se invoca a la API de ECS getSecuritykey. Optimizado el proceso temporal de AK/SK. Resuelto el problema de la pérdida de memoria de ResourceManager. Corregido el error reportado cuando se utiliza la sentencia de Hive union para combinar archivos pequeños. Resuelto el problema de que Hadoop task no se ejecutaba debido a la falta de espacio. Resuelto el problema de que no se generan datos después de ejecutar correctamente un trabajo de Hive.

Compatibilidad con otros parches	Ninguna

Impacto de la instalación de parches

- Durante la instalación del parche MRS 1.9.2.2, MRS Manager se reiniciará y los componentes como Hadoop, Hive, Spark, Kafka, Ranger, Presto y los servicios dependientes relacionados se reiniciarán en modo rodante. Durante el reinicio de MRS Manager, los servicios no están disponibles temporalmente, pero los servicios no se interrumpen durante el reinicio rodante.
- Después de instalar el parche MRS 1.9.2.2, debe reiniciar el servicio OMS.

  NOTA

  - Inicie sesión en los nodos de OMS activos y en espera como usuario **root**, cambie a usuario **omm** y ejecute el comando **sh ${BIGDATA_HOME}/om-0.0.1/sbin/restart-oms.sh** para reiniciar el servicio OMS.
  - Es necesario reiniciar tanto los nodos OMS activo como en espera.
- Después de instalar el parche MRS 1.9.2.2, debe descargar e instalar de nuevo todos los clientes, incluidos los clientes originales de los nodos de Master y los clientes utilizados por otros nodos de VPC (es decir, los clientes que ha configurado).
  - Para obtener más información acerca de cómo actualizar completamente el cliente original del nodo maestro activo, consulte **Actualización completa del cliente original del nodo de Master activo**.
  - Para obtener más información acerca de cómo actualizar completamente el cliente original del nodo maestro en espera, consulte **Actualización completa del cliente original del nodo de Master en espera**.
  - Para obtener más información acerca de cómo instalar completamente los clientes que configuró, consulte **Instalación de un cliente (Versiones anteriores a 3.x)**.

  NOTA

  - Se le aconseja hacer una copia de respaldo de los clientes antiguos antes de volver a instalar los nuevos.
  - Si ha modificado las configuraciones de cliente según el escenario del servicio, vuelva a modificarlas después de reinstalar los clientes.

3.9.4.19 Descripción del parche MRS 1.9.0.8, 1.9.0.9 y 1.9.0.10

Información básica:

Tabla 3-76 Información básica:

Problemas resueltos	Número de parche: **MRS 1.9.0.10** Fecha de lanzamiento: 17 de enero de 2023 **Problemas resueltos** **Componentes de big data de MRS** OBSA soporta reintentos de control de flujo.
	Número de parche: **MRS 1.9.0.9** Fecha de lanzamiento: 10 de agosto de 2022 **Problemas resueltos** **Componentes de big data de MRS** Optimización superior del algoritmo de programación
	Número de parche **MRS 1.9.0.8** Fecha de lanzamiento: 20 de febrero de 2021 **Problemas resueltos** **Componentes de big data de MRS** Agregado el monitoreo en la excepción que se produce cuando se invoca a la API de ECS getSecuritykey. Optimizado el proceso temporal de AK/SK. Resuelto el problema de la pérdida de memoria de ResourceManager.
	Lista de problemas resueltos en MRS 1.9.0.7: **MRS Manager** Resuelto el problema de pérdida de información de cola debido a la actualización de cola durante la expansión de la capacidad. **Componentes de big data de MRS** Resuelto el problema de que la tarea Hive on Spark estaba suspendida porque el block ID se mostraba con caracteres confusos. Resuelva el problema de que la tarea Hadoop no se ejecuta debido a espacio insuficiente. Las API autodesarrolladas se agregan a Hive. Resuelto el problema de que el archivo **map.xml** no se podía leer. Resuelto el problema de que Yarn no estaba disponible debido a los datos sucios de ZooKeeper. Resuelto el problema de la pérdida de memoria de ResourceManager. Optimizada la función Hive Har. Actualizados los paquetes de OBS. Actualizado la versión de JDK.

	Lista de problemas resueltos en MRS 1.9.0.6: **MRS Manager** MRS Manager admite el escalamiento vertical de nodos especificados en un clúster anual/mensual. **Componentes de big data de MRS** Resuelto el problema de la respuesta lenta cuando HiveSE entrega sentencias SQL. Compatible con la interfaz de información de error de consulta de JobHistory. Resuelto el problema de que los permisos de grano fino no surtían efecto. Resuelta la excepción que se produce cuando Hive on Spark lee datos. Resuelto el problema de que el volumen de datos aumenta cuando la tarea Hive en la señora se ejecuta dos veces. Resuelto el problema de que el rendimiento de algunas cadenas es deficiente cuando la consulta vectorizada basada en vectores está habilitada en Hive.

	Lista de problemas resueltos en MRS 1.9.0.5: **MRS Manager** Optimizado el proceso de reinicio del servicio durante el ahorro de configuración en MRS Manager. Rectificada la falla periódica de la copia de respaldo en MRS Manager. **Componentes de big data de MRS** Parche privado de Ranger Resuelto el problema JVM Create GC thread failed de Yarn. Agregada la alarma de apilamiento de tareas de HiveServer2. Agregada la alarma que indica que el tiempo de GC de HiveServer HiveMetastore supera los 5s. Agregada la alarma que indica que HiveServer2 descomenta ZooKeeper. Agregada la alarma que indica que las tareas Yarn han fallado y el número de tareas eliminadas es superior a 5 en 20 minutos. Corregida la zona horaria de Spark JobHistory. Optimizado el mecanismo de reinicio de MetaStore. Resuelto el problema de código abierto HIVE-22771. Resueltos los errores de impresión del registro beeline de Hive. Corregido el número de nodos activos mostrados en la página de Yarn. Resuelta la lentitud de respuesta de la página RM, causada por un gran número de subprocesos de RM. Monitoreo de OBS soportado. Actualizados los paquetes de OBS. Resuelto el problema de que algunos datos no se insertan cuando 10 registros de datos se insertan simultáneamente en hive-jdbc. Resuelto el problema de que Hive informa ocasionalmente de una falla de deserialización de Kryo. Resuelto el problema de fuga de memoria de Spark JobHistory. Resuelto el problema por el que la lista de aplicaciones no se puede mostrar ocasionalmente en Spark JobHistory.
	Lista de problemas resueltos en MRS 1.9.0.3: **MRS Manager** Actualizado ARM JDK en MRS Manager. Resuelto el problema de que el disco del sistema está totalmente ocupado por registros del nodo Core en MRS Manager. **Componentes de big data de MRS** Resuelto el problema de que no se puede establecer la versión de registros de Ranger, lo que puede causar la ocupación total del disco.

	Lista de problemas resueltos en MRS 1.9.0.2: **MRS Manager** Resuelta la pérdida de confianza mutua entre algunos nodos Core en el clúster. Resuelto el problema de que las instancias no se podían agregar después de instalar el parche. Resuelto el problema de que el intervalo de tiempo de espera de reinicio continuo de HiveServer no se podía modificar en MRS Manager. **Componentes de big data de MRS** Actualizados los paquetes de OBS.
	Lista de problemas resueltos en MRS 1.9.0.1: **MRS Manager** Resuelto el problema de que MRS Manager no admite la instalación de parches continuos sin reiniciar los servicios. **Componentes de big data de MRS** Resuelto el problema de que la frecuencia de acceso confiada a la OBS no se limita a 140 veces en 5 minutos. Resuelto el problema de que Kafka no admite el acceso de código abierto. Resuelto el problema de código abierto SPARK-27637. Optimizado el reinicio continuo de Hive. Actualizados los paquetes de OBS.
Compatibilidad con otros parches	El parche MRS 1.9.0.10 puede resolver todos los problemas que se han resuelto con el parche MRS 1.9.0.

Impacto de la instalación de parches

- Durante la instalación del parche MRS 1.9.0.10, MRS Manager se reiniciará y los componentes como Hadoop, Hive, Spark, Presto y los servicios dependientes relacionados se reiniciarán en modo rodante. Durante el reinicio de MRS Manager, los servicios no están disponibles temporalmente y los servicios no se interrumpen durante el reinicio continuo.
- Después de instalar el parche MRS 1.9.0.10, debe descargar e instalar de nuevo todos los clientes, incluidos los clientes originales de los nodos de Master y los clientes utilizados por otros nodos de VPC (es decir, los clientes que ha configurado).
  - Para obtener más información acerca de cómo actualizar completamente el cliente original del nodo maestro activo, consulte **Actualización completa del cliente original del nodo de Master activo**.
  - Para obtener más información acerca de cómo actualizar completamente el cliente original del nodo maestro en espera, consulte **Actualización completa del cliente original del nodo de Master en espera**.
  - Para obtener más información acerca de cómo instalar completamente los clientes que configuró, consulte **Instalación de un cliente (Versiones anteriores a 3.x)**.

NOTA

- Se le aconseja hacer una copia de respaldo de los clientes antiguos antes de volver a instalar los nuevos.
- Si ha modificado las configuraciones de cliente según el escenario del servicio, vuelva a modificarlas después de reinstalar los clientes.

- (Opcional) En el escenario donde se obtiene un AK/SK temporal usando una delegación para acceder a OBS, configure el parámetro **fs.obs.auth.node-cache-short-circuit.enable** para determinar si permitir el acceso a la API de metadatos de ECS, determinando de este modo si desencadenar el control de flujo de ECS.

  El clúster MRS puede acceder a OBS utilizando un AK/SK temporal obtenido por una delegación. El AK/SK temporal se obtiene usando la API de metadatos de ECS. La API de metadatos ECS tiene un umbral de control de flujo de 140 veces en 5 minutos para un solo nodo. Después de activar el control de flujo, el nodo se agrega a la lista negra y no puede volver a invocar a la API de metadatos en 30 minutos. Para evitar el control de flujo, MRS proporciona el meta del servicio de caché de procesos cruzados a nivel de nodo para almacenar en caché AK/SK temporal.

  Escenario de aplicación: trabajos de Yarn como Spark y Hadoop que acceden a OBS mediante un AK/SK temporal obtenido por una delegación. Este parámetro se configura en el archivo **core-site.xml** del cliente.

  El valor predeterminado es **true**. El proceso de aplicación Yarn en el clúster MRS obtiene el AK/SK temporal del meta del servicio de caché a nivel de nodo. Si la meta es anormal, obtenga el AK/SK temporal de la API de metadatos de ECS.

  Si no desea acceder directamente a la API de metadatos de ECS cuando la meta es anormal, establezca este parámetro en **false** para evitar que el nodo se agregue a la lista negra debido al control de flujo.

3.9.4.20 Descripción del parche MRS 1.9.0.7

Información básica:

Tabla 3-77 Información básica:

Versión del parche	MRS 1.9.0.7
Fecha de lanzamiento	2021-01-15

Problemas resueltos	**Lista de problemas resueltos en MRS 1.9.0.7:** **MRS Manager** Resuelto el problema de pérdida de información de cola debido a la actualización de cola durante la expansión de la capacidad. **Componentes de big data de MRS** Resuelto el problema de que la tarea Hive on Spark estaba suspendida porque el ID de bloque se muestra como caracteres inexactos. Resuelva el problema de que la tarea Hadoop no se ejecuta debido a espacio insuficiente. Las API autodesarrolladas se agregan a Hive. Resuelto el problema de que el archivo **map.xml** no se puede leer. Resuelto el problema de que Yarn no está disponible debido a los datos sucios de ZooKeeper. Se resuelve el problema de fuga de memoria ResourceManager de Yarn. La función Hive Har está optimizada. Actualizados los paquetes de OBS. La versión de JDK está actualizada.
	Lista de problemas resueltos en MRS 1.9.0.6: **MRS Manager** MRS Manager admite el escalamiento vertical de nodos especificados en un clúster anual/mensual. **Componentes de big data de MRS** Resuelto el problema de la respuesta lenta cuando HiveSE entrega sentencias SQL. Compatible con la interfaz de información de error de consulta de historial de trabajos. Resuelto el problema de que los permisos de grano fino no surten efecto. Resuelta la excepción que se produce cuando Hive on Spark lee datos. Resuelto el problema de que el volumen de datos aumenta cuando la tarea Hive on mrs se ejecuta dos veces. Resuelto el problema de que el rendimiento de algunas cadenas es deficiente cuando se activa la consulta vectorizada basada en vectores en Hive.

	Lista de problemas resueltos en MRS 1.9.0.5: **MRS Manager** Optimizado el proceso de reinicio del servicio durante el ahorro de configuración en MRS Manager. Rectificada la falla periódica de la copia de respaldo en MRS Manager. **Componentes de big data de MRS** Parche privado de Ranger Resuelto el problema JVM Create GC thread failed de Yarn. Agregada la alarma de apilamiento de tareas de HiveServer2. Agregada la alarma que indica que el tiempo de GC de HiveServer HiveMetastore supera los 5s. Agregada la alarma que indica que HiveServer2 descomenta ZooKeeper. Agregada la alarma que indica que las tareas Yarn han fallado y el número de tareas eliminadas es superior a 5 en 20 minutos. Corregida la zona horaria de Spark JobHistory. Optimizado el mecanismo de reinicio de MetaStore. Resuelto el problema de código abierto HIVE-22771. Resueltos los errores de impresión del registro beeline de Hive. Corregido el número de nodos activos mostrados en la página de Yarn. Resuelta la lentitud de respuesta de la página RM, causada por un gran número de subprocesos de RM. Monitoreo de OBS soportado. Actualizados los paquetes de OBS. Resuelto el problema de que algunos datos no se insertan cuando 10 registros de datos se insertan simultáneamente en hive-jdbc. Resuelto el problema de que Hive informa ocasionalmente de una falla de deserialización de Kryo. Resuelto el problema de fuga de memoria de Spark JobHistory. Resuelto el problema por el que la lista de aplicaciones no se puede mostrar ocasionalmente en Spark JobHistory.
	Lista de problemas resueltos en MRS 1.9.0.3: **MRS Manager** Actualizado ARM JDK en MRS Manager. Resuelto el problema de que el disco del sistema está totalmente ocupado por registros del nodo Core en MRS Manager. **Componentes de big data de MRS** Resuelto el problema de que no se puede establecer la versión de registros de Ranger, lo que puede causar la ocupación total del disco.

	Lista de problemas resueltos en MRS 1.9.0.2: **MRS Manager** Resuelta la pérdida de confianza mutua entre algunos nodos Core en el clúster. Resuelto el problema de que las instancias no se podían agregar después de instalar el parche. Resuelto el problema de que el intervalo de tiempo de espera de reinicio continuo de HiveServer no se podía modificar en MRS Manager. **Componentes de big data de MRS** Actualizados los paquetes de OBS.
	Lista de problemas resueltos en MRS 1.9.0.1: **MRS Manager** Resuelto el problema de que MRS Manager no admite la instalación de parches continuos sin reiniciar los servicios. **Componentes de big data de MRS** Resuelto el problema de que la frecuencia de acceso confiada a la OBS no se limita a 140 veces en 5 minutos. Resuelto el problema de que Kafka no admite el acceso de código abierto. Resuelto el problema de código abierto SPARK-27637. Optimizado el reinicio continuo de Hive. Actualizados los paquetes de OBS.
Compatibilidad con otros parches	El parche MRS 1.9.0.7 puede resolver todos los problemas que se han resuelto con el parche MRS 1.9.0.

Impacto de la instalación de parches

- Durante la instalación del parche MRS 1.9.0.7, MRS Manager se reiniciará y los componentes como Hadoop, Hive, Spark, Kafka, Ranger y los servicios dependientes relacionados se reiniciarán en modo rodante. Durante el reinicio de MRS Manager, los servicios no están disponibles temporalmente, pero los servicios no se interrumpen durante el reinicio rodante.
- Después de instalar el parche MRS 1.9.0.7, debe descargar e instalar de nuevo todos los clientes, incluidos los clientes originales de los nodos Master y los clientes utilizados por otros nodos de VPC (es decir, los clientes que ha configurado).
  - Para obtener más información acerca de cómo actualizar completamente el cliente original del nodo maestro activo, consulte **Actualización completa del cliente original del nodo de Master activo**.
  - Para obtener más información acerca de cómo actualizar completamente el cliente original del nodo maestro en espera, consulte **Actualización completa del cliente original del nodo de Master en espera**.
  - Para obtener más información acerca de cómo instalar completamente los clientes que configuró, consulte **Instalación de un cliente (Versiones anteriores a 3.x)**.

NOTA

- Se le aconseja hacer una copia de respaldo de los clientes antiguos antes de volver a instalar los nuevos.
- Si ha modificado las configuraciones de cliente según el escenario del servicio, vuelva a modificarlas después de reinstalar los clientes.

3.9.4.21 Descripción del parche MRS 1.9.0.6

Información básica

Tabla 3-78 Información básica

Versión del parche	MRS 1.9.0.6
Fecha de lanzamiento	2020-05-20
Problemas resueltos	**Lista de problemas resueltos en MRS 1.9.0.6:** **MRS Manager** MRS Manager admite el escalamiento vertical de nodos especificados en un clúster anual/mensual. **Componentes de big data de MRS** Resuelto el problema de la respuesta lenta cuando HiveSE entrega sentencias SQL. Compatible con la interfaz de información de error de consulta de historial de trabajos. Resuelto el problema de que los permisos de grano fino no surten efecto. Solucionada la excepción que se producía cuando Hive on Spark leía datos. Resuelto el problema de que el volumen de datos aumenta cuando la tarea Hive on mrs se ejecuta dos veces. Resuelto el problema de que el rendimiento de algunas cadenas es deficiente cuando se activa la consulta vectorizada basada en vectores en Hive.

	Lista de problemas resueltos en MRS 1.9.0.5: **MRS Manager** Optimizado el proceso de reinicio del servicio durante el ahorro de configuración en MRS Manager. Rectificado la falla periódica de la copia de respaldo en MRS Manager. **Componentes de big data de MRS** Parche privado de Ranger Resuelto el problema JVM Create GC thread failed de Yarn. Agregada la alarma de apilamiento de tareas de HiveServer2. Agregada la alarma que indica que el tiempo de GC de HiveServer HiveMetastore supera los 5s. Agregada la alarma que indica que HiveServer2 descomenta ZooKeeper. Agregada la alarma que indica que las tareas Yarn han fallado y el número de tareas eliminadas es superior a 5 en 20 minutos. Corregida la zona horaria de Spark JobHistory. Optimizado el mecanismo de reinicio de MetaStore. Resuelto el problema de código abierto HIVE-22771. Resueltos los errores de impresión del registro beeline de Hive. Corregido el número de nodos activos mostrados en la página de Yarn. Resuelta la lentitud de respuesta de la página RM, causada por un gran número de subprocesos de RM. Monitoreo de OBS soportado. Actualizados los paquetes de OBS. Resuelto el problema de que algunos datos no se insertan cuando 10 registros de datos se insertan simultáneamente en hive-jdbc. Resuelto el problema de que Hive informa ocasionalmente de una falla de deserialización de Kryo. Resuelto el problema de fuga de memoria de Spark JobHistory. Resuelto el problema por el que la lista de aplicaciones no se puede mostrar ocasionalmente en Spark JobHistory.
	Lista de problemas resueltos en MRS 1.9.0.3: **MRS Manager** Actualizado ARM JDK en MRS Manager. Resuelto el problema de que el disco del sistema está totalmente ocupado por registros del nodo Core en MRS Manager. **Componentes de big data de MRS** Resuelto el problema de que no se puede establecer la versión de registros de Ranger, lo que puede causar la ocupación total del disco.

	Lista de problemas resueltos en MRS 1.9.0.2: **MRS Manager** Resuelta la pérdida de confianza mutua entre algunos nodos Core en el clúster. Resuelto el problema de que las instancias no se podían agregar después de instalar el parche. Resuelto el problema de que el intervalo de tiempo de espera de reinicio continuo de HiveServer no se podía modificar en MRS Manager. **Componentes de big data de MRS** Actualizados los paquetes de OBS.
	Lista de problemas resueltos en MRS 1.9.0.1: **MRS Manager** Resuelto el problema de que MRS Manager no admite la instalación de parches continuos sin reiniciar los servicios. **Componentes de big data de MRS** Resuelto el problema de que la frecuencia de acceso confiada a la OBS no se limita a 140 veces en 5 minutos. Resuelto el problema de que Kafka no admite el acceso de código abierto. Resuelto el problema de código abierto SPARK-27637. Optimizado el reinicio continuo de Hive. Actualizados los paquetes de OBS.
Compatibilidad con otros parches	El parche MRS 1.9.0.6 puede resolver todos los problemas que se han resuelto con el parche MRS 1.9.0.

Impacto de la instalación de parches

- Durante la instalación del parche MRS 1.9.0.6, MRS Manager se reiniciará, y los componentes como Hadoop, Hive, Spark, Kafka, Ranger y los servicios dependientes relacionados se reiniciarán en modo rodante. Durante el reinicio de MRS Manager, los servicios no están disponibles temporalmente, pero los servicios no se interrumpen durante el reinicio rodante.
- Después de instalar el parche MRS 1.9.0.6, debe descargar e instalar de nuevo todos los clientes, incluidos los clientes originales de los nodos Master y los clientes utilizados por otros nodos de VPC (es decir, los clientes que ha configurado).
  - Para obtener más información acerca de cómo actualizar completamente el cliente original del nodo maestro activo, consulte **Actualización completa del cliente original del nodo de Master activo**.
  - Para obtener más información acerca de cómo actualizar completamente el cliente original del nodo Master en espera, consulte **Actualización completa del cliente original del nodo de Master en espera**.
  - Para obtener más información acerca de cómo instalar completamente los clientes que configuró, consulte **Instalación de un cliente (Versiones anteriores a 3.x)**.

NOTA

- Se le aconseja hacer una copia de respaldo de los clientes antiguos antes de volver a instalar los nuevos.
- Si ha modificado las configuraciones de cliente según el escenario del servicio, vuelva a modificarlas después de reinstalar los clientes.

3.9.4.22 Descripción del parche MRS 1.9.0.5

Información básica

Tabla 3-79 Información básica

Versión del parche	MRS 1.9.0.5
Fecha de lanzamiento	2020-03-21

Problemas resueltos	**Lista de problemas resueltos en MRS 1.9.0.5:** **MRS Manager** Optimizado el proceso de reinicio del servicio durante el ahorro de configuración en MRS Manager. Rectificado la falla periódica de la copia de respaldo en MRS Manager. **Componentes de big data de MRS** Parche privado de Ranger Resuelto el problema JVM Create GC thread failed de Yarn. Agregada la alarma de apilamiento de tareas de HiveServer2. Agregada la alarma que indica que el tiempo de GC de HiveServer HiveMetastore supera los 5s. Agregada la alarma que indica que HiveServer2 descomenta ZooKeeper. Agregada la alarma que indica que las tareas Yarn han fallado y el número de tareas eliminadas es superior a 5 en 20 minutos. Corregida la zona horaria de Spark JobHistory. Optimizado el mecanismo de reinicio de MetaStore. Resuelto el problema de código abierto HIVE-22771. Resueltos los errores de impresión del registro beeline de Hive. Corregido el número de nodos activos mostrados en la página de Yarn. Resuelta la lentitud de respuesta de la página RM, causada por un gran número de subprocesos de RM. Monitoreo de OBS soportado. Actualizados los paquetes de OBS. Resuelto el problema de que algunos datos no se insertan cuando 10 registros de datos se insertan simultáneamente en hive-jdbc. Resuelto el problema de que Hive informa ocasionalmente de una falla de deserialización de Kryo. Resuelto el problema de fuga de memoria de Spark JobHistory. Resuelto el problema por el que la lista de aplicaciones no se puede mostrar ocasionalmente en Spark JobHistory.
	Lista de problemas resueltos en MRS 1.9.0.3: **MRS Manager** Actualizado ARM JDK en MRS Manager. Resuelto el problema de que el disco del sistema está totalmente ocupado por registros del nodo Core en MRS Manager. **Componentes de big data de MRS** Resuelto el problema de que no se puede establecer la versión de registros de Ranger, lo que puede causar la ocupación total del disco.

	Lista de problemas resueltos en MRS 1.9.0.2: **MRS Manager** Resuelta la pérdida de confianza mutua entre algunos nodos Core en el clúster. Resuelto el problema de que las instancias no se podían agregar después de instalar el parche. Resuelto el problema de que el intervalo de tiempo de espera de reinicio continuo de HiveServer no se podía modificar en MRS Manager. **Componentes de big data de MRS** Actualizados los paquetes de OBS.
	Lista de problemas resueltos en MRS 1.9.0.1: **MRS Manager** Resuelto el problema de que MRS Manager no admite la instalación de parches continuos sin reiniciar los servicios. **Componentes de big data de MRS** Resuelto el problema de que la frecuencia de acceso confiada a la OBS no se limita a 140 veces en 5 minutos. Resuelto el problema de que Kafka no admite el acceso de código abierto. Resuelto el problema de código abierto SPARK-27637. Optimizado el reinicio continuo de Hive. Actualizados los paquetes de OBS.
Compatibilidad con otros parches	El parche MRS 1.9.0.5 puede resolver todos los problemas que se han resuelto con el parche MRS 1.9.0.

Impacto de la instalación de parches

- Durante la instalación del parche MRS 1.9.0.5, MRS Manager se reiniciará, y los componentes como Hadoop, Hive, Spark, Kafka, Ranger y los servicios dependientes relacionados se reiniciarán en modo rodante. Durante el reinicio de MRS Manager, los servicios no están disponibles temporalmente, pero los servicios no se interrumpen durante el reinicio rodante.
- Después de instalar el parche MRS 1.9.0.5, debe descargar e instalar de nuevo todos los clientes, incluidos los clientes originales de los nodos Master y los clientes utilizados por otros nodos de VPC (es decir, los clientes que ha configurado).
  - Para obtener más información acerca de cómo actualizar completamente el cliente original del nodo maestro activo, consulte **Actualización completa del cliente original del nodo de Master activo**.
  - Para obtener más información acerca de cómo actualizar completamente el cliente original del nodo Master en espera, consulte **Actualización completa del cliente original del nodo de Master en espera**.
  - Para obtener más información acerca de cómo instalar completamente los clientes que configuró, consulte **Instalación de un cliente (Versiones anteriores a 3.x)**.

NOTA

- Se le aconseja hacer una copia de respaldo de los clientes antiguos antes de volver a instalar los nuevos.
- Si ha modificado las configuraciones de cliente según el escenario del servicio, vuelva a modificarlas después de reinstalar los clientes.

3.9.4.23 Descripción del parche MRS 1.8.10.1

Información básica

Tabla 3-80 Información básica

Versión del parche	MRS 1.8.10.1
Fecha de lanzamiento	2020-01-07
Problemas resueltos	**Componentes de big data de MRS** La comprobación de estado y la lógica de reinicio continuo de MRS Kafka se han optimizado.
Compatibilidad con otros parches	Ninguna

Impacto de la instalación de parches

Durante la instalación de los parches MRS 1.8.10.1, MRS Manager y Kafka se reinician. Durante el reinicio, los servicios no están disponibles temporalmente.

3.10 Gestión de tenant

3.10.1 Antes de comenzar

Esta sección describe cómo gestionar tenants en la consola MRS.

Las operaciones de gestión de tenant en la consola solo se aplican a clústeres de versiones anteriores a MRS 3.x.

Las operaciones de gestión de tenant en FusionInsight Manager se aplican a todas las versiones. Para las versiones MRS 3.x y posteriores, consulte **Descripción**. Para versiones anteriores a MRS 3.x, consulte **Descripción**.

3.10.2 Descripción

Definición

Un clúster de MRS proporciona varios recursos y servicios para que compartan varias organizaciones, departamentos o aplicaciones. El clúster proporciona tenants como entidad lógica para usar estos recursos y servicios. Un modo que involucra diferentes tenants se llama modo multitenant. Actualmente, solo el clúster de análisis admite la gestión de tenant.

Principios

El clúster de MRS proporciona la función multitenant. Soporta un modelo de tenant por capas y permite agregar o eliminar tenants dinámicos para aislar recursos. Gestiona y configura dinámicamente los recursos informáticos y de almacenamiento de tenants.

Los recursos informáticos indican los recursos de cola de tareas de Yarn de tenants. La cuota de cola de tareas se puede modificar y se pueden ver el estado de uso y las estadísticas de la cola de tareas.

Los recursos de almacenamiento se pueden almacenar en HDFS. Puede agregar y eliminar los directorios de almacenamiento HDFS de tenants y establecer las cuotas de cantidad de archivos y el espacio de almacenamiento de los directorios.

Los tenants pueden crear y gestionar tenants en un clúster según los requisitos de servicio.

- Los roles, los recursos informáticos y los recursos de almacenamiento se crean automáticamente cuando se crean los tenants. De forma predeterminada, todos los permisos de los nuevos recursos informáticos y de almacenamiento se asignan a los roles de un tenant.
- Los permisos para ver los recursos del tenant actual, agregar un subtenant y gestionar los recursos del subtenant se otorgan a los roles del tenant de forma predeterminada.
- Después de modificar los recursos informáticos o de almacenamiento de tenant, los permisos de las funciones de tenant se actualizan automáticamente.

MRS es compatible con un máximo de 512 tenants. Los tenants predeterminados creados por el sistema incluyen **default**. Los tenants que están en la capa superior con el tenant por defecto se denominan tenants de nivel 1.

Grupos de recursos

Las colas de tareas de Yarn sólo admiten la política de programación basada en etiquetas. Esta política permite que las colas de tareas de Yarn asocien NodeManagers que tienen etiquetas de nodo específicas. De esta manera, las tareas de Yarn se ejecutan en nodos especificados para que las tareas se planifiquen y se utilicen ciertos recursos de hardware. Por ejemplo, las tareas de Yarn que requieren una gran capacidad de memoria pueden ejecutarse en nodos con una gran capacidad de memoria por medio de la asociación de etiquetas, evitando un rendimiento de servicio deficiente.

En un clúster MRS, el tenant divide lógicamente los nodos del clúster de Yarn para combinar múltiples NodeManagers en un grupo de recursos. Las colas de tareas de Yarn se pueden asociar a grupos de recursos especificados mediante la configuración de políticas de capacidad de cola, lo que garantiza una utilización eficiente e independiente de los recursos en los grupos de recursos.

MRS admite un máximo de 50 grupos de recursos. De forma predeterminada, el sistema contiene un grupo de recursos de **default**.

3.10.3 Creación de un tenant

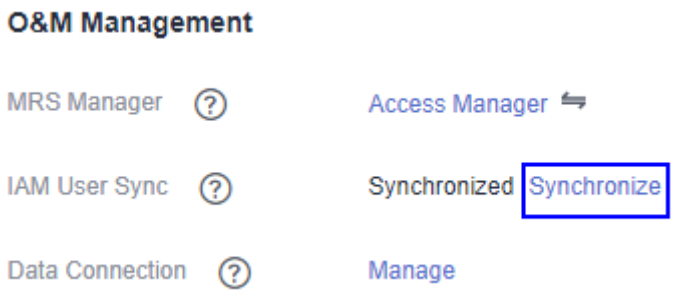
Escenario

Puede crear un tenant en MRS Manager para especificar el uso de recursos.

Prerrequisitos

- Se ha planeado un nombre de tenant. El nombre no debe ser el mismo que el de un rol o una cola de Yarn que exista en el clúster actual.
- Si un tenant requiere recursos de almacenamiento, se planificó un directorio de almacenamiento en función de los requisitos de servicio y el directorio planificado no existe en el directorio HDFS.
- Los recursos que se pueden asignar al tenant actual han sido planificados y la suma de los porcentajes de recursos de subtenants directos bajo el tenant principal en cada nivel no supera el 100%.
- Tiene usuarios de IAM sincronizados. (En la página **Dashboard**, haga clic en **Synchronize** en el lado derecho de **IAM User Sync** para sincronizar usuarios de IAM.)

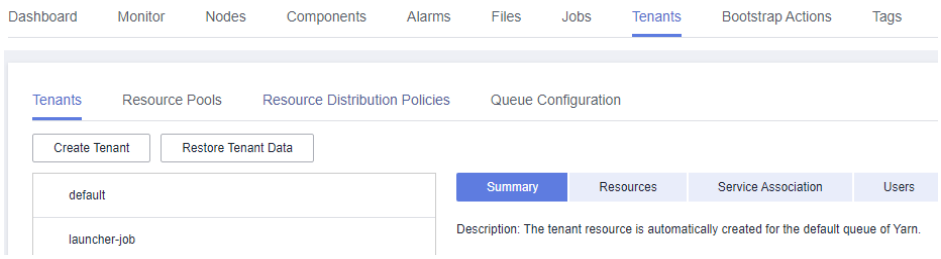
Figura 3-71 Sincronización de usuarios de IAM



Procedimiento

Paso 1 En la página de detalles de MRS, haga clic en **Tenants**.

Figura 3-72 Página de pestaña de tenants



NOTA

Para MRS 3.x o posterior, véase **Descripción**.

Paso 2 Haga clic en **Create Tenant**. En la página que se muestra, configure las propiedades de tenant.

Tabla 3-81 Parámetros del tenant

Parámetro	Descripción
Name	Especifica el nombre del tenant actual. El valor consta de 3 a 50 caracteres y puede contener letras, dígitos y guiones bajos (_).
Tenant Type	Las opciones incluyen **Leaf** y **Non-leaf**. Si se selecciona **Leaf**, el tenant actual es un tenant hoja y no se puede agregar ningún subtenant. Si se selecciona **Non-leaf**, se pueden agregar subtenants al tenant actual.
Dynamic Resource	Especifica los recursos de cálculo dinámicos para el tenant actual. El sistema crea automáticamente una cola de tareas con el nombre del tenant en Yarn. Cuando los recursos dinámicos no son **Yarn**, el sistema no crea automáticamente una cola de tareas.
Default Resource Pool Capacity (%)	Especifica el porcentaje de los recursos informáticos utilizados por el tenant actual en el grupo de recursos **default**.
Default Resource Pool Max. Capacity (%)	Especifica el porcentaje máximo de los recursos informáticos utilizados por el tenant actual en el grupo de recursos **default**.
Storage Resource	Especifica los recursos de almacenamiento para el tenant actual. El sistema crea automáticamente una carpeta de archivos con el nombre de tenant en el directorio **/tenant**. Cuando se crea un tenant por primera vez, el sistema crea automáticamente el directorio **/tenant** en el directorio raíz HDFS. Si los recursos de almacenamiento no son **HDFS**, el sistema no crea un directorio de almacenamiento bajo el directorio raíz de HDFS.
Space Quota (MB)	Especifica la cuota de espacio de almacenamiento de HDFS utilizada por el tenant actual. El valor oscila entre **1** y **8796093022208**. La unidad es MB. Este parámetro indica el espacio de almacenamiento de HDFS máximo que puede utilizar un tenant, pero no indica el espacio real utilizado. Si el valor es mayor que el tamaño del disco físico de HDFS, el espacio máximo disponible es el espacio completo del disco físico de HDFS. **NOTA** Para garantizar la confiabilidad de los datos, se genera automáticamente una copia de respaldo por cada archivo guardado en HDFS, es decir, se generan dos copias en total. El espacio de almacenamiento de HDFS indica el espacio total en disco ocupado por todas estas copias. Por ejemplo, si el valor se establece en **500**, el espacio real para almacenar archivos es de aproximadamente 250 MB (500/2 = 250).

Parámetro	Descripción
Storage Path	Especifica el directorio de almacenamiento de HDFS del tenant. El sistema crea automáticamente una carpeta de archivos con el nombre del tenant en el directorio **/tenant** de forma predeterminada. Por ejemplo, el directorio de almacenamiento HDFS predeterminado para **ta1** es **tenant/ta1**. Cuando se crea un tenant por primera vez, el sistema crea automáticamente el directorio **/tenant** en el directorio raíz HDFS. La ruta de almacenamiento es personalizable.
Service	Especifica otros recursos de servicio asociados con el tenant actual. HBase es compatible. Para configurar este parámetro, haga clic en **Associate Services**. En el cuadro de diálogo que se muestra, establezca **Service** en **HBase**. Si **Association Mode** se establece en **Exclusive**, los recursos de servicio se ocupan exclusivamente. Si se selecciona **share**, se comparten los recursos de servicio.
Description	Especifica la descripción del tenant actual.

Paso 3 Haga clic en **OK** para guardar la configuración.

Se tarda unos minutos en guardar la configuración. Si el **Tenant created successfully** se muestra en la esquina superior derecha, el tenant se agrega correctamente. El tenant se crea con éxito.

NOTA

- Los roles, los recursos informáticos y los recursos de almacenamiento se crean automáticamente cuando se crean los tenants.
- El nuevo rol tiene permisos sobre los recursos informáticos y de almacenamiento. El rol y sus permisos son controlados por el sistema automáticamente y no pueden ser controlados manualmente en **Manage Role**.
- Si desea utilizar el tenant, cree un usuario del sistema y asigne al usuario el rol Manager_tenant y el rol correspondiente al tenant. Para obtener más información, consulte **Creación de un usuario**.

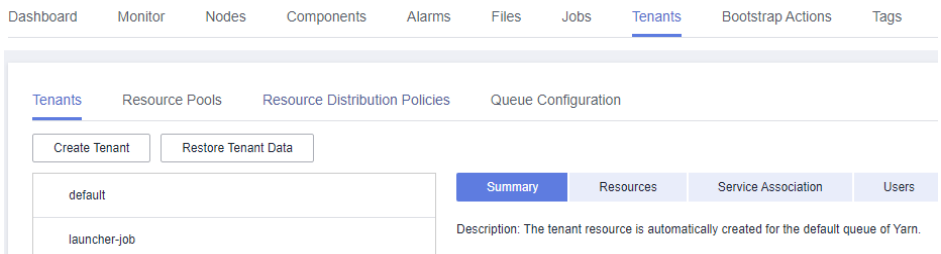
----Fin

Tareas relacionadas

Ver un tenant agregado.

Paso 1 En la página de detalles de MRS, haga clic en **Tenants**.

Figura 3-73 Página de pestaña de tenants



Paso 2 En la lista de tenant de la izquierda, haga clic en el nombre del tenant agregado.

La pestaña **Summary** se muestra a la derecha de forma predeterminada.

Paso 3 Vea **Basic Information**, **Resource Quota** y **Statistics** del tenant.

Si HDFS está en el estado **Stopped**, **Available** y **Used** de **Space** en **Resource Quota** son **unknown.**

----Fin

3.10.4 Creación de un subtenant

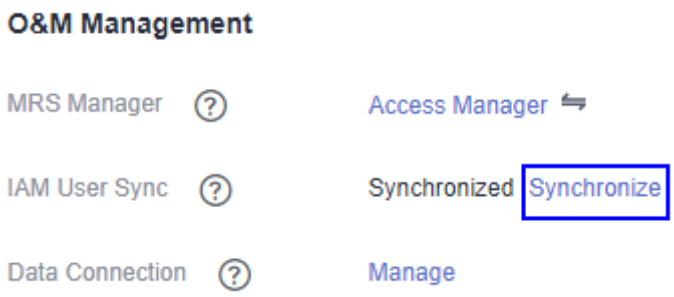
Escenario

Puede crear un subtenant en MRS si los recursos del tenant actual necesitan ser asignados más.

Prerrequisitos

- Se ha añadido un tenant principal.
- Se ha planeado un nombre de tenant. El nombre no debe ser el mismo que el de un rol o una cola de Yarn que exista en el clúster actual.
- Si un subtenant requiere recursos de almacenamiento, se ha planificado un directorio de almacenamiento en función de los requisitos de servicio y el directorio planificado no existe en el directorio de almacenamiento del tenant principal.
- Los recursos que se pueden asignar al tenant actual han sido planificados y la suma de los porcentajes de recursos de subtenants directos bajo el tenant principal en cada nivel no supera el 100%.
- Tiene usuarios de IAM sincronizados. (En la página **Dashboard**, haga clic en **Synchronize** en el lado derecho de **IAM User Sync** para sincronizar usuarios de IAM.)

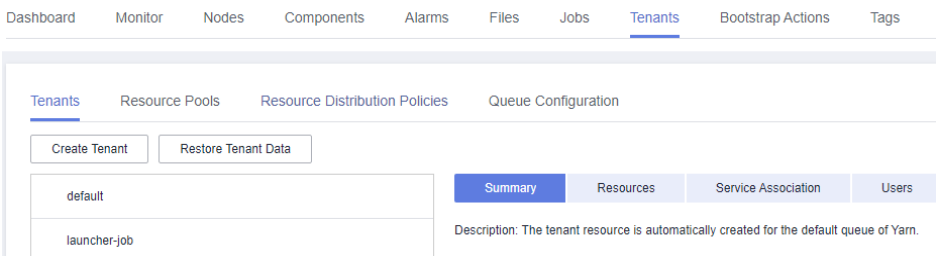
Figura 3-74 Sincronización de usuarios de IAM



Procedimiento

Paso 1 En la página de detalles de MRS, haga clic en **Tenants**.

Figura 3-75 Página de pestaña de tenants



NOTA

Para MRS 3.x o posterior, véase **Descripción**.

Paso 2 En la lista de tenant de la izquierda, mueva el cursor al nodo de tenant al que se va a agregar un subtenant. Haga clic en **Create sub-tenant**. En la página mostrada, configure los atributos de subtenant de acuerdo con la siguiente tabla:

Tabla 3-82 Parámetros de subtenant

Parámetro	Descripción
Parent tenant	Especifica el nombre del tenant principal.
Name	Especifica el nombre del tenant actual. El valor consta de 3 a 20 caracteres y puede contener letras, dígitos y guiones bajos (_).
Tenant Type	Las opciones incluyen **Leaf** y **Non-leaf**. Si se selecciona **Leaf**, el tenant actual es un tenant hoja y no se puede agregar ningún subtenant. Si se selecciona **Non-leaf**, se pueden agregar subtenants al tenant actual.
Dynamic Resource	Especifica los recursos de cálculo dinámicos para el tenant actual. El sistema crea automáticamente una cola de tareas con el nombre del subtenant en la cola principal de Yarn. Cuando los recursos dinámicos no son **Yarn**, el sistema no crea automáticamente una cola de tareas. Si el tenant principal no tiene recursos dinámicos, el subtenant no puede usar recursos dinámicos.
Default Resource Pool Capacity (%)	Especifica el porcentaje de recursos utilizados por el tenant actual. El valor base es el total de recursos del tenant principal.
Default Resource Pool Max. Capacity (%)	Especifica el porcentaje máximo de los recursos informáticos utilizados por el tenant actual. El valor base es el total de recursos del tenant principal.

Parámetro	Descripción
Storage Resource	Especifica los recursos de almacenamiento para el tenant actual. El sistema crea automáticamente un archivo en el directorio de tenant principal de HDFS. El nombre del archivo es el mismo que el nombre del subtenant. Si los recursos de almacenamiento no son **HDFS**, el sistema no crea un directorio de almacenamiento bajo el directorio raíz de HDFS. Si el tenant principal no tiene recursos de almacenamiento, el subtenant no puede usar recursos de almacenamiento.
Space Quota (MB)	Especifica la cuota de espacio de almacenamiento de HDFS utilizada por el tenant actual. El valor mínimo es 1, y el valor máximo es la cuota de almacenamiento total del tenant principal. La unidad es MB. Este parámetro indica el espacio de almacenamiento de HDFS máximo que puede utilizar un tenant, pero no indica el espacio real utilizado. Si el valor es mayor que el tamaño del disco físico de HDFS, el espacio máximo disponible es el espacio completo del disco físico de HDFS. Si la cuota es mayor que la cuota del tenant principal, la capacidad de almacenamiento real está sujeta a la cuota del tenant principal. **NOTA** Para garantizar la confiabilidad de los datos, se genera automáticamente una copia de respaldo por cada archivo guardado en HDFS, es decir, se generan dos copias en total. El espacio de almacenamiento de HDFS indica el espacio total en disco ocupado por todas estas copias. Por ejemplo, si el valor se establece en **500**, el espacio real para almacenar archivos es de aproximadamente 250 MB (500/2 = 250).
Storage Path	Especifica el directorio de almacenamiento de HDFS del tenant. El sistema crea automáticamente una carpeta de archivos con el nombre del subtenant en el directorio del tenant principal de forma predeterminada. Por ejemplo, si el subtenant es **ta1s** y el directorio principal es **tenant/ta1**, el sistema establece este parámetro para el subtenant en **tenant/ta1/ta1s**. La ruta de almacenamiento se puede personalizar en el directorio principal. El directorio principal de la ruta de almacenamiento debe ser el directorio de almacenamiento del tenant principal.
Service	Especifica otros recursos de servicio asociados con el tenant actual. HBase es compatible. Para configurar este parámetro, haga clic en **Associate Services**. En el cuadro de diálogo que se muestra, establezca **Service** en **HBase**. Si **Association Mode** se establece en **Exclusive**, los recursos de servicio se ocupan exclusivamente. Si se selecciona **share**, se comparten los recursos de servicio.
Description	Especifica la descripción del tenant actual.

Paso 3 Haga clic en **OK** para guardar la configuración.

Se tarda unos minutos en guardar la configuración. Si el **Tenant created successfully** se muestra en la esquina superior derecha, el tenant se agrega correctamente. El tenant se crea con éxito.

NOTA

- Los roles, los recursos informáticos y los recursos de almacenamiento se crean automáticamente cuando se crean los tenants.
- El nuevo rol tiene permisos sobre los recursos informáticos y de almacenamiento. El rol y sus permisos son controlados por el sistema automáticamente y no pueden ser controlados manualmente en **Manage Role**.
- Cuando utilice este tenant, cree un usuario del sistema y asigne al usuario un rol de tenant relacionado. Para obtener más información, consulte **Creación de un usuario**.

----Fin

3.10.5 Eliminación de un tenant

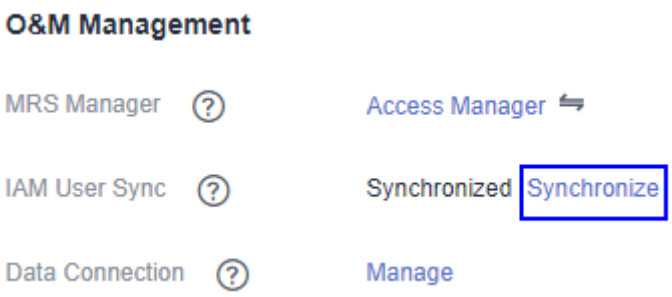
Escenario

Puede eliminar un tenant que no sea necesario en MRS.

Prerrequisitos

- Se ha agregado un tenant.
- Ha comprobado si el tenant que se va a eliminar tiene subtenants. Si el tenant tiene subtenants, elimínelos; de lo contrario, no podrá eliminar el tenant.
- El rol del tenant que se va a eliminar no se puede asociar a ningún usuario o grupo de usuarios. Para obtener más información sobre cómo cancelar el enlace entre un rol y un usuario, consulte **Modificación de la información de usuario**.
- Tiene usuarios de IAM sincronizados. (En la página **Dashboard**, haga clic en **Synchronize** en el lado derecho de **IAM User Sync** para sincronizar usuarios de IAM.)

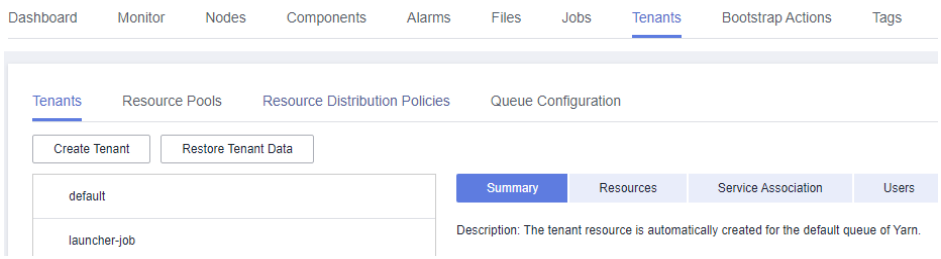
Figura 3-76 Sincronización de usuarios de IAM



Procedimiento

Paso 1 En la página de detalles de MRS, haga clic en **Tenants**.

Figura 3-77 Página de pestaña de tenants



NOTA

Para MRS 3.x o posterior, consulte **Descripción**.

Paso 2 En la lista de inquilinos de la izquierda, mueva el cursor hasta el nodo de tenant que se va a eliminar y haga clic en **Delete**.

Aparece el cuadro de diálogo **Delete Tenant**. Si desea guardar los datos del tenant, seleccione **Reserve the data of this tenant**. De lo contrario, se eliminará el espacio de almacenamiento del tenant.

Paso 3 Haga clic en **OK**.

Se tarda unos minutos en guardar la configuración. Una vez que el tenant se elimina correctamente, el rol y el espacio de almacenamiento del tenant también se eliminan.

NOTA

- Después de eliminar el tenant, la cola de tareas del tenant todavía existe en Yarn.
- Si decide no reservar datos al eliminar el tenant principal, también se eliminarán los datos de los subtenants si los subtenants utilizan recursos de almacenamiento.

----Fin

3.10.6 Gestión de directorio de tenant

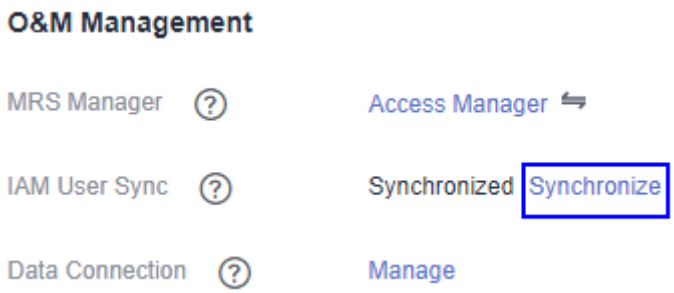
Escenario

Puede gestionar el directorio de almacenamiento de HDFS utilizado por un tenant específico en MRS. Las operaciones de gestión incluyen agregar un directorio de tenant, modificar la cuota de archivo de directorio, modificar el espacio de almacenamiento y eliminar un directorio.

Prerrequisitos

- Se ha agregado un tenant asociado con los recursos de almacenamiento de HDFS.
- Tiene usuarios de IAM sincronizados. (En la página **Dashboard**, haga clic en **Synchronize** en el lado derecho de **IAM User Sync** para sincronizar usuarios de IAM.)

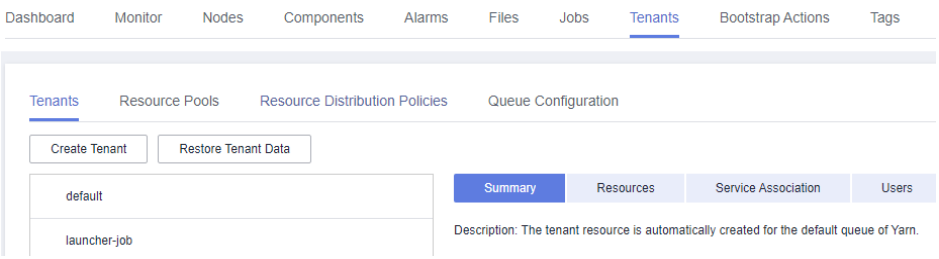
Figura 3-78 Sincronización de usuarios de IAM



Procedimiento

- Ver un directorio de tenant.
  a. En la página de detalles de MRS, haga clic en **Tenants**.

  Figura 3-79 Página de pestaña de tenants

  NOTA

  Para MRS 3.x o posterior, consulte **Descripción**.

  b. En la lista de tenant de la izquierda, haga clic en el tenant de destino.
  c. Haga clic en la pestaña **Resources**.
  d. Vea la tabla **HDFS Storage**.
     - La columna **Maximum Number of Files/Directories** indica las cuotas para la cantidad de archivos y directorios del directorio del tenant.
     - La columna **Space Quota** indica el tamaño del espacio de almacenamiento de los directorios del tenant.
- Agregue un directorio de tenant.
  a. En la página de detalles de MRS, haga clic en **Tenants**.

  NOTA

  Para MRS 3.x o posterior, consulte **Descripción**.

  b. En la lista de tenant de la izquierda, haga clic en el tenant cuyo directorio de almacenamiento de HDFS debe agregarse.
  c. Haga clic en la pestaña **Resources**.
  d. En la tabla **HDFS Storage**, haga clic en **Create Directory**.
     - Establezca **Path** en una ruta de directorio del tenant.

NOTA

- Si el tenant actual no es un subtenant, la nueva ruta se crea en el directorio raíz de HDFS.
- Si el tenant actual es un subtenant, la nueva ruta se crea en el directorio especificado.

Un directorio de almacenamiento de HDFS completo puede contener un máximo de 1,023 caracteres. Un nombre de directorio de HDFS contiene dígitos, letras, espacios y guiones bajos (_). El nombre no puede comenzar ni terminar con un espacio.

- Establezca **Maximum Number of Files/Directories** en las cuotas de cantidad de archivos y directorios.

  Maximum Number of Files/Directories es opcional. Su valor oscila entre **1** y **9223372036854775806**.

- Establezca **Storage Space Quota** en el tamaño del espacio de almacenamiento del directorio del tenant.

  El valor de **Storage Space Quota** oscila entre **1** y **8796093022208**.

  NOTA

  Para garantizar la confiabilidad de los datos, se genera automáticamente una copia de respaldo por cada archivo guardado en HDFS, es decir, se generan dos copias en total. El espacio de almacenamiento HDFS indica el espacio total en disco ocupado por todas estas copias. Por ejemplo, si el valor de **Storage Space Quota** se establece en **500**, el espacio real para almacenar archivos es de aproximadamente 250 MB (500/2 = 250).

e. Haga clic en **OK**. El sistema crea directorios de tenant en el directorio raíz de HDFS.

- Modificar un directorio de tenant.

  a. En la página de detalles de MRS, haga clic en **Tenants**.

  NOTA

  Para MRS 3.x o posterior, consulte **Descripción**.

  b. En la lista de tenant de la izquierda, haga clic en el tenant cuyo directorio de almacenamiento de HDFS necesita modificarse.

  c. Haga clic en la pestaña **Resources**.

  d. En la tabla **HDFS Storage**, haga clic en **Modify** en la columna **Operation** del directorio de tenant especificado.

  - Establezca **Maximum Number of Files/Directories** en las cuotas de cantidad de archivos y directorios.

    Maximum Number of Files/Directories es opcional. Su valor oscila entre **1** y **9223372036854775806**.

  - Establezca **Storage Space Quota** en el tamaño del espacio de almacenamiento del directorio del tenant.

    El valor de **Storage Space Quota** oscila entre **1** y **8796093022208**.

> **NOTA**
>
> Para garantizar la confiabilidad de los datos, se genera automáticamente una copia de respaldo por cada archivo guardado en HDFS, es decir, se generan dos copias en total. El espacio de almacenamiento HDFS indica el espacio total en disco ocupado por todas estas copias. Por ejemplo, si el valor de **Storage Space Quota** se establece en **500**, el espacio real para almacenar archivos es de aproximadamente 250 MB (500/2 = 250).

e. Haga clic en **OK**.

- Eliminar un directorio de tenant.

  a. En la página de detalles de MRS, haga clic en **Tenants**.

  > **NOTA**
  >
  > Para MRS 3.x o posterior, consulte **Descripción**.

  b. En la lista de tenant de la izquierda, haga clic en el tenant cuyo directorio de almacenamiento HDFS debe eliminarse.

  c. Haga clic en la pestaña **Resources**.

  d. En la tabla **HDFS Storage**, haga clic en **Delete** en la columna **Operation** del directorio de tenant especificado.

  No se puede eliminar el directorio de almacenamiento HDFS predeterminado establecido durante la creación del tenant. Solo se puede eliminar el directorio de almacenamiento HDFS recién agregado.

  e. Haga clic en **OK**. Se elimina el directorio del tenant.

3.10.7 Restauración de datos de tenant

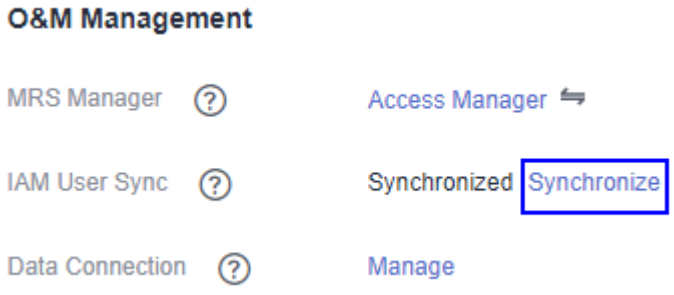
Escenario

Los datos del tenant se almacenan en Manager y en los componentes del clúster de forma predeterminada. Cuando los componentes se restauran de fallas o se reinstalan, algunos datos de configuración del tenant pueden ser anormales. En este caso, puede restaurar manualmente los datos del tenant.

Prerrequisitos

Tiene usuarios de IAM sincronizados. (En la página **Dashboard**, haga clic en **Synchronize** en el lado derecho de **IAM User Sync** para sincronizar usuarios de IAM.)

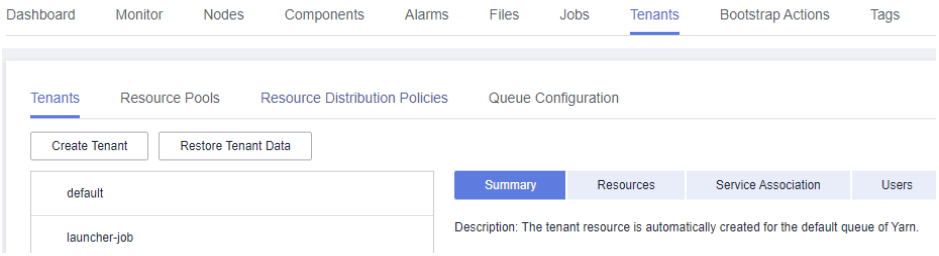
Figura 3-80 Sincronización de usuarios de IAM



Procedimiento

Paso 1 En la página de detalles de MRS, haga clic en **Tenants**.

Figura 3-81 Página de pestaña de tenants



NOTA

Para MRS 3.x o posterior, consulte **Descripción**.

Paso 2 En la lista de tenant de la izquierda, haga clic en un nodo de tenant.

Paso 3 Compruebe el estado de los datos del tenant.

1. En **Summary**, comprueba el color del círculo a la izquierda de **Basic Information**. El verde indica que el tenant está disponible y el gris indica que el tenant no está disponible.
2. Haga clic en **Resources** y marque el círculo a la izquierda de **Yarn** o **HDFS Storage**. El verde indica que el recurso está disponible y el gris indica que el recurso no está disponible.
3. Haga clic en **Service Association** y compruebe la columna **Status** de la tabla de servicios asociada. **Good** indica que el componente puede proporcionar servicios para el tenant asociado. **Bad** indica que el componente no puede proporcionar servicios al tenant.
4. Si cualquier resultado de la comprobación es anormal, vaya a **Paso 4** para restaurar los datos del tenant.

Paso 4 Haga clic en **Restore Tenant Data**.

Paso 5 En la ventana **Restore Tenant Data**, seleccione uno o más componentes cuyos datos deben restaurarse. Haga clic en **OK**. El sistema restaura automáticamente los datos del tenant.

----Fin

3.10.8 Creación de un grupo de recursos

Escenario

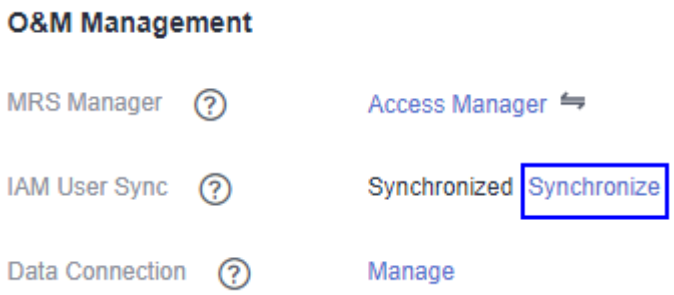
En un clúster MRS, los usuarios pueden dividir lógicamente los nodos del clúster de Yarn para combinar múltiples NodeManagers en un grupo de recursos de Yarn. Cada NodeManager pertenece únicamente a un grupo de recursos. El sistema contiene un grupo de recursos **default** de forma predeterminada. Todas las NodeManagers que no se agregan a grupos de recursos personalizados pertenecen a este grupo de recursos.

Puede crear un grupo de recursos personalizado en MRS y agregar hosts que no se hayan agregado a otros grupos de recursos personalizados.

Prerrequisitos

Tiene usuarios de IAM sincronizados. (En la página **Dashboard**, haga clic en **Synchronize** en el lado derecho de **IAM User Sync** para sincronizar usuarios de IAM.)

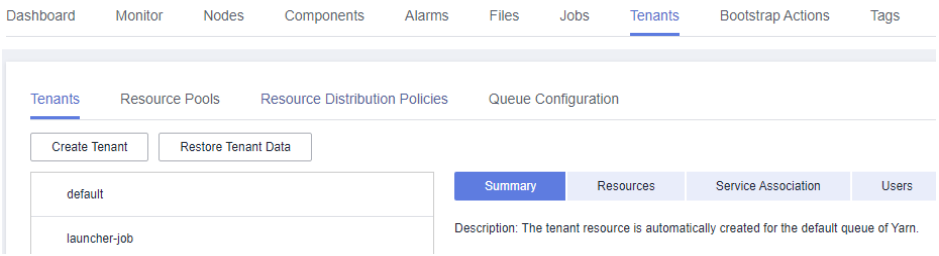
Figura 3-82 Sincronización de usuarios de IAM



Procedimiento

Paso 1 En la página de detalles de MRS, haga clic en **Tenants**.

Figura 3-83 Página de pestaña de tenants



NOTA

Para MRS 3.x o posterior, consulte **Descripción**.

Paso 2 Haga clic en la pestaña **Resource Pools**.

Paso 3 Haga clic en **Create Resource Pool**.

Paso 4 En **Create Resource Pool**, defina las propiedades del grupo de recursos.

- **Name**: Introduzca un nombre para el grupo de recursos. El nombre del grupo de recursos recién creado no puede ser **default**.

  El nombre consta de 1 a 20 caracteres y puede contener dígitos, letras y guiones bajos (_) pero no puede comenzar con un guion bajo (_).
- **Available Hosts**: En la lista de hosts de la izquierda, seleccione un nombre de host especificado y agréguelo al grupo de recursos. Solo se pueden seleccionar los hosts del clúster. La lista de hosts de un grupo de recursos se puede dejar en blanco.

Paso 5 Haga clic en **OK**.

Paso 6 Después de crear un grupo de recursos, los usuarios pueden ver **Name**, **Members**, **Type**, **vCore** y **Memory** en la lista del grupo de recursos. Los hosts que se agregan al grupo de recursos personalizado ya no son miembros del grupo de recursos **default**.

----Fin

3.10.9 Modificación de un grupo de recursos

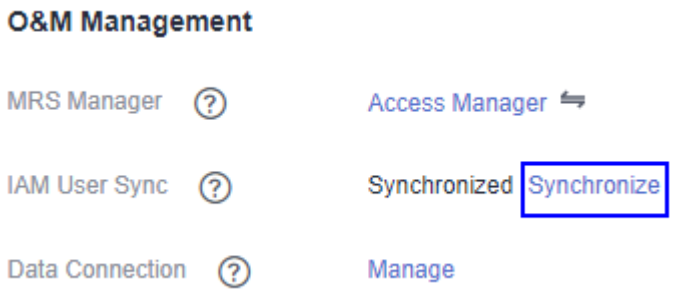
Escenario

Puede modificar miembros de un grupo de recursos existente en MRS.

Prerrequisitos

Tiene usuarios de IAM sincronizados. (En la página **Dashboard**, haga clic en **Synchronize** en el lado derecho de **IAM User Sync** para sincronizar usuarios de IAM.)

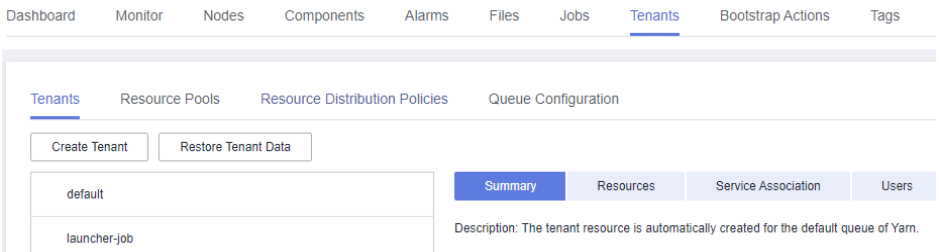
Figura 3-84 Sincronización de usuarios de IAM



Procedimiento

Paso 1 En la página de detalles de MRS, haga clic en **Tenants**.

Figura 3-85 Página de pestaña de tenants



NOTA

Para MRS 3.x o posterior, consulte **Descripción**.

Paso 2 Haga clic en la pestaña **Resource Pools**.

Paso 3 Busque la fila que contiene el grupo de recursos especificado y haga clic en **Modify** en la columna **Operation**.

Paso 4 En **Modify Resource Pool**, modifique **Added Hosts**.

- Agregar un host: En la lista de hosts de la izquierda, seleccione el nombre de host especificado y agréguelo al grupo de recursos.
- Eliminar un host: En la lista de hosts de la derecha, haga clic en junto a un host para quitar el host del grupo de recursos. La lista de hosts de un grupo de recursos se puede dejar en blanco.

Paso 5 Haga clic en **OK**.

----Fin

3.10.10 Eliminación de un grupo de recursos

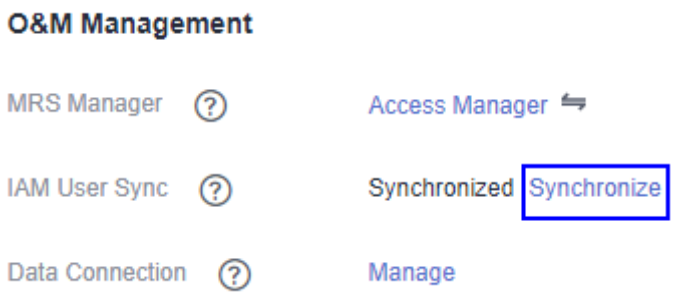
Escenario

Puede eliminar un grupo de recursos existente en MRS.

Prerrequisitos

- Cualquier cola de un clúster no puede utilizar el grupo de recursos que se va a eliminar como grupo de recursos predeterminado. Antes de eliminar el grupo de recursos, cancele el grupo de recursos predeterminado. Para más detalles, consulte **Configuración de una cola**.
- Las políticas de distribución de recursos de todas las colas se han borrado del grupo de recursos que se está eliminando. Para más detalles, consulte **Borrar la configuración de una cola**.
- Tiene usuarios de IAM sincronizados. (En la página **Dashboard**, haga clic en **Synchronize** en el lado derecho de **IAM User Sync** para sincronizar usuarios de IAM.)

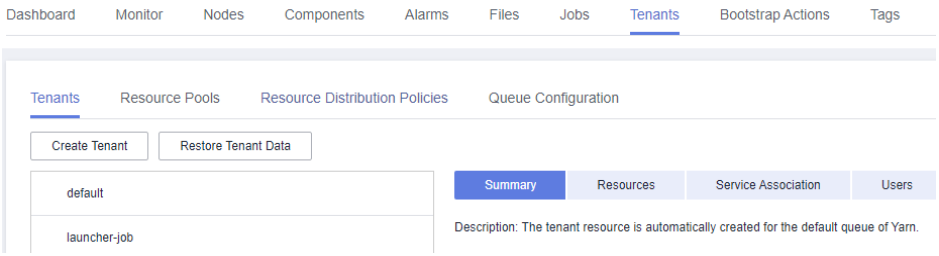
Figura 3-86 Sincronización de usuarios de IAM



Procedimiento

Paso 1 En la página de detalles de MRS, haga clic en **Tenant**.

Figura 3-87 Página de pestaña de tenants



NOTA

Para MRS 3.x o posterior, consulte **Descripción**.

Paso 2 Haga clic en la pestaña **Resource Pools**.

Paso 3 Busque la fila que contiene el grupo de recursos especificado y haga clic en **Delete** en la columna **Operation**.

En el cuadro de diálogo que se muestra, haga clic en **OK**.

----Fin

3.10.11 Configuración de una cola

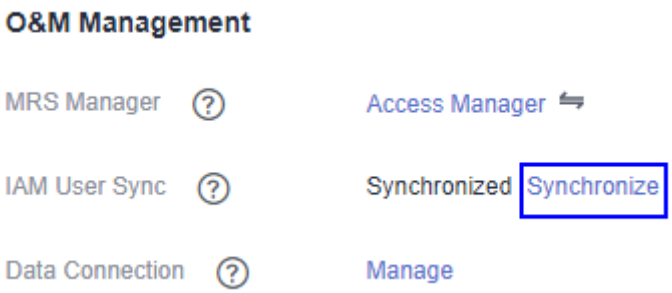
Escenario

Puede modificar la configuración de cola de un tenant especificado en MRS según los requisitos de servicio.

Prerrequisitos

- Se ha agregado un tenant asociado con Yarn y recursos dinámicos asignados.
- Tiene usuarios de IAM sincronizados. (En la página **Dashboard**, haga clic en **Synchronize** en el lado derecho de **IAM User Sync** para sincronizar usuarios de IAM.)

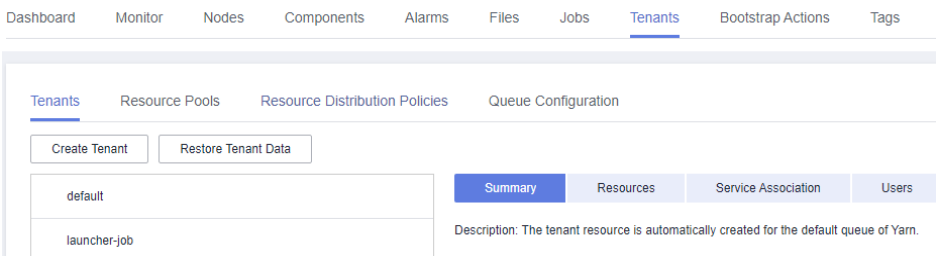
Figura 3-88 Sincronización de usuarios de IAM



Procedimiento

Paso 1 En la página de detalles de MRS, haga clic en **Tenants**.

Figura 3-89 Página de pestaña de tenants



NOTA

Para MRS 3.x o posterior, consulte **Descripción**.

Paso 2 Haga clic en la pestaña **Queue Configuration**.

Paso 3 En la tabla de colas de tenant, haga clic en **Modify** en la columna **Operation** de la cola de tenant especificada.

NOTA

- En la lista de tenant a la izquierda de la pestaña **Tenant Management**, haga clic en el tenant de destino. En la ventana que se muestra, elija **Resource**. En la página que se muestra, haga clic en para abrir la página de modificación de cola.
- Una cola puede estar enlazada a un solo grupo de recursos no predeterminado.

Versiones anteriores a MRS 3.x:

Tabla 3-83 Parámetros de configuración de cola

Parámetro	Descripción
Maximum Applications	Especifica el número máximo de aplicaciones. El valor oscila entre 1 y 2147483647.
Maximum AM Resource Percent	Especifica el porcentaje máximo de recursos que se pueden utilizar para ejecutar el ApplicationMaster en un clúster. El valor varía de 0 a 1.
Minimum User Limit Percent (%)	Especifica el porcentaje mínimo de recursos consumidos por un usuario. El valor varía de 0 a 100.
User Limit Factor	Especifica el factor límite del uso máximo de recursos de usuario. El porcentaje máximo de uso de recursos de usuario se puede obtener multiplicando el factor límite por el porcentaje del uso real de recursos del tenant en el clúster. El valor mínimo es **0**.
Status	Especifica el estado actual de un plan de recursos. Los valores son **Running** y **Stopped**.

Parámetro	Descripción
Default Resource Pool (Default Node Label Expression)	Especifica el grupo de recursos utilizado por una cola. El valor predeterminado es **default**. Si desea cambiar el grupo de recursos, configure primero la capacidad de la cola. Para obtener más información, consulte **Configuración de la política de capacidad de cola de un grupo de recursos**.

MRS 3.x o posterior:

Tabla 3-84 Parámetros de configuración de cola

Parámetro	Descripción
Max Master Shares (%)	Indica el porcentaje máximo de recursos ocupados por todas las ApplicationMasters de la cola actual.
Max Allocated vCores	Indica el número máximo de núcleos que se pueden asignar a un solo contenedor de YARN en la cola actual. El valor predeterminado es **-1**, lo que indica que el número de núcleos no está limitado dentro del rango de valores.
Max Allocated Memory (MB)	Indica la memoria máxima que se puede asignar a un solo contenedor de Yarn en la cola actual. El valor predeterminado es **-1**, lo que indica que la memoria no está limitada dentro del rango de valores.
Max Running Apps	Número máximo de tareas que se pueden ejecutar al mismo tiempo en la cola actual. El valor predeterminado es **-1**, lo que indica que el número no está limitado dentro del rango de valores. (el significado es el mismo si el valor está vacío). El valor 0 indica que la tarea no se puede ejecutar. El valor oscila entre -1 y 2147483647.
Max Running Apps per User	Número máximo de tareas que puede ejecutar cada usuario en la cola actual al mismo tiempo. El valor predeterminado es **-1**, lo que indica que el número no está limitado dentro del rango de valores. Si el valor es de **0**, no se puede ejecutar la tarea. El valor oscila entre -1 y 2147483647.
Max Pending Apps	Número máximo de tareas que se pueden suspender al mismo tiempo en la cola actual. El valor predeterminado es **-1**, lo que indica que el número no está limitado dentro del rango de valores (el significado es el mismo si el valor está vacío). El valor **0** indica que las tareas no se pueden suspender. El valor oscila entre -1 y 2147483647.

Parámetro	Descripción
Resource Allocation Rule	Indica la regla para asignar recursos a diferentes tareas de un usuario. La regla puede ser FIFO o FAIR. Si un usuario envía varias tareas en la cola actual y la regla es FIFO, las tareas se ejecutan una por una en orden secuencial. Si la regla es FAIR, los recursos se asignan uniformemente a todas las tareas.
Default Resource Label	Indica que las tareas se ejecutan en un nodo con una etiqueta de recurso especificada. **NOTA** Si necesita utilizar un nuevo grupo de recursos, cambie la etiqueta predeterminada por la nueva etiqueta del grupo de recursos.
Active	● **ACTIVE**: indica que la cola actual puede recibir y ejecutar tareas. ● **INACTIVE**: indica que la cola actual puede recibir pero no puede ejecutar tareas. Las tareas enviadas a la cola se suspenden.
Open	● **OPEN**: indica que la cola actual está abierta. ● **CLOSED**: indica que la cola actual está cerrada. Las tareas enviadas a la cola se rechazan.

----Fin

3.10.12 Configuración de la política de capacidad de cola de un grupo de recursos

Escenario

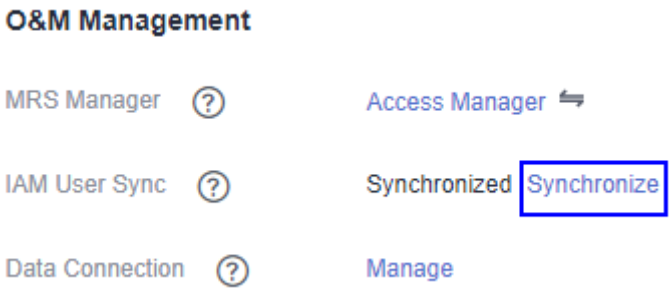
Después de agregar un grupo de recursos, las políticas de capacidad de los recursos disponibles deben configurarse para las colas de tareas de Yarn. Esto garantiza que las tareas del grupo de recursos se estén ejecutando correctamente. Cada cola se puede configurar con la política de capacidad de cola de un solo grupo de recursos. Los usuarios pueden ver las colas en cualquier grupo de recursos y configurar políticas de capacidad de cola. Una vez configuradas las políticas de cola, se asocian las colas de tareas de Yarn y los grupos de recursos.

Puede configurar las directivas de cola en MRS.

Prerrequisitos

- Se ha agregado un grupo de recursos.
- Las colas de tareas no están asociadas con otros grupos de recursos. De forma predeterminada, todas las colas están asociadas al grupo de recursos **Default**.
- Tiene usuarios de IAM sincronizados. (En la página **Dashboard**, haga clic en **Synchronize** en el lado derecho de **IAM User Sync** para sincronizar usuarios de IAM.)

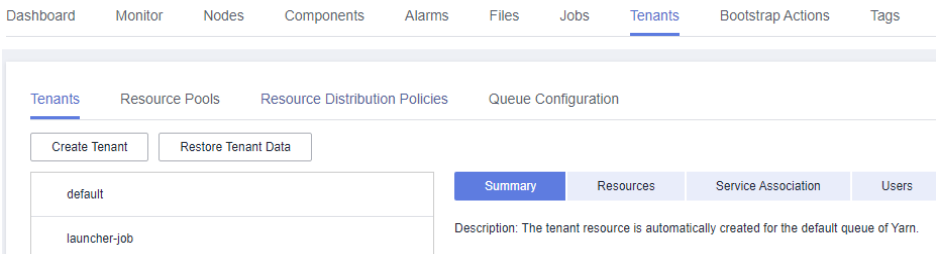
Figura 3-90 Sincronización de usuarios de IAM



Procedimiento

Paso 1 En la página de detalles de MRS, haga clic en **Tenants**.

Figura 3-91 Página de pestaña de tenants



NOTA

Para MRS 3.x o posterior, consulte **Descripción**.

Paso 2 Haga clic en la pestaña **Resource Distribution Policies**.

Paso 3 En el campo **Resource Pools**, seleccione un grupo de recursos especificado.

Available Resource Quota: indica que todos los recursos de cada grupo de recursos están disponibles para colas de forma predeterminada.

Paso 4 Busque la cola especificada en la tabla **Resource Allocation** y haga clic en **Modify** en la columna **Operation**.

Paso 5 En **Modify Resource Allocation**, configure la política de capacidad de recursos de la cola de tareas en el grupo de recursos.

- **Capacity (%)**: especifica el porcentaje del uso de recursos informáticos del tenant actual.
- **Maximum Capacity (%)**: especifica el porcentaje del uso máximo de recursos informáticos del tenant actual.

Paso 6 Haga clic en **OK** para guardar la configuración.

----Fin

3.10.13 Borrar la configuración de una cola

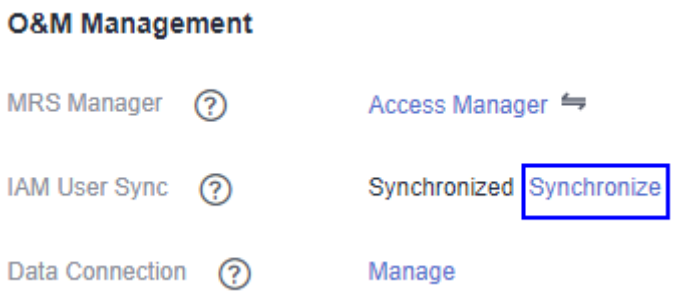
Escenario

Los usuarios pueden borrar la configuración de una cola en MRS Manager cuando la cola no necesita recursos de un grupo de recursos o si un grupo de recursos necesita estar desasociado de la cola. Borrar configuraciones de cola significa que se cancela la política de capacidad de recursos de la cola.

Prerrequisitos

- Si una cola va a ser independiente de un grupo de recursos, este grupo de recursos no puede servir como el grupo de recursos predeterminado de la cola. Por lo tanto, primero debe cambiar el grupo de recursos predeterminado de la cola a otro. Para obtener más información, véase **Configuración de una cola**.
- Tiene usuarios de IAM sincronizados. (En la página **Dashboard**, haga clic en **Synchronize** en el lado derecho de **IAM User Sync** para sincronizar usuarios de IAM.)

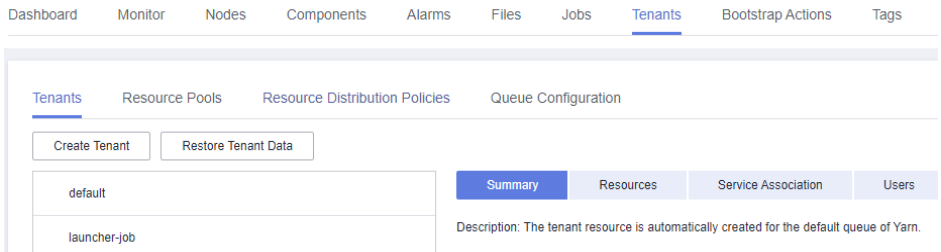
Figura 3-92 Sincronización de usuarios de IAM



Procedimiento

Paso 1 En la página de detalles de MRS, haga clic en **Tenants**.

Figura 3-93 Página de pestaña de tenants



NOTA

Para MRS 3.x o posterior, consulte **Descripción**.

Paso 2 Haga clic en la pestaña **Resource Distribution Policies**.

Paso 3 En el campo **Resource Pools**, seleccione un grupo de recursos especificado.

Paso 4 Busque la cola especificada en la tabla **Resource Allocation** y haga clic en **Clear** en la columna **Operation**

En el cuadro de diálogo **Clear Queue Configuration**, haga clic en **OK** para borrar la configuración de cola en el grupo de recursos actual.

NOTA

Si no se configura ninguna política de capacidad de recursos para una cola, la función de borrado no está disponible para la cola de forma predeterminada.

----Fin

3.11 Acciones de arranque

3.11.1 Introducción a las acciones de arranque

Puede ejecutar acciones de arranque para instalar software adicional de terceros, modificar el entorno de ejecución del clúster y realizar otras personalizaciones. Las acciones de arranque pueden ejecutar scripts en nodos especificados antes o después del primer inicio de los componentes del clúster. Solo puede ejecutar manualmente el script de instalación de componentes de terceros en el nodo para instalar un componente de clúster en ejecución.

Si elige ejecutar acciones de arranque al escalar un clúster, las acciones de arranque se ejecutarán en los nodos recién agregados de la misma manera. Si el escalado automático está habilitado en un clúster, puede agregar un script de automatización además de configurar un plan de recursos. A continuación, el script de automatización ejecuta el script correspondiente en los nodos que se escalan o se ejecutan para implementar operaciones personalizadas.

Para versiones anteriores a MRS 3.*x*, los scripts se ejecutan como usuario **root**. Puede ejecutar el comando **su - XXX** en un script para cambiar a otro usuario.

Para MRS 3.*x* o posterior, los scripts se ejecutan como usuario **omm** de forma predeterminada. Puede ejecutar el comando **su - XXX** en un script para cambiar a otro usuario.

NOTA

Versiones anteriores a MRS 3.*x*: Los scripts de acción de arranque deben ejecutarse como usuario **root**. De lo contrario, es posible que el clúster no esté disponible.

MRS 3.*x* o posterior: Los scripts de acción de arranque deben ejecutarse como usuario **omm**. De lo contrario, es posible que el clúster no esté disponible.

MRS determina el resultado basado en el código devuelto después de la ejecución del script de acción de arranque. Si el código de retorno es de **0**, el script se ejecuta correctamente. Si el código devuelto no es **0**, la ejecución falla. Si un script de acción de arranque no se ejecuta en un nodo, el script de arranque correspondiente no se ejecutará. En este caso, puede configurar **Action upon Failure** para que elija si desea continuar con la ejecución de los scripts posteriores. Ejemplo 1: Si establece **Action upon Failure** en **Continue** para todos los scripts durante la creación del clúster, todos los scripts se ejecutarán independientemente de si se ejecutan correctamente, y el proceso de inicio se completará. Ejemplo 2: Si un script no se ejecuta y **Action upon Failure** se establece en **Stop**, los scripts posteriores no se ejecutarán y la creación de clúster o el escalado horizontal fallarán.

Puede agregar un máximo de 18 acciones de arranque, que se ejecutarán antes o después de iniciar el componente de clúster en el orden especificado. Las acciones de arranque realizadas

antes o después del inicio del componente deben completarse en un plazo de 60 minutos. De lo contrario, se producirá un error en la creación o la escalabilidad horizontal del clúster.

3.11.2 Preparación del script de acción de arranque

Actualmente, las acciones de arranque solo soportan scripts de Linux shell. Los archivos de secuencias de comandos deben terminar con **.sh**.

Carga de paquetes y archivos de instalación en un sistema de archivos de OBS

Antes de compilar un script, debe cargar todos los paquetes de instalación necesarios, paquetes de configuración y archivos relevantes en el sistema de archivos de OBS en la misma región. Debido a que las redes de diferentes regiones están aisladas entre sí, las máquinas virtuales de MRS no pueden descargar archivos de OBS de otras regiones.

Compilación de un script para descargar archivos desde el sistema de archivos de OBS

Puede especificar el archivo que se descargará de OBS en el script. Si carga archivos a un sistema de archivos privado, debe ejecutar el comando **hadoop fs** para descargar los archivos. El siguiente ejemplo muestra que el archivo **obs://yourbucket/myfile.tar.gz** se descargará en el host local y se descomprimirá en el directorio **/your-dir**.

```
#!/bin/bash
source /opt/Bigdata/client/bigdata_env;hadoop fs -D fs.obs.endpoint=<obs-
endpoint> -D fs.obs.access.key=<your-ak> -D fs.obs.secret.key=<your-sk> -
copyToLocal obs://yourbucket/myfile.tar.gz ./
mkdir -p /<your-dir>
tar -zxvf myfile.tar.gz -C /<your-dir>
```

NOTA

- El cliente de Hadoop se ha preinstalado en el nodo de MRS. Puede ejecutar el comando **hadoop fs** para descargar o cargar datos desde o hacia OBS.
- Obtenga el punto de conexión de obs de cada región.
- **Scripts de muestra** muestra que los paquetes de instalación se han cargado en el sistema de archivos de OBS legible al público. Por lo tanto, puede ejecutar el comando **curl** en el script de ejemplo para descargar los paquetes de instalación.

Subir el script al sistema de archivos de OBS

Después de la compilación de script, cargue la secuencia de comandos en el sistema de archivos de OBS en la misma región. En el momento de especificar, cada nodo del clúster descarga el script de OBS y ejecuta el script como usuario **root**.

3.11.3 Ver registros de ejecución

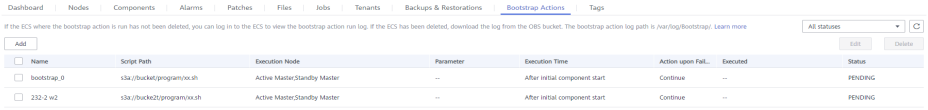
Puede ver el resultado de la ejecución de la operación de arranque en la página **Bootstrap Action**.

Consulta del resultado de la ejecución

1. Inicie sesión en la consola de MRS.
2. En el panel de navegación izquierdo, elija **Clusters** >**Active Clusters**. Haga clic en el clúster que desee consultar.

Se muestra la página de detalles del clúster.

3. En la página de detalles del clúster, haga clic en la pestaña **Bootstrap Action**. Se muestra información acerca de las acciones de arranque agregadas durante la creación del clúster.



NOTA

- Seleccione **Before initial component start** o **After initial component start** en la esquina superior derecha para consultar información sobre las acciones de arranque relacionadas.
- El último resultado de la ejecución se muestra aquí. Para un clúster recién creado, se enumeran los registros de las acciones de arranque ejecutadas durante la creación del clúster. Si se expande un clúster, se enumeran los registros de las acciones de arranque ejecutadas en los nodos recién agregados.

Consulta de registros de ejecución

Si desea ver los registros de ejecución de una acción de arranque, establezca **Action upon Failure** en **Continue** al agregar la acción de arranque. Y luego, inicie sesión en cada nodo para ver los registros de ejecución en el directorio **/var/log/Bootstrap**. Si agrega acciones de arranque antes y después del inicio del componente, puede distinguir los registros de acciones de arranque de las dos fases basándose en las marcas de tiempo.

Se recomienda imprimir los registros en detalle en el script para que pueda ver el resultado detallado de la ejecución. MRS redirige la salida estándar y la salida de error del script al directorio de registro de la acción de arranque.

3.11.4 Adición de una acción de arranque

Añade una acción de arranque.

Procedimiento

Paso 1 Inicie sesión en la consola de gestión de MRS.

Paso 2 Seleccione **Clusters** > **Active Clusters** y haga clic en el nombre del clúster que desee.

Paso 3 En la página que se muestra, haga clic en la pestaña **Bootstrap Actions**.

Paso 4 Haga clic en **Add** y defina los parámetros según se le solicite.

Figura 3-94 Agregar acción de arranque

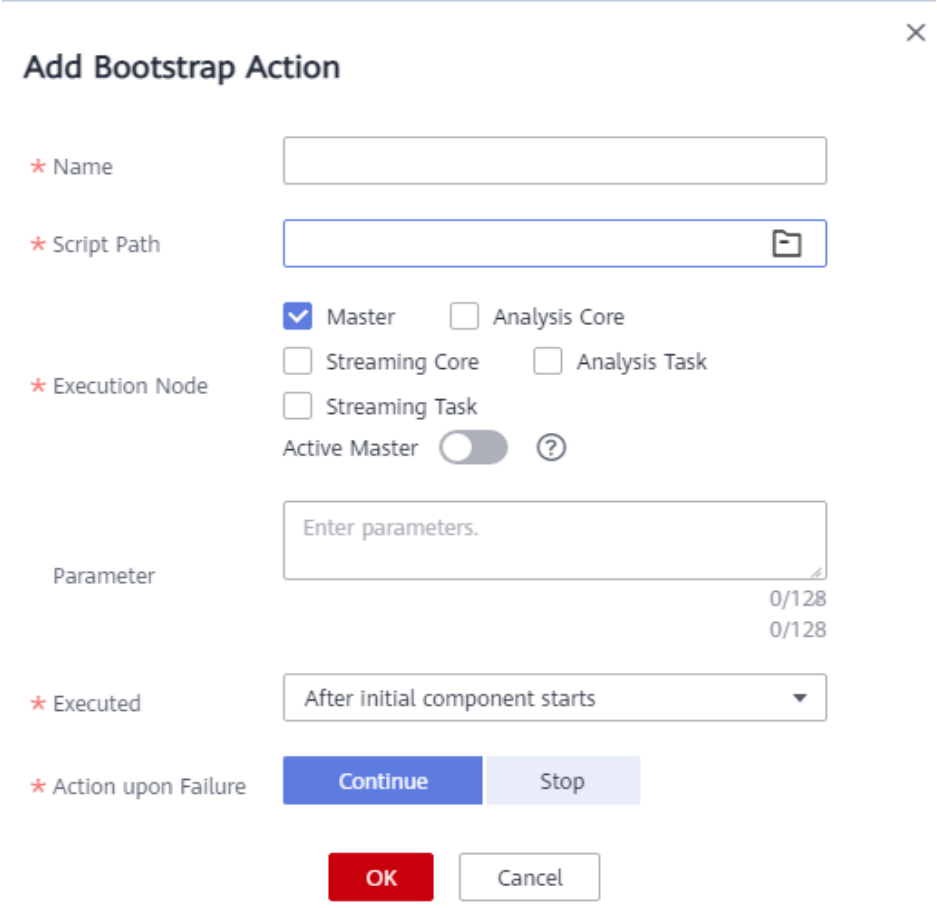


Tabla 3-85 Parámetros

Parámetro	Descripción
Name	Nombre de una secuencia de comandos de acción de arranque El valor solo puede contener dígitos, letras, espacios, guiones (-) y guiones bajos (_) y no debe comenzar con un espacio. El valor puede contener de 1 a 64 caracteres. **NOTA** Un nombre debe ser único en el mismo clúster. Puede establecer el mismo nombre para diferentes clústeres.
Script Path	Ruta del script. El valor puede ser una ruta de sistema de archivos OBS o una ruta de VM local. ● Una ruta de sistema de archivos de OBS debe comenzar por **s3a://** y terminar por **.sh**, por ejemplo, **s3a://mrs-samples/***xxx***.sh**. ● Una ruta de VM local debe comenzar con una barra diagonal (/) y terminar con **.sh**. **NOTA** Una ruta de acceso debe ser única en el mismo clúster, pero puede ser la misma para diferentes clústeres.

Parámetro	Descripción
Parameter	Parámetros de script de acción de arranque
Execution Node	Seleccione un tipo del nodo donde se ejecuta el script de acción de arranque.
Executed	Seleccione la hora a la que se ejecuta el script de acción de arranque. ● Antes del inicio del componente inicial ● Después del inicio del componente inicial **NOTA** Solo puede ejecutar manualmente el script de instalación de componentes de terceros en el nodo para instalar un componente de clúster en ejecución.
Action upon Failure	Si se deben continuar ejecutando secuencias de comandos posteriores y crear un clúster después de que la secuencia de comandos no se ejecute. **NOTA** Se recomienda establecer este parámetro en **Continue** en la fase de depuración para que el clúster pueda seguir siendo instalado e iniciado sin importar si la acción de arranque es correcta.
Run as root	Si se debe escalar el permiso al usuario **root** Si la acción de arranque requiere operaciones de usuario root, habilite esta función, o la acción de arranque puede no ejecutarse. **NOTA** Esta operación se aplica a los clústeres MRS 3.1.5 o posteriores.

Paso 5 Haga clic en **OK** para guardar la configuración.

Paso 6 Haga clic en **Yes**.

----Fin

3.11.5 Modificación de una acción de arranque

Escenario

Modificar una acción de arranque existente en un clúster MRS.

Procedimiento

Paso 1 Inicie sesión en la consola de gestión de MRS.

Paso 2 Seleccione **Clusters** > **Active Clusters** y haga clic en el nombre del clúster que desee.

Paso 3 En la página que se muestra, haga clic en la pestaña **Bootstrap Actions**.

Paso 4 En la lista, seleccione el elemento que se va a modificar y haga clic en **Edit**.

Paso 5 Modifique los parámetros según sea necesario.

Paso 6 Haga clic en **OK** para guardar la modificación.

Paso 7 Haga clic en **Yes**.

----Fin

3.11.6 Eliminación de una acción de arranque

Escenario

Eliminar una acción de arranque en un clúster MRS.

Procedimiento

Paso 1 Inicie sesión en la consola de gestión de MRS.

Paso 2 Seleccione **Clusters** > **Active Clusters** y haga clic en el nombre del clúster que desee.

Paso 3 En la página que se muestra, haga clic en la pestaña **Bootstrap Actions**.

Paso 4 En la lista, seleccione el elemento que desea eliminar y haga clic en **Delete**.

Paso 5 Haga clic en **OK**.

----Fin

3.11.7 Scripts de muestra

Zeppelin

Zeppelin es un cuaderno basado en la web que admite análisis de datos interactivos. Para obtener más información, visite el sitio web oficial de Zeppelin en **http://zeppelin.apache.org/**.

Este script de ejemplo se utiliza para instalar automáticamente Zeppelin. Seleccione la ruta de script correspondiente en función de la región en la que se va a crear el clúster. Introduzca la ruta del script en **Script Path** en la página **Bootstrap Action** cuando agregue una acción de arranque durante la creación del clúster. No es necesario introducir parámetros para este script. Basado en el hábito de uso de Zeppelin, solo necesita ejecutar el script en el nodo de Master activo.

- Ruta del script que debe introducir al agregar la acción de arranque:
- Ruta para descargar el script de ejemplo:
  - **CN-Hong Kong**: **https://mrs-samples-bootstrap-ap-southeast-1.obs.ap-southeast-1.myhuaweicloud.com/zeppelin/zeppelin_install.sh**
  - **AP-Bangkok**: **https://mrs-samples-bootstrap-ap-southeast-2.obs.ap-southeast-2.myhuaweicloud.com/zeppelin/zeppelin_install.sh**

Una vez completada la acción de arranque, utilice cualquiera de los siguientes métodos para verificar que Zeppelin esté instalado correctamente.

Método 1: Inicie sesión en el nodo de Master activo como usuario **root** y ejecute **/home/apache/zeppelin-0.7.3-bin-all/bin/zeppelin-daemon.sh status**. Si aparece el mensaje que indica "Zeppelin is running [OK]", la instalación se realiza correctamente.

Método 2: Inicie un ECS de Windows en la misma VPC. Puerto de acceso 7510 del nodo de Master activo en el clúster. Si se muestra la página Zeppelin, la instalación se realiza correctamente.

Presto

Presto es un motor de consultas SQL distribuido de código abierto, que es aplicable al análisis y consultas interactivas. Para obtener más información, visite el sitio web oficial en **http://prestodb.io/**.

El script de ejemplo se puede usar para instalar Presto automáticamente. La ruta del script es la siguiente:

- Ruta del script que debe introducir al agregar la acción de arranque:
  - **CN-Hong Kong**: s3a://mrs-samples-bootstrap-ap-southeast-1/presto/presto_install.sh
  - **AP-Bangkok**: s3a://mrs-samples-bootstrap-ap-southeast-2/presto/presto_install.sh
- Ruta para descargar el script de ejemplo:
  - **CN-Hong Kong**: **https://mrs-samples-bootstrap-ap-southeast-1.obs.ap-southeast-1.myhuaweicloud.com/presto/presto_install.sh**
  - **AP-Bangkok**: **https://mrs-samples-bootstrap-ap-southeast-2.obs.ap-southeast-2.myhuaweicloud.com/presto/presto_install.sh**

Basado en el hábito de uso de Presto, se recomienda instalar **dualroles** en los nodos Master activos y **worker** en los nodos de Core. Se recomienda agregar el script de operación de arranque y configurar los parámetros de la siguiente manera:

Tabla 3-86 Parámetros de script de acción de arranque

Script 1	Nombre: install dualroles Ruta de script: Seleccione la ruta del script **presto-install.sh** en función de la región. Nodo de ejecución: Active Master Parámetros: dualroles Tiempo de ejecución: Después del inicio del componente Acción fallida: Continuar
Script 2	Nombre: install worker Ruta de script: Seleccione la ruta del script **presto-install.sh** en función de la región. Nodo de ejecución: Core Parámetros: worker Tiempo de ejecución: Después del inicio del componente Acción fallida: Continuar

Una vez completada la acción de arranque, puede iniciar un ECS de Windows en la misma VPC del clúster y el puerto de acceso 7520 del nodo de Master activo para ver la página web de Presto.

También puede iniciar sesión en el nodo de Master activo para probar Presto y ejecutar los siguientes comandos como usuario **root**:

Comando para cargar la variable de entorno:

#source /opt/Bigdata/client/bigdata_env

Comando para ver el estado del proceso:

#/home/apache/presto/presto-server-0.201/bin/launcher status

Comando para conectarse a Presto y realizar la operación

#/home/apache/presto/presto-server-0.201/bin/presto --server localhost:7520 --catalog tpch --schema sf100

presto:sf100> select * from nation;

presto:sf100> select count(*) from customer

Superset

Superset es una herramienta de BI moderna y a nivel empresarial basada en web. Para obtener más información, visite el sitio web oficial de Superset en **https://superset.incubator.apache.org/**.

Este script de ejemplo se utiliza para instalar automáticamente Superset. Seleccione la ruta de script correspondiente en función de la región en la que se va a crear el clúster. Introduzca la ruta del script de **Script Path** en la página **Bootstrap Action** al agregar una acción de arranque durante la creación del clúster. No es necesario introducir parámetros para este script. Basado en el hábito de uso de Superset, solo necesita ejecutar el script en el nodo de Master activo.

- Ruta del script que debe introducir al agregar la acción de arranque:
  - **CN-Hong Kong**: s3a://mrs-samples-bootstrap-ap-southeast-1/superset/superset_install.sh
  - **AP-Bangkok**: s3a://mrs-samples-bootstrap-ap-southeast-2/superset/superset_install.sh
- Ruta para descargar el script de ejemplo:
  - **CN-Hong Kong**: **https://mrs-samples-bootstrap-ap-southeast-1.obs.ap-southeast-1.myhuaweicloud.com/superset/superset_install.sh**
  - **AP-Bangkok**: **https://mrs-samples-bootstrap-ap-southeast-2.obs.ap-southeast-2.myhuaweicloud.com/superset/superset_install.sh**

Una vez completada la acción de arranque, utilice cualquiera de los métodos siguientes para comprobar que Superset está instalado correctamente.

Método 1: Inicie sesión remotamente en el nodo de Master activo como usuario **root** y ejecute el comando **lsof -i:38088**. Si el resultado del comando contiene **LISTEN**, la instalación se realiza correctamente.

Método 2: Inicie un ECS de Windows en la misma VPC. Puerto de acceso 38088 del nodo de Master activo en el clúster. Si se muestra la página Superset, la instalación se realiza correctamente.

OpenTSDB

OpenTSDB es una plataforma de recopilación y visualización de información de monitorización en tiempo real basada en HBase. Admite la recopilación de métricas de segundo nivel, utiliza HBase para el almacenamiento permanente, la planificación de la capacidad y el fácil acceso al sistema de monitoreo existente. OpenTSDB puede obtener métricas de un gran número de dispositivos y almacenar e indexar métricas, así como utilizar las métricas para proporcionar servicios, lo que facilita la comprensión de los datos, por ejemplo, mostrando datos en la web y en gráficos. Para obtener más información, visite el sitio web oficial de OpenTSDB en **http://opentsdb.net/**.

Este script de ejemplo se utiliza para instalar automáticamente OpenTSDB. Seleccione la ruta de script correspondiente en función de la región en la que se va a crear el clúster. Introduzca la ruta del script de **Script Path** en la página **Bootstrap Action** al agregar una acción de arranque durante la creación del clúster. No es necesario introducir parámetros para este script. Basado en el hábito de uso de OpenTSDB, solo necesita ejecutar el script en el nodo de Master activo.

OpenTSDB depende del servicio HBase. Por lo tanto, debe seleccionar HBase al crear un clúster y configurar el **Execution Time** de la acción de arranque en **After component start**.

- Ruta para descargar el script de ejemplo:
  - **CN-Hong Kong**: **https://mrs-samples-bootstrap-ap-southeast-1.obs.ap-southeast-1.myhuaweicloud.com/opentsdb/opentsdb_install.sh**
  - **AP-Bangkok**: **https://mrs-samples-bootstrap-ap-southeast-2.obs.ap-southeast-2.myhuaweicloud.com/opentsdb/opentsdb_install.sh**

Una vez completada la acción de arranque, utilice cualquiera de los métodos siguientes para verificar que OpenTSDB esté instalado correctamente.

Método 1: Inicie sesión remotamente en el nodo de Master activo como usuario **root** y ejecute el comando **lsof -i:4242**. Si el resultado del comando contiene **LISTEN**, la instalación se realiza correctamente.

Método 2: Inicie un ECS de Windows en la misma VPC. Puerto de acceso 4242 del nodo Master activo en el clúster. Si se muestra la página OpenTSDB, la instalación se realiza correctamente.

obsutil

obsutil es una herramienta de línea de comandos para acceder al Object Storage Service (OBS). Puede utilizar esta herramienta para realizar configuraciones comunes en OBS, como la creación de sistemas de archivos, la carga y descarga de archivos/carpetas y la eliminación de archivos/carpetas. Si está familiarizado con la interfaz de línea de comandos (CLI), use obsutil para el procesamiento por lotes y tareas automatizadas. Para obtener más información, consulte **Introducción a obsutil**.

Este script de muestra se utiliza para instalar automáticamente obsutil. Seleccione la ruta de script correspondiente en función de la región en la que se va a crear el clúster. Introduzca la ruta del script de **Script Path** en la página **Bootstrap Action** al agregar una acción de arranque durante la creación del clúster. No es necesario introducir parámetros para este script. En **Execution Time**, seleccione **After component start**. En **Action upon Failure**, seleccione **Continue**.

- Ruta del script que debe introducir al agregar la acción de arranque:

  - **CN-Hong Kong**: s3a://mrs-samples-bootstrap-ap-southeast-1.obs.ap-southeast-1.myhuaweicloud.com/obsutil/obsutil_install.sh
  - **AP-Bangkok**: s3a://mrs-samples-bootstrap-ap-southeast-2.obs.ap-southeast-2.myhuaweicloud.com/obsutil/obsutil_install.sh
- Ruta para descargar el script de ejemplo:
  - **CN-Hong Kong**: **https://mrs-samples-bootstrap-ap-southeast-1.obs.ap-southeast-1.myhuaweicloud.com/obsutil/obsutil_install.sh**
  - **AP-Bangkok**: **https://mrs-samples-bootstrap-ap-southeast-2.obs.ap-southeast-2.myhuaweicloud.com/obsutil/obsutil_install.sh**

Una vez completada la ejecución de la acción de arranque, realice las siguientes operaciones para configurar y verificar la conectividad de obsutil:

1. Métodos de configuración

   Puede ejecutar los siguientes comandos para inicializar obsutil:

   ```
   ./opt/obsutil_linux_amd64_5.1.7.2/obsutil config-i=ak -k=sk -e=endpoint
   ```

2. Comprobación de la conectividad

   Una vez completada la configuración, puede comprobar si es correcta ejecutando el siguiente comando:

   ```
   ./obsutil ls -s
   ```

   Compruebe el resultado de la configuración basado en la salida del comando.

   - Si la salida del comando contiene **"Bucket number is:**", la configuración es correcta.
   - Si la salida del comando contiene **"Http status [403]**", las claves de acceso están configuradas incorrectamente.
   - Si la salida del comando contiene **"A connection attempt failed"**, no se puede acceder a OBS. En este caso, compruebe la condición de la red.

4 Uso de un cliente de MRS

4.1 Instalación de un cliente

4.1.1 Instalación de un cliente (MRS 3.*x* o posterior)

Escenario

Instalar clientes de todos los servicios (excepto Flume) en un clúster MRS. Para obtener detalles sobre cómo instalar el cliente Flume, consulte **Instalación de un cliente Flume**.

Puede instalar los clientes en un nodo dentro o fuera del clúster.

Después de modificar la configuración del servidor de un componente de clúster, vuelva a instalar el cliente del componente para asegurarse de que tanto el servidor como el cliente ejecuten la misma versión para proporcionar los servicios correctamente.

Prerrequisitos

- Si el nodo en el que se va a instalar el cliente está fuera del clúster, el nodo debe poder comunicarse con los nodos del clúster. De lo contrario, la instalación del cliente fallará.
- El nodo donde se va a instalar el cliente debe tener el servicio NTP habilitado y sincronizado con el servidor. De lo contrario, la instalación del cliente fallará.
- Instalar el cliente como usuario **root** o cualquier usuario del sistema operativo. El usuario debe tener el permiso de operación en el directorio de almacenamiento de archivos del cliente y el directorio de instalación. El permiso para los dos directorios es **755**.

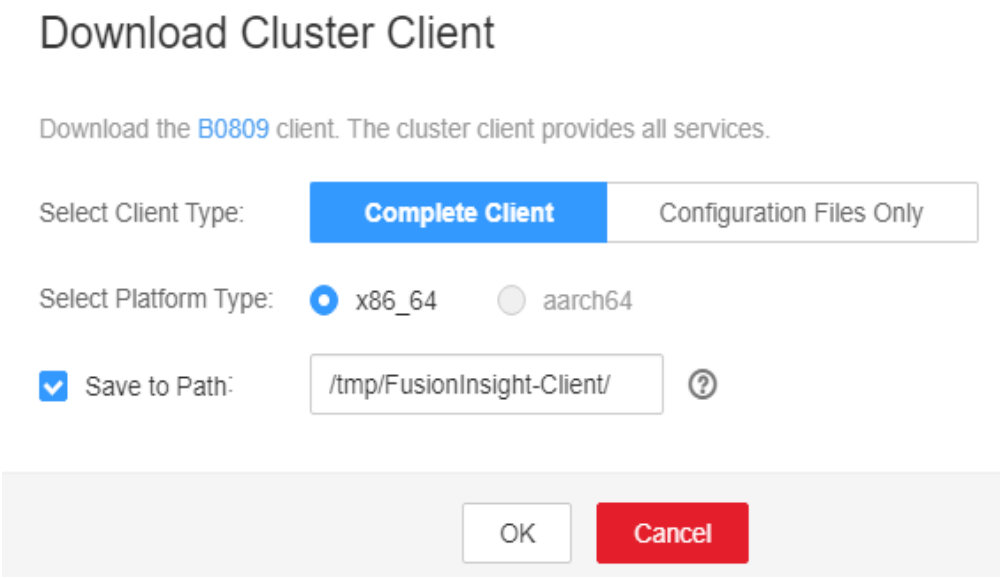
  En esta sección se utiliza el usuario del sistema operativo **user_client** como ejemplo para describir cómo instalar el cliente en el directorio **/opt/hadoopclient**.
- Cuando instala el cliente como un usuario distinto de **omm** y **root** y el directorio **/var/tmp/patch** ya existe, ha cambiado el permiso para el directorio a **777** y ha cambiado el permiso para los registros en el directorio a **666**.

Instalación de un cliente en un nodo dentro de un clúster

Paso 1 Obtenga el paquete de software del cliente.

Inicie sesión en FusionInsight Manager consultando a **Acceder a FusionInsight Manager (MRS 3.x o posterior)**. En la página **Cluster** > **Dashboard**, haga clic en el signo más (...) y seleccione **Download Client**. En el cuadro de diálogo **Download Cluster Client** que se muestra, configure los parámetros y haga clic en **OK**.

Figura 4-1 Descargar un cliente



NOTA

El paquete de software de cliente descargado de la página de inicio del FusionInsight Manager contiene los clientes de todos los servicios (excluido Flume) del clúster. Para descargar el cliente de un solo servicio, elija **Cluster** > **Services** > *Service name*, haga clic en **More** y seleccione **Download Client**.

Tabla 4-1 Parámetros de descarga del cliente

Parámetro	Descripción	Valor de ejemplo
Select Client Type	• **Complete Client**: contiene el paquete de software cliente completo y los archivos de configuración, que se aplican a los escenarios de tareas que no son de desarrollo. • **Configuration Files Only** descarga solo los archivos de configuración del cliente en el escenario donde el administrador modifica la configuración del servidor en FusionInsight Manager después de que el cliente completo se descarga e instala en una tarea de desarrollo de aplicaciones, y los desarrolladores necesitan actualizar los archivos de configuración del cliente.	Complete Client

Parámetro	Descripción	Valor de ejemplo
Select Platform Type	**El tipo de cliente debe coincidir con la arquitectura del nodo en el que se va a instalar el cliente. De lo contrario, la instalación falla. Para los clusters de la versión LTS, solo puede descargarse el paquete de software cliente cuyo tipo coincida con el de FusionInsight Manager.** ● **x86_64**: indica el paquete de software cliente que se puede desplegar en una plataforma x86. ● **aarch64**: indica el paquete de software cliente que se puede desplegar en un servidor de TaiShan.	x86_64
Save to Path	La ruta para almacenar el paquete de software cliente en el nodo OMS activo ● Seleccione **Save to Path**: Personalice la ruta de acceso para almacenar el paquete de software cliente en el nodo OMS activo. El usuario **omm** debe tener los permisos de lectura, escritura y ejecución en la ruta de acceso. Si no se cambia la ruta de acceso, el archivo cliente generado se guarda en el directorio **/tmp/FusionInsight-Client** del nodo OMS activo del clúster de forma predeterminada. ● No seleccionar **Save to Path**: El archivo de cliente generado se descarga automáticamente y se guarda en el host local. Antes de instalar el cliente, debe cargar el archivo en un directorio especificado en el nodo de destino.	Seleccione **Save to Path**

Paso 2 Copie el paquete de software cliente en un directorio especificado en el nodo donde se va a instalar el cliente.

De forma predeterminada, el paquete de software cliente se almacena en el nodo OMS activo del clúster. Para instalar el cliente en otros nodos del clúster, inicie sesión en el nodo OMS activo como usuario **omm** y ejecute el siguiente comando para copiar el paquete de software en el nodo especificado. De lo contrario, omita este paso.

Por ejemplo, copie el paquete de software en el directorio **/tmp/clienttemp**.

scp -p */tmp/FusionInsight-Client/***FusionInsight_Cluster_1_Services_Client.tar** *IP address of the node where the client is to be installed:/tmp/clienttemp*

Paso 3 Inicie sesión en el nodo de destino como usuario, por ejemplo, **user_client**.

NOTA

Puede instalar el cliente como usuario **root** o cualquier otro usuario del sistema operativo. El usuario debe tener el permiso de operación en el directorio de almacenamiento de archivos del cliente y el directorio de instalación. El permiso para los dos directorios es **755**.

Paso 4 Descomprima el paquete de software cliente.

Vaya al directorio donde está almacenado el paquete, por ejemplo, **/tmp/clienttemp**.

cd /tmp/clienttemp

Ejecute los siguientes comandos para descomprimir el paquete:

tar -xvf FusionInsight_Cluster_1_Services_Client.tar

tar -xvf FusionInsight_Cluster_1_Services_ClientConfig.tar

Paso 5 Vaya al directorio del paquete y ejecute el siguiente comando para instalar el cliente en un directorio especificado:

cd FusionInsight_Cluster_1_Services_ClientConfig

./install.sh *Client installation directory*

Por ejemplo, ejecute el comando **./install.sh /opt/hadoopclient** para instalar el cliente y espere hasta que se complete la instalación.

```
...
The component client is installed successfully
```

NOTA

- **Es posible que el directorio de instalación del cliente no exista. Si es así, se crea uno nuevo automáticamente. No obstante, si existe, debe estar vacío. El directorio no puede contener espacios.**
- Debe eliminar manualmente el directorio de instalación del cliente al desinstalar un cliente.
- Para asegurarse de que el cliente instalado solo puede ser utilizado por el usuario de la instalación, agregue el parámetro **-o** durante la instalación. Por ejemplo, ejecute el comando **./install.sh /opt/hadoopclient -o** para instalar el cliente.
- Si se instala un cliente HBase, se recomienda que el directorio de instalación del cliente contenga solo letras mayúsculas y minúsculas, números y caracteres especiales (_-?.@+=) debido a la limitación de la sintaxis Ruby utilizada por HBase.

Paso 6 Utilice el cliente haciendo referencia a "Usar el cliente de cada componente".

----Fin

Instalación de un cliente en un nodo fuera de un clúster

Paso 1 Cree un ECS que cumpla con los siguientes requisitos:

- Se ha preparado un ECS de Linux. Para obtener más información sobre el sistema operativo compatible con ECS, consulte **Tabla 4-2**.

Tabla 4-2 Lista de referencias

Arquitectura de CPU	Sistema operativo	Versión admitida
x86 computing	EulerOS	EulerOS 2.5
	SUSE	SUSE Linux Enterprise Server 12 SP4 (SUSE 12.4)
	Red Hat	Red Hat-7.5-x86_64 (Red Hat 7.5)
	CentOS	CentOS 7.6

Arquitectura de CPU	Sistema operativo	Versión admitida
Kunpeng computing (Arm)	EulerOS	EulerOS 2.8
	CentOS	CentOS 7.6

Además, se asigna suficiente espacio en disco para el ECS, por ejemplo, 40 GB.

- El ECS y el clúster MRS están en la misma VPC.
- El grupo de seguridad del ECS debe ser el mismo que el del nodo master en el clúster MRS.
- El servicio NTP se ha instalado en el sistema operativo ECS y se está ejecutando correctamente.

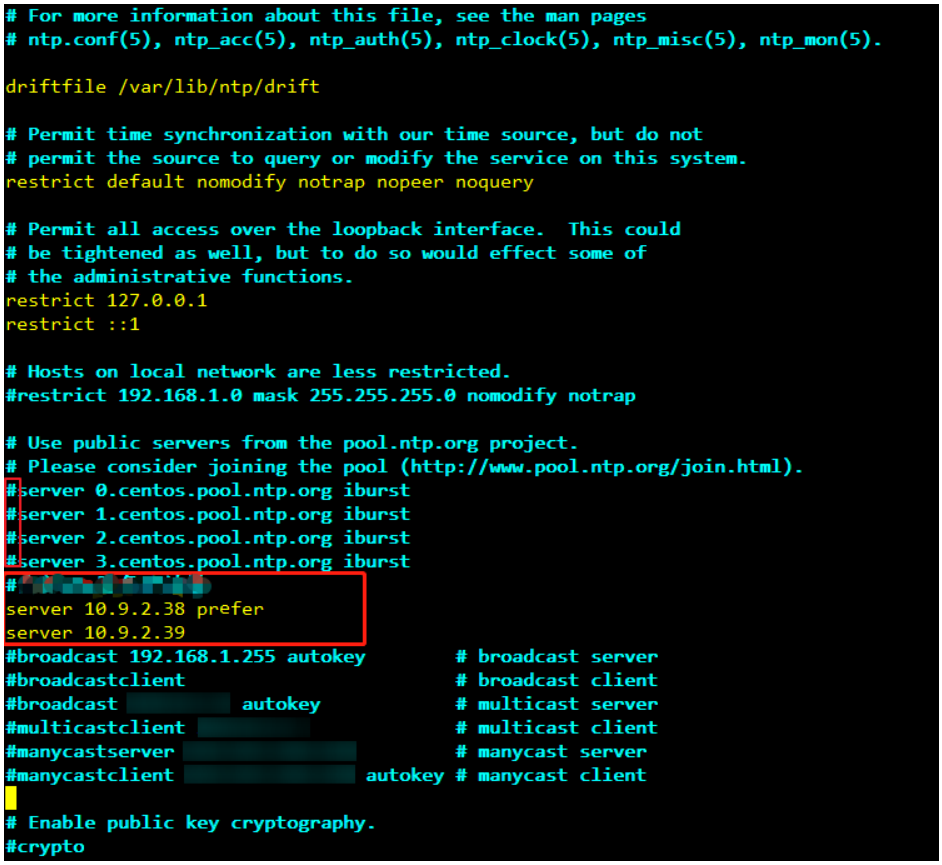
  Si el servicio NTP no está instalado, ejecute el comando **yum install ntp -y** para instalarlo cuando el origen **yum** esté configurado.
- Un usuario puede iniciar sesión en el ECS de Linux usando la contraseña (en modo SSH).
- Todos los puertos en la dirección de entrada del grupo de seguridad del clúster MRS están abiertos al nodo cliente. Para obtener más información, consulte **Adición de una regla de grupo de seguridad**.

Paso 2 Realice la sincronización de tiempo de NTP para sincronizar el tiempo de los nodos fuera del clúster con el tiempo del clúster MRS.

1. Ejecute el comando **vi /etc/ntp.conf** para editar el archivo de configuración del cliente NTP, agregue las direcciones IP del nodo master en el clúster MRS y comente la dirección IP de otros servidores.

```
server master1_ip prefer
server master2_ip
```


Figura 4-2 Adición de las direcciones IP del nodo de master



2. Ejecute el comando **service ntpd stop** para detener el servicio NTP.
3. Ejecute el siguiente comando para sincronizar manualmente la hora:

   /usr/sbin/ntpdate *192.168.10.8*

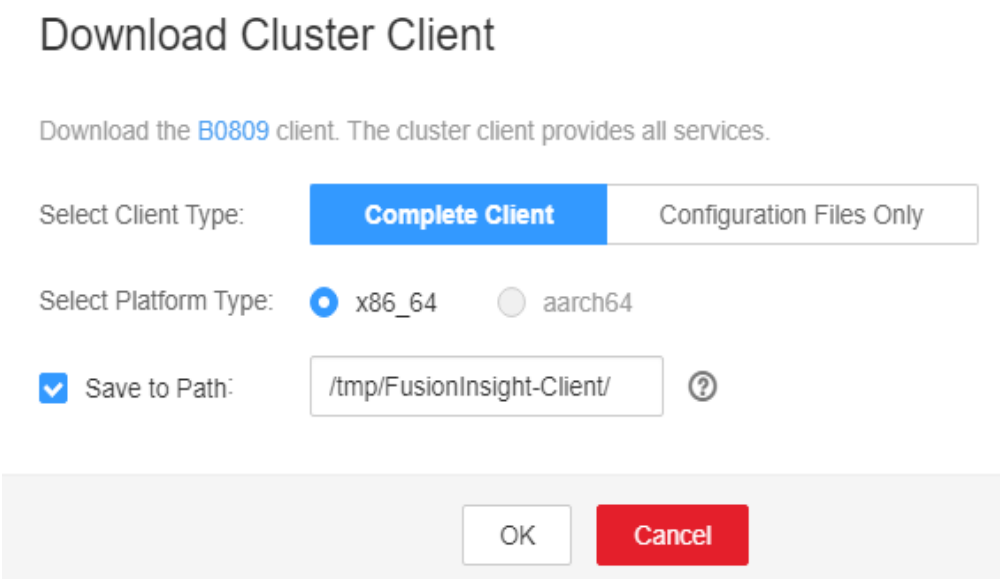
   NOTA

   192.168.10.8 indica la dirección IP del nodo de Master activo.
4. Ejecute el comando **service ntpd start** o **systemctl restart ntpd** para iniciar el servicio NTP.
5. Ejecute el comando **ntpstat** para comprobar el resultado de la sincronización de tiempo.

Paso 3 Obtenga el paquete de software del cliente.

Inicie sesión en FusionInsight Manager consultando a **Acceder a FusionInsight Manager (MRS 3.x o posterior)**. En la página **Cluster** > **Dashboard**, haga clic en el signo más (...) y seleccione **Download Client**. En el cuadro de diálogo **Download Cluster Client** que se muestra, configure los parámetros y haga clic en **OK**.

Figura 4-3 Descargar un cliente



NOTA

El paquete de software de cliente descargado de la página de inicio del FusionInsight Manager contiene los clientes de todos los servicios (excluido Flume) del clúster. Para descargar el cliente de un solo servicio, elija **Cluster** > **Services** > *Service name*, haga clic en **More** y seleccione **Download Client**.

Tabla 4-3 Parámetros de descarga del cliente

Parámetro	Descripción	Valor de ejemplo
Select Client Type	● **Complete Client**: contiene el paquete de software cliente completo y los archivos de configuración, que se aplican a los escenarios de tareas que no son de desarrollo. ● **Configuration Files Only** descarga solo los archivos de configuración del cliente en el escenario donde el administrador modifica la configuración del servidor en FusionInsight Manager después de que el cliente completo se descarga e instala en una tarea de desarrollo de aplicaciones, y los desarrolladores necesitan actualizar los archivos de configuración del cliente.	Complete Client

Parámetro	Descripción	Valor de ejemplo
Select Platform Type	**El tipo de cliente debe coincidir con la arquitectura del nodo en el que se va a instalar el cliente. De lo contrario, la instalación falla. Para los clusters de la versión LTS, solo puede descargarse el paquete de software cliente cuyo tipo coincida con el de FusionInsight Manager.** ● **x86_64**: indica el paquete de software cliente que se puede desplegar en una plataforma x86. ● **aarch64**: indica el paquete de software cliente que se puede desplegar en un servidor de TaiShan.	x86_64
Save to Path	La ruta para almacenar el paquete de software cliente en el nodo OMS activo ● Seleccione **Save to Path**: Personalice la ruta de acceso para almacenar el paquete de software cliente en el nodo OMS activo. El usuario **omm** debe tener los permisos de lectura, escritura y ejecución en la ruta de acceso. Si no se cambia la ruta de acceso, el archivo cliente generado se guarda en el directorio **/tmp/FusionInsight-Client** del nodo OMS activo del clúster de forma predeterminada. ● No seleccionar **Save to Path**: El archivo de cliente generado se descarga automáticamente y se guarda en el host local. Antes de instalar el cliente, debe cargar el archivo en un directorio especificado en el nodo de destino.	Seleccione **Save to Path**

Paso 4 Copie el paquete de software cliente en un directorio especificado en el nodo donde se va a instalar el cliente.

El paquete de software cliente generado se almacena en el nodo OMS activo del clúster de forma predeterminada. Debe iniciar sesión en el nodo OMS activo como usuario **omm** y ejecutar el siguiente comando para copiar el paquete de software en un ECS especificado:

Por ejemplo, copie el paquete de software en el directorio **/tmp/clienttemp**.

scp -p */tmp/FusionInsight-Client/***FusionInsight_Cluster_1_Services_Client.tar** *IP address of the node where the client is to be installed:/tmp/clienttemp*

Paso 5 Inicie sesión en el nodo de destino como usuario, por ejemplo, **user_client**.

NOTA

Puede instalar el cliente como usuario **root** o cualquier otro usuario del sistema operativo. El usuario debe tener el permiso de operación en el directorio de almacenamiento de archivos del cliente y el directorio de instalación. El permiso para los dos directorios es **755**.

Paso 6 Descomprima el paquete de software cliente.

Vaya al directorio donde está almacenado el paquete, por ejemplo, **/tmp/clienttemp**.

cd /tmp/clienttemp

Ejecute los siguientes comandos para descomprimir el paquete:

tar -xvf FusionInsight_Cluster_1_Services_Client.tar

tar -xvf FusionInsight_Cluster_1_Services_ClientConfig.tar

Paso 7 Compruebe la conexión de red del cliente.

1. Asegúrese de que el host donde está instalado el cliente puede comunicarse con los hosts listados en el archivo **hosts** almacenado en el directorio que contiene el paquete descomprimido, por ejemplo, **/tmp/FusionInsight_Cluster_1_Services_ClientConfig/hosts**.
2. Si el host en el que está instalado el cliente no es un host del clúster, debe establecer la asignación entre el nombre del host y la dirección IP del plano de servicio para cada nodo de clúster de **/etc/hosts** como usuario **root**. Cada nombre de host asigna de forma única una dirección IP. Puede realizar los siguientes pasos para importar la asignación de nombres de dominio del clúster al archivo **hosts**:
   a. Cambie a usuario **root** o a un usuario que tenga permiso para modificar el archivo **hosts**.

      su - root

   b. Vaya al directorio donde se descomprime el paquete cliente.

      cd /tmp/FusionInsight_Cluster_1_Services_ClientConfig

   c. Ejecute el comando **cat realm.ini >> /etc/hosts** para importar la asignación de nombres de dominio al archivo **hosts**.

NOTA

- Si el host donde está instalado el cliente no es un nodo del clúster, configure las conexiones de red para que el cliente evite errores al ejecutar comandos en el cliente.
- Si las tareas de Spark se ejecutan en modo yarn-client, agregue el parámetro **spark.driver.host** al archivo *Client installation directory*/**Spark/spark/conf/spark-defaults.conf** y establezca el parámetro en la dirección IP del cliente.
- Si se utiliza el modo yarn-client, debe configurar la asignación entre la dirección IP y el nombre de host del cliente en el archivo **hosts** en los nodos Yarn activo y en espera (nodos ResourceManager en el clúster) para asegurarse de que la Spark web UI se muestra correctamente.

Paso 8 Inicie sesión en el nodo donde se va a instalar el cliente como usuario **user_client**, vaya al directorio de paquetes de software del cliente y ejecute el siguiente comando para instalar el cliente en un directorio especificado:

cd /tmp/clienttemp/FusionInsight_Cluster_1_Services_ClientConfig

./install.sh *Client installation directory*

Por ejemplo, ejecute el comando **./install.sh /opt/hadoopclient** para instalar el cliente y espere hasta que se complete la instalación.

```
...
The component client is installed successfully
```


NOTA

- **Es posible que el directorio de instalación del cliente no exista. Si es así, se crea uno nuevo automáticamente. No obstante, si existe, debe estar vacío. El directorio no puede contener espacios.**
- Debe eliminar manualmente el directorio de instalación del cliente al desinstalar un cliente.
- Para asegurarse de que el cliente instalado solo puede ser utilizado por el usuario de la instalación, agregue el parámetro **-o** durante la instalación. Por ejemplo, ejecute el comando **./install.sh /opt/hadoopclient -o** para instalar el cliente.
- Si se instala un cliente HBase, se recomienda que el directorio de instalación del cliente contenga solo letras mayúsculas y minúsculas, números y caracteres especiales (_-?.@+=) debido a la limitación de la sintaxis Ruby utilizada por HBase.

Paso 9 Utilice el cliente haciendo referencia a "Usar el cliente de cada componente".

----Fin

4.1.2 Instalación de un cliente (Versiones anteriores a 3.x)

Escenario

Se requiere un cliente de MRS. El cliente de clúster MRS se puede instalar en el nodo de Master o Core en el clúster o en un nodo fuera del clúster.

Después de crear un clúster de versiones anteriores a MRS 3.x, se instala un cliente en el nodo de Master activo de forma predeterminada. Puede utilizar directamente el cliente. El directorio de instalación es **/opt/client**.

Para obtener más información sobre cómo instalar un cliente de MRS 3.x o posterior, consulte **Instalación de un cliente (MRS 3.x o posterior)**.

NOTA

Si se ha instalado un cliente en el nodo fuera del clúster MRS y el cliente solo necesita actualizarse, actualice el cliente mediante el usuario que instaló el cliente, por ejemplo, usuario **root**.

Instalación de un cliente en el nodo de Core

1. Inicie sesión en MRS Manager y elija **Services** > **Download Client** para descargar el paquete de instalación del cliente en el nodo de gestión activa.

   NOTA

   Si solo es necesario actualizar el archivo de configuración del cliente, consulte el método 2 en **Actualización de un cliente (Versiones anteriores a 3.x)**.

2. Utilice la dirección IP para buscar el nodo de gestión activa e inicie sesión en el nodo de gestión activa mediante VNC.
3. Inicie sesión en el nodo de gestión activo y ejecute el siguiente comando para cambiar al usuario:

   sudo su - omm

4. En la consola de gestión de MRS, vea la dirección IP en la página de pestaña **Nodes** del clúster especificado.

   Registre la dirección IP del nodo de Core donde se va a utilizar el cliente.

5. En el nodo de gestión activo, ejecute el siguiente comando para copiar el paquete de instalación del cliente en el nodo de Core:

scp -p /tmp/MRS-client/MRS_Services_Client.tar *IP address of the Core node*:**/opt/client**

6. Inicie sesión en el nodo de Core como usuario **root**.

   Los nodos de Master admiten Cloud-Init. El nombre de usuario preestablecido para Cloud-Init es **root** y la contraseña es la que configuró durante la creación del clúster.

7. Ejecute los siguientes comandos para instalar el cliente:

   cd /opt/client

   tar -xvf MRS_Services_Client.tar

   tar -xvf MRS_Services_ClientConfig.tar

   cd /opt/client/MRS_Services_ClientConfig

   ./install.sh *Client installation directory*

   Por ejemplo, ejecute el siguiente comando:

   ./install.sh /opt/client

8. Para obtener más información acerca de cómo usar el cliente, consulte **Uso de un cliente de MRS**.

Uso de un cliente de MRS

1. En el nodo donde está instalado el cliente, ejecute el comando **sudo su - omm** para cambiar al usuario. Ejecute el siguiente comando para ir al directorio del cliente:

   cd /opt/client

2. Ejecute el siguiente comando para configurar las variables de entorno:

   source bigdata_env

3. Si la autenticación de Kerberos está habilitada para el clúster actual, ejecute el siguiente comando para autenticar al usuario. Si la autenticación de Kerberos está deshabilitada para el clúster actual, omita este paso.

   kinit *MRS cluster user*

   Ejemplo: **kinit admin**

   NOTA

   Usuario **admin** se crea de forma predeterminada para los clústeres de MRS con autenticación de Kerberos activada y se utiliza para que los administradores mantengan los clústeres.

4. Ejecute el comando de cliente de un componente directamente.

   Por ejemplo, ejecute el comando **hdfs dfs -ls /** para ver los archivos en el directorio raíz HDFS.

Instalación de un cliente en un nodo fuera del clúster

Paso 1 Cree un ECS que cumpla con los siguientes requisitos:

- Para clústeres de versiones anteriores a MRS 3.*x*, debe confirmar la arquitectura de CPU de los nodos de clúster MRS actuales. Para clústeres de versiones anteriores a MRS 3.*x*, la arquitectura de CPU del ECS debe ser la misma que la del nodo del clúster MRS. Para MRS 3.*x* o posterior, el cliente de MRS es compatible con las dos arquitecturas de CPU siguientes.
- Se ha preparado un ECS. Para obtener más información sobre el sistema operativo y su versión del ECS, consulte **Tabla 4-4**.

Tabla 4-4 Lista de referencias

Arquitectura de CPU	Sistema operativo	Versión admitida
Cómputo x86	EulerOS	– Disponible: EulerOS 2.2 – Disponible: EulerOS 2.3 – Disponible: EulerOS 2.5
Cómputo Kunpeng (Arm)	EulerOS	Disponible: EulerOS 2.8

Por ejemplo, un usuario puede seleccionar un ECS que ejecute EulerOS.

Además, se asigna suficiente espacio en disco para el ECS, por ejemplo, 40 GB.

- El ECS y el clúster MRS están en la misma VPC.
- El grupo de seguridad del ECS es el mismo que el del nodo master en el clúster MRS.

  Si no se cumple este requisito, modifique el grupo de seguridad de ECS o configure las reglas entrantes y salientes del grupo de seguridad de ECS para permitir que todos los grupos de seguridad de los nodos del clúster de MRS accedan al grupo de seguridad de ECS.
- Para permitir que los usuarios inicien sesión en un ECS de Linux con una contraseña (SSH), consulte *"Instancias" > "Iniciar sesión con un ECS de Linux" > "Iniciar sesión con una contraseña SSH" en Guía de usuario de Elastic Cloud Server* .
- Todos los puertos en la dirección de entrada del grupo de seguridad del clúster MRS están abiertos al nodo cliente. Para obtener más información, consulte **Agregar una regla de grupo de seguridad**.

Paso 2 Inicie sesión en MRS Manager. Para obtener más información, consulte **Acceso a MRS Manager (MRS 2.x o anterior)**. A continuación, seleccione **Services**.

Paso 3 Haga clic en **Download Client**.

Paso 4 En **Client Type**, seleccione **All client files**.

Paso 5 En **Download To**, seleccione **Remote host**.

Paso 6 Establezca **Host IP Address** en la dirección IP del ECS, **Host Port** en **22** y **Save Path** en **/tmp**.

- Si se ha cambiado el puerto predeterminado **22** para iniciar sesión en un ECS usando SSH, establezca **Host Port** en el puerto nuevo.
- **Save Path** contiene un máximo de 256 caracteres.

Paso 7 Ajuste **Login User** a **root**.

Si se utilizan otros usuarios, asegúrese de que los usuarios tienen permisos de lectura, escritura y ejecución en la ruta de guardado.

Paso 8 Seleccione **Password** o **SSH Private Key** para **Login Mode**.

- **Password**: Ingrese la contraseña del usuario **root** establecida durante la creación del clúster.

- **SSH Private Key**: Seleccione y cargue el archivo de clave utilizado para crear el clúster.

Paso 9 Haga clic en **OK** para generar un archivo de cliente.

Si se muestra la siguiente información, se guarda el paquete de cliente. Haga clic en **Close**. Obtenga el archivo de cliente de la ruta de guardado en el host remoto que se establece cuando se descarga el cliente.

```
Se descargaron los archivos del cliente al host remoto.
```

Si se muestra la siguiente información, compruebe las configuraciones de nombre de usuario, contraseña y grupo de seguridad del host remoto. Asegúrese de que el nombre de usuario y la contraseña sean correctos y de que se haya agregado una regla de entrada del puerto SSH (22) al grupo de seguridad del host remoto. Y luego, vaya a **Paso 2** para descargar el cliente de nuevo.

```
Failed to connect to the server. Please check the network connection or
parameter settings.
```

NOTA

La generación de un cliente ocupará un gran número de E/S de disco. Recomendamos no descargar un cliente cuando el clúster se está instalando, iniciando, cuando se están instalando parches en él o cuando su estado es inestable.

Paso 10 Inicie sesión en el ECS con VNC. Para obtener más información, consulte **Instancia** > **Inicio de sesión en un Linux** > **Inicio de sesión en un Linux** en la *Guía de usuario de Elastic Cloud Server*

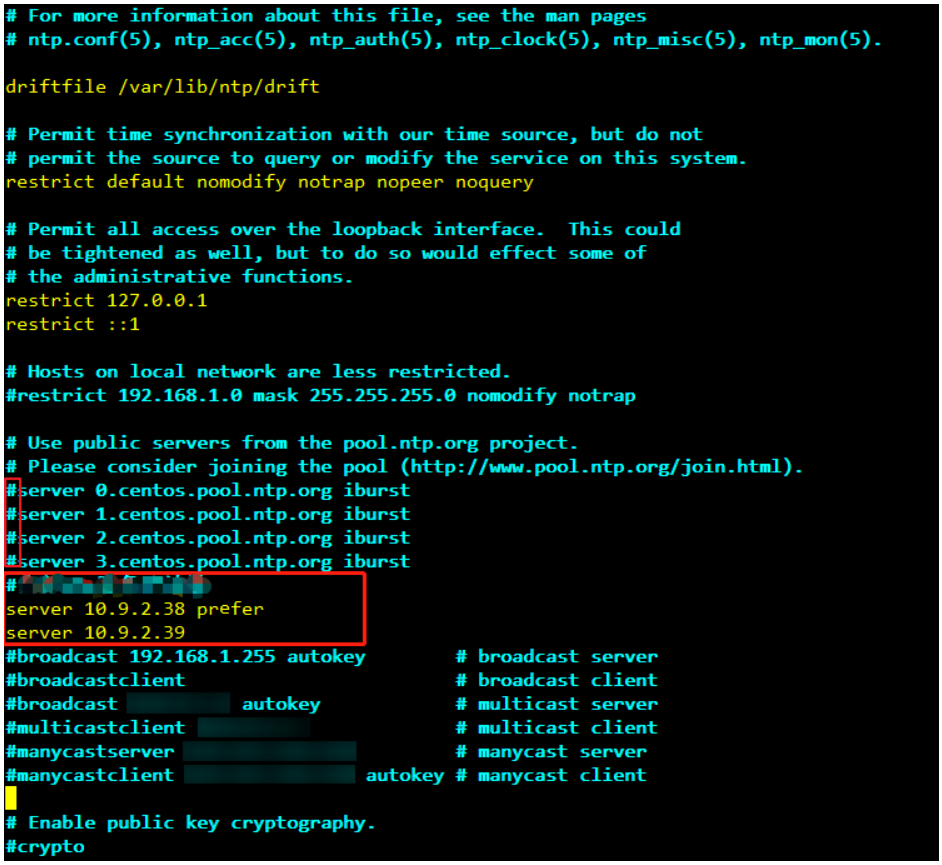
Todas las imágenes son compatibles con Cloud-Init. El nombre de usuario preestablecido para Cloud-Init es **root** y la contraseña es la que configuró durante la creación del clúster. Se recomienda que cambie la contraseña en el primer inicio de sesión.

Paso 11 Realice la sincronización de tiempo de NTP para sincronizar el tiempo de los nodos fuera del clúster con el tiempo del clúster MRS.

1. Compruebe si el servicio NTP está instalado. Si no está instalado, ejecute el comando **yum install ntp -y** para instalarlo.
2. Ejecute el comando **vim /etc/ntp.conf** para editar el archivo de configuración del cliente NTP, agregue la dirección IP del nodo de Master en el clúster MRS y comente las direcciones IP de otros servidores.

   ```
   server master1_ip prefer
   server master2_ip
   ```


Figura 4-4 Adición de las direcciones IP del nodo de master



3. Ejecute el comando **service ntpd stop** para detener el servicio NTP.
4. Ejecute el siguiente comando para sincronizar manualmente la hora:

   /usr/sbin/ntpdate *192.168.10.8*

   NOTA

   192.168.10.8 indica la dirección IP del nodo de Master activo.
5. Ejecute el comando **service ntpd start** o **systemctl restart ntpd** para iniciar el servicio NTP.
6. Ejecute el comando **ntpstat** para comprobar el resultado de la sincronización de tiempo:

Paso 12 En ECS, cambie a usuario **root** y copie el paquete de instalación en **Save Path** en **Paso 6** al directorio **/opt**. Por ejemplo, si **Save Path** está establecido en **/tmp**, ejecute los siguientes comandos:

sudo su - root

cp /tmp/MRS_Services_Client.tar /opt

Paso 13 Ejecute el siguiente comando en el directorio **/opt** para descomprimir el paquete y obtener el archivo de verificación y el paquete de configuración del cliente:

tar -xvf MRS_Services_Client.tar

Paso 14 Ejecute el siguiente comando para verificar el paquete de archivos de configuración del cliente:

sha256sum -c MRS_Services_ClientConfig.tar.sha256

La salida de comandos es la siguiente:

```
MRS_Services_ClientConfig.tar: OK
```

Paso 15 Ejecute el siguiente comando para descomprimir **MRS_Services_ClientConfig.tar**:

tar -xvf MRS_Services_ClientConfig.tar

Paso 16 Ejecute el siguiente comando para instalar el cliente en un nuevo directorio, por ejemplo **/opt/Bigdata/client**. Un directorio se genera automáticamente durante la instalación del cliente.

sh /opt/MRS_Services_ClientConfig/install.sh /opt/Bigdata/client

Si se muestra la siguiente información, el cliente se ha instalado correctamente:

```
Components client installation is complete.
```

Paso 17 Compruebe si la dirección IP del nodo de ECS está conectada a la dirección IP del nodo de Master del clúster.

Por ejemplo, ejecute el siguiente comando: **ping** *Master node IP address*.

- En caso afirmativo, vaya a **Paso 18**.
- Si no, compruebe si la VPC y el grupo de seguridad son correctos y si el clúster de ECS y MRS están en el mismo grupo de VPC y seguridad, y vaya a **Paso 18**.

Paso 18 Ejecute el siguiente comando para configurar las variables de entorno:

source /opt/Bigdata/client/bigdata_env

Paso 19 Si la autenticación de Kerberos está habilitada para el clúster actual, ejecute el siguiente comando para autenticar al usuario. Si la autenticación de Kerberos está deshabilitada para el clúster actual, omita este paso.

kinit *MRS cluster user*

Ejemplo: **kinit admin**

Paso 20 Ejecute el comando de cliente de un componente.

Por ejemplo, ejecute el siguiente comando para consultar el directorio de HDFS:

hdfs dfs -ls /

----Fin

4.2 Actualización de un cliente

4.2.1 Actualización de un cliente (Versión 3.x o posterior)

Un clúster proporciona un cliente para que pueda conectarse a un servidor, ver resultados de tareas o gestionar datos. Si modifica los parámetros de configuración del servicio en Manager y reinicia el servicio, deberá descargar e instalar el cliente de nuevo o utilizar el archivo de configuración para actualizarlo.

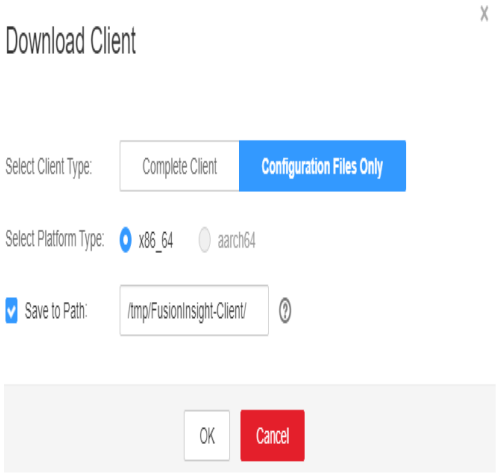
Actualización de la configuración del cliente

Método 1:

Paso 1 Inicie sesión en FusionInsight Manager. Para más detalles, consulte **Acceder a FusionInsight Manager (MRS 3.x o posterior)**. Haga clic en el nombre del clúster que se va a operar en la lista desplegable **Cluster**.

Paso 2 Elija **More** > **Download Client** > **Configuration Files Only**.

El archivo comprimido generado contiene los archivos de configuración de todos los servicios.



Paso 3 Determine si desea generar un archivo de configuración en el nodo del clúster.

- En caso afirmativo, seleccione **Save to Path** y haga clic en **OK** para generar el archivo cliente. De forma predeterminada, el archivo cliente se genera en **/tmp/FusionInsight-Client** en el nodo de gestión activa. También puede almacenar el archivo cliente en otros directorios, y el usuario **omm** tiene los permisos de lectura, escritura y ejecución en los directorios. Entonces vaya a **Paso 4**.
- Si no, haga clic en **OK**, especifique una ruta de guardado local y descargue el cliente completo. Espere hasta que se complete la descarga y vaya a **Paso 4**.

Paso 4 Utilice WinSCP para guardar el archivo comprimido en el directorio de instalación del cliente, por ejemplo **/opt/hadoopclient** como usuario de instalación del cliente.

Paso 5 Descomprima el paquete de software.

Ejecute los siguientes comandos para ir al directorio donde está instalado el cliente y descomprima el archivo en un directorio local. Por ejemplo, el archivo de cliente descargado es **FusionInsight_Cluster_1_Services_Client.tar**.

cd /opt/hadoopclient

tar -xvf FusionInsight_Cluster_1_Services_Client.tar

Paso 6 Verifique el paquete de software.

Ejecute el siguiente comando para verificar el archivo descomprimido y verifique si la salida del comando es consistente con la información del archivo **sha256**.

sha256sum -c FusionInsight_Cluster_1_Services_ClientConfig_ConfigFiles.tar.sha256

```
FusionInsight_Cluster_1_Services_ClientConfig_ConfigFiles.tar: OK
```


Paso 7 Descomprima el paquete para obtener el archivo de configuración.

tar -xvf FusionInsight_Cluster_1_Services_ClientConfig_ConfigFiles.tar

Paso 8 Ejecute el siguiente comando en el directorio de instalación del cliente para actualizar el cliente mediante el archivo de configuración:

sh refreshConfig.sh *Client installation directory Directory where the configuration file is located*

Por ejemplo, ejecute el siguiente comando:

sh refreshConfig.sh /opt/hadoopclient /opt/hadoopclient/FusionInsight_Cluster_1_Services_ClientConfig_ConfigFiles

Si se muestra la siguiente información, las configuraciones se han actualizado correctamente.

```
Acceda a actualizar la configuración del cliente de componentes.
```

----Fin

Método 2:

Paso 1 Inicie sesión en el nodo de instalación del cliente como usuario **root**.

Paso 2 Vaya al directorio de instalación del cliente, por ejemplo **/opt/hadoopclient** y ejecute los siguientes comandos para actualizar el archivo de configuración:

cd /opt/hadoopclient

sh autoRefreshConfig.sh

Paso 3 Introduzca el nombre de usuario y la contraseña del FusionInsight Manager y la dirección IP flotante del FusionInsight Manager.

Paso 4 Introduzca los nombres de los componentes cuya configuración debe actualizarse. Utilice comas (,) para separar los nombres de los componentes. Presione **Enter** para actualizar las configuraciones de todos los componentes si es necesario.

Si se muestra la siguiente información, las configuraciones se han actualizado correctamente.

```
Succeed to refresh components client config.
```

----Fin

4.2.2 Actualización de un cliente (Versiones anteriores a 3.x)

NOTA

Esta sección se aplica a clústeres de versiones anteriores a MRS 3.x. Para MRS 3.x o posterior, consulte **Actualización de un cliente (Versión 3.x o posterior)**.

Actualización de un archivo de configuración de cliente

Escenario

Un clúster de MRS proporciona un cliente para la conexión con el servidor, la visualización de resultados de tareas o la gestión de datos. Antes de utilizar un cliente de MRS deberá descargar y actualizar el archivo de configuración del cliente tanto si se modifican los parámetros de configuración del servicio y se reinicia un servicio o simplemente si se reinicia el servicio en MRS Manager.

Durante la creación del clúster, el cliente original se almacena en el directorio **/opt/client** en todos los nodos del clúster de forma predeterminada. Una vez creado el clúster, solo el cliente de un nodo principal podrá utilizarse de forma directa. Para poder utilizar el cliente de un nodo secundario, primero debe actualizar el archivo de configuración del cliente.

Procedimiento

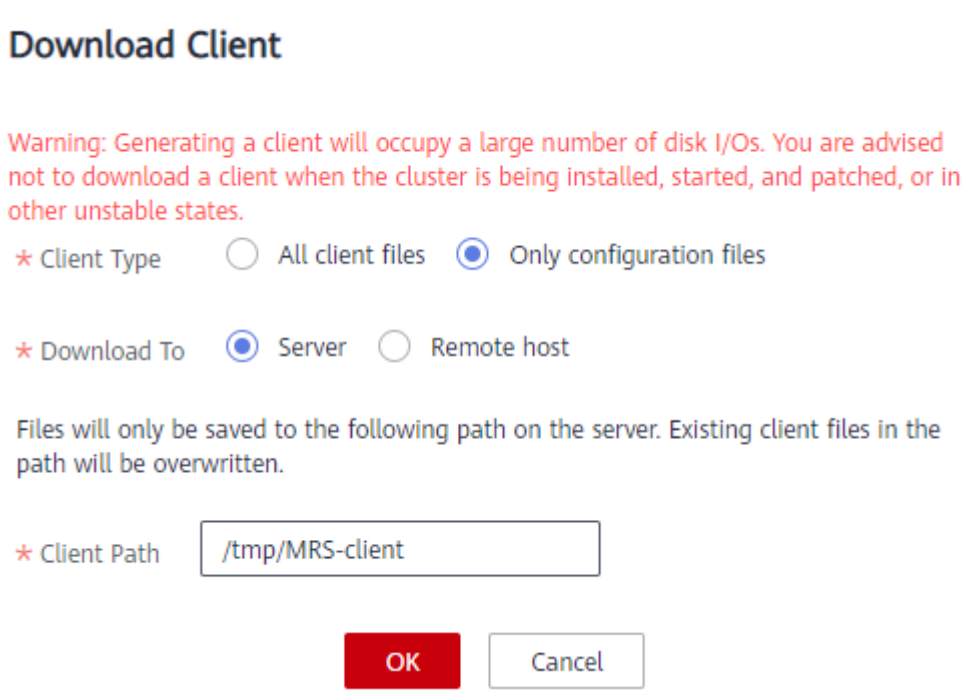
Método 1: aplicable a todas las versiones

Paso 1 Inicie sesión en MRS Manager. Para obtener más información, consulte **Acceso a MRS Manager (MRS 2.x o anterior)**. A continuación, seleccione **Services**.

Paso 2 Haga clic en **Download Client**.

Establezca **Client Type** en **Only configuration files**, **Download To** en **Server** y haga clic en **OK** para generar el archivo de configuración del cliente. El archivo generado se guarda en el directorio **/tmp/MRS-client** del nodo de gestión activo de forma predeterminada. Puede personalizar la ruta del archivo.

Figura 4-5 Descargar el archivo de configuración del cliente



Paso 3 Consulte e inicie sesión en el nodo de Master activo.

Paso 4 Si utiliza el cliente en el clúster, ejecute el siguiente comando para cambiar a usuario **omm**. Si utiliza el cliente fuera del clúster, cambie a usuario **root**.

sudo su - omm

Paso 5 Ejecute el siguiente comando para cambiar al directorio del cliente, por ejemplo **/opt/Bigdata/client**:

cd /opt/Bigdata/client

Paso 6 Ejecute el siguiente comando para actualizar las configuraciones del cliente:

sh refreshConfig.sh *Client installation directory Full path of the client configuration file package*

Por ejemplo, ejecute el siguiente comando:

sh refreshConfig.sh /opt/Bigdata/client /tmp/MRS-client/MRS_Services_Client.tar

Si se muestra la siguiente información, las configuraciones se han actualizado correctamente.

```
ReFresh components client config is complete.
Succeed to refresh components client config.
```

----Fin

Método 2:

Paso 1 Una vez instalado el clúster, ejecute el siguiente comando para cambiar a usuario **omm**. Si utiliza el cliente fuera del clúster, cambie a usuario **root**.

sudo su - omm

Paso 2 Ejecute el siguiente comando para cambiar al directorio del cliente, por ejemplo **/opt/Bigdata/client**:

cd /opt/Bigdata/client

Paso 3 Ejecute el siguiente comando e introduzca el nombre de un usuario de MRS Manager con el permiso de descarga y su contraseña (por ejemplo, el nombre de usuario es **admin** y la contraseña es la establecida durante la creación del clúster) cuando se le solicite actualizar las configuraciones del cliente.

sh autoRefreshConfig.sh

Paso 4 Después de ejecutar el comando, se muestra la siguiente información, donde *XXX* indica el nombre del componente instalado en el clúster. Para actualizar las configuraciones del cliente de todos los componentes, presione **Enter**. Para actualizar las configuraciones de cliente de algunos componentes, introduzca los nombres de los componentes y sepárelos con comas (,).

```
Components "xxx" have been installed in the cluster. Please input the comma-
separated names of the components for which you want to update client
configurations. If you press Enter without inputting any component name, the
client configurations of all components will be updated:
```

Si se muestra la siguiente información, las configuraciones se han actualizado correctamente.

```
Succeed to refresh components client config.
```

Si se muestra la siguiente información, el nombre de usuario o la contraseña son incorrectos.

```
login manager failed,Incorrect username or password.
```

NOTA

- Este script se conecta automáticamente al clúster e invoca el script **refreshConfig.sh** para descargar y actualizar el archivo de configuración del cliente.
- De forma predeterminada, el cliente utiliza la dirección IP flotante especificada por **wsom=xxx** en el archivo **Version** del directorio de instalación para actualizar las configuraciones del cliente. Para actualizar el archivo de configuración de otro clúster, modifique el valor de **wsom=xxx** en el archivo **Version** a la dirección IP flotante del clúster correspondiente antes de realizar este paso.

----Fin

Actualización completa del cliente original del nodo de Master activo

Escenario

Durante la creación del clúster, el cliente original se almacena en el directorio **/opt/client** en todos los nodos del clúster de forma predeterminada. A continuación se utiliza **/opt/Bigdata/client** como ejemplo.

- Para un clúster MRS normal, usará el cliente preinstalado en un nodo de Master para enviar un trabajo en la página de consola de gestión.
- También puede utilizar el cliente preinstalado en el nodo de Master para conectarse a un servidor, ver resultados de tareas y gestionar datos.

Después de instalar el parche en el clúster, debe actualizar el cliente en el nodo de Master para asegurarse de que las funciones del cliente integrado están disponibles.

Procedimiento

Paso 1 Inicie sesión en MRS Manager. Para obtener más información, consulte **Acceso a MRS Manager (MRS 2.x o anterior)**. A continuación, seleccione **Services**.

Paso 2 Haga clic en **Download Client**.

Establezca **Client Type** en **All client files**, **Download To** en **Server** y haga clic en **OK** para generar el archivo de configuración del cliente. El archivo generado se guarda en el directorio **/tmp/MRS-client** del nodo de gestión activo de forma predeterminada. Puede personalizar la ruta del archivo.

Paso 3 Consulte e inicie sesión en el nodo de Master activo.

Paso 4 En ECS, cambie a usuario **root** y copie el paquete de instalación en el directorio **/opt**.

sudo su - root

cp /tmp/MRS-client/MRS_Services_Client.tar /opt

Paso 5 Ejecute el siguiente comando en el directorio **/opt** para descomprimir el paquete y obtener el archivo de verificación y el paquete de configuración del cliente:

tar -xvf MRS_Services_Client.tar

Paso 6 Ejecute el siguiente comando para verificar el paquete de archivos de configuración del cliente:

sha256sum -c MRS_Services_ClientConfig.tar.sha256

La salida de comandos es la siguiente:

```
MRS_Services_ClientConfig.tar: OK
```

Paso 7 Ejecute el siguiente comando para descomprimir **MRS_Services_ClientConfig.tar**:

tar -xvf MRS_Services_ClientConfig.tar

Paso 8 Ejecute el siguiente comando para mover el cliente original al directorio **/opt/Bigdata/client_bak**:

mv /opt/Bigdata/client /opt/Bigdata/client_bak

Paso 9 Ejecute el siguiente comando para instalar el cliente en un directorio nuevo. La ruta de acceso del cliente debe ser **/opt/Bigdata/client**.

sh /opt/MRS_Services_ClientConfig/install.sh /opt/Bigdata/client

Si se muestra la siguiente información, el cliente se ha instalado correctamente:

```
Components client installation is complete.
```

Paso 10 Ejecute el siguiente comando para modificar el usuario y el grupo de usuarios del directorio **/opt/Bigdata/client**:

chown omm:wheel /opt/Bigdata/client -R

Paso 11 Ejecute el siguiente comando para configurar las variables de entorno:

source /opt/Bigdata/client/bigdata_env

Paso 12 Si la autenticación de Kerberos está habilitada para el clúster actual, ejecute el siguiente comando para autenticar al usuario. Si la autenticación de Kerberos está deshabilitada para el clúster actual, omita este paso.

kinit *MRS cluster user*

Ejemplo: **kinit admin**

Paso 13 Ejecute el comando de cliente de un componente.

Por ejemplo, ejecute el siguiente comando para consultar el directorio de HDFS:

hdfs dfs -ls /

----Fin

Actualización completa del cliente original del nodo de Master en espera

Paso 1 Repita **Paso 1** a **Paso 3** para iniciar sesión en el nodo de Master en espera y ejecute el siguiente comando para cambiar a usuario **omm**:

sudo su - omm

Paso 2 Ejecute el siguiente comando en el nodo de Master en espera para copiar el paquete cliente descargado del nodo de Master activo:

scp omm@*master1 nodeIP address***:/tmp/MRS-client/MRS_Services_Client.tar /tmp/MRS-client/**

NOTA

- En este comando, el nodo **master1** es el nodo de master activo.
- **/tmp/MRS-client/** es un directorio de destino de ejemplo del nodo master en espera.

Paso 3 Repita **Paso 4** a **Paso 13** para actualizar el cliente del nodo de Master en espera.

----Fin

5 Acceso a páginas web de componentes de código abierto gestionados en clústeres de MRS

5.1 Interfaz de usuario web de componentes de código abierto

Escenario

Las interfaces de usuarios web de los diferentes componentes se crean y alojan en los nodos principales o secundarios en el clúster de MRS, de forma predeterminada. Estas interfaces de usuario web permiten ver información de los componentes.

Procedimiento para acceder a las interfaces de usuario web del componente de código abierto:

1. Seleccione un método de acceso.

   MRS proporciona los siguientes métodos para acceder a las interfaces de usuario web de los componentes de código abierto:

   - **Acceso basado en EIP**: Este método se recomienda porque es fácil vincular un EIP a un clúster.
   - **Acceso mediante un ECS de Windows**: Los ECS independientes deben crearse y configurarse.
   - **Creación de un canal de SSH para conectarse a un clúster de MRS y configurar el navegador** Utilice este método cuando el usuario y el clúster MRS están en redes diferentes.

2. Acceda a las interfaces de usuario web. Para obtener más información, consulte **Tabla 5-1**.

Web UIs

NOTA

Para los clústeres con autenticación de Kerberos activada, el usuario **admin** no tiene el permiso de gestión en cada componente. Para acceder a la interfaz de usuario web de cada componente, cree un usuario que tenga el permiso de gestión en el componente correspondiente.

Tabla 5-1 Direcciones de interfaz de usuario web de componentes de código abierto

Tipo de clúster	Tipo de Web UI	Dirección de Web UI
Todos los tipos	MRS Manager	● Aplicable a clústeres de todas las versiones **https://***Floating IP address of Manager***:28443/web** **NOTA** 1. Asegúrese de que el host local pueda comunicarse con el clúster MRS. 2. Inicie sesión en el nodo Master2 de forma remota y ejecute el comando **ifconfig**. En la salida del comando, **eth0:wsom** indica la dirección IP flotante del MRS Manager. Registre el valor de **inet**. Si la dirección IP flotante del MRS Manager no se puede consultar en el nodo de Master2, cambie al nodo de Master1 para consultar y registrar la dirección IP flotante. Si solo hay un nodo maestro, consulte y registre la dirección IP del administrador de clústeres del nodo de Master. ● Para versiones anteriores a MRS 3.x: https://<*EIP*>:9022/mrsmanager?locale=en-us Para obtener más información, consulte **Acceso a MRS Manager (MRS 2.x o anterior)**. ● Para MRS 3.*x* o posterior, consulte **Acceder a FusionInsight Manager (MRS 3.x o posterior)**.
Clúster de análisis	HDFS NameNode	● Versiones anteriores a MRS 3.x: En la página de detalles del clúster, elija **Components** > **HDFS** > **NameNode Web UI** > **NameNode (Active)**. ● MRS 3.x o posterior: en la página principal del Manager, elija **Cluster** > **Services** > **HDFS** > **NameNode Web UI** > **NameNode (*Host name*, Active)**.
	HBase HMaster	● Versiones anteriores a MRS 3.x: En la página de detalles del clúster, elija **Components** > **HBase** > **HMaster Web UI** > **HMaster (Active)**. ● MRS 3.x o posterior: en la página principal del Manager, elija **Cluster** > **Services** > **HBase** > **HMaster Web UI** > **HMaster (*Host name*, Active)**.

Tipo de clúster	Tipo de Web UI	Dirección de Web UI
	MapReduce JobHistoryServer	● Versiones anteriores a MRS 3.x: En la página de detalles del clúster, elija **Components** > **MapReduce** > **JobHistoryServer Web UI** > **JobHistoryServer**. ● MRS 3.x o posterior: En la página principal de Manager, elija **Cluster** > **Services** > **MapReduce** > **JobHistoryServer Web UI** > **JobHistoryServer (*Host name*, Active)**.
	YARN ResourceManager	● Versiones anteriores a MRS 3.x: En la página de detalles del clúster, elija **Components** > **Yarn** > **ResourceManager Web UI** > **ResourceManager (Active)**. ● MRS 3.x o posterior: en la página principal del Manager, elija **Cluster** > **Services** > **Yarn** > **ResourceManager Web UI** > **ResourceManager (*Host name*, Active)**.
	Spark JobHistory	● Versiones anteriores a MRS 3.x: En la página de detalles del clúster, elija **Components** > **Spark** > **Spark Web UI** > **JobHistory**. ● MRS 3.x o posterior: en la página de inicio de Manager, elija **Cluster** > **Services** > **Spark2x** > **Spark2x Web UI** > **JobHistory2x (*Host name*, Active)**.
	Hue	● Versiones anteriores a MRS 3.x: En la página de detalles del clúster, elija **Components** > **Hue** > **Hue Web UI** > **Hue (Active)**. ● MRS 3.x o posterior: en la página principal del Manager, elija **Cluster** > **Services** > **Hue** > **Hue Web UI** > **Hue (*Host name*, Active)**. Loader es una herramienta de gestión de migración de datos gráfica basada en la interfaz de usuario web de código abierto de Sqoop, y su interfaz está alojada en la interfaz de usuario web de Hue.

Tipo de clúster	Tipo de Web UI	Dirección de Web UI
	Tez	● Versiones anteriores a MRS 3.x: En la página de detalles del clúster, elija **Components** > **Tez** > **Tez Web UI** > **TezUI**. ● MRS 3.x o posterior: En la página principal del Manager, elija **Cluster** > **Services** > **Tez** > **Tez Web UI** > **TezUI (*Host name*, Active)**.
	Presto	● Versiones anteriores a MRS 3.x: En la página de detalles del clúster, elija **Components** > **Presto** > **Presto Web UI** > **Coordinator (Active)**. ● En la página principal del Manager, elija **Cluster** > **Services** > **Presto** > **Coordinator Web UI** > **Coordinator (Coordinator)**.
	Ranger	● Versiones anteriores a MRS 3.x: En la página de detalles del clúster, elija **Components** > **Ranger** > **Ranger Web UI** > **RangerAdmin (Active)**. ● MRS 3.x o posterior: En la página principal del Manager, elija **Cluster** > **Services** > **Ranger** > **Ranger Web UI** > **RangerAdmin**.
Clúster de procesamiento de flujo	Storm	● Versiones anteriores a MRS 3.x: En la página de detalles del clúster, elija **Components** > **Storm** > **Storm Web UI** > **UI**. ● En la página principal del Manager, elija **Cluster** > **Services** > **Storm** > **Storm Web UI** > **UI (*Host name*)**.

5.2 Puertos comunes de componentes

Escenario

Cuando usted **compra un clúster personalizado** de una versión LTS, puede personalizar el puerto del componente. Si no desea personalizar un puerto, se utiliza un puerto de código abierto.

- **Open source**: Encuentre el puerto predeterminado del componente en la columna de Puerto de código abierto predeterminado de la siguiente tabla.
- **Custom**: Encuentre el puerto predeterminado del componente en la columna Puerto personalizado predeterminado de la siguiente tabla.

- Si solo hay la columna Puerto predeterminado, el puerto de código abierto del componente es el mismo que el puerto personalizado predeterminado.

Si el clúster no es de una versión LTS, el parámetro **Component Port** no está disponible y solo se puede usar un puerto de código abierto. Para obtener más información, consulte la columna de Puerto de código abierto predeterminado o Puerto predeterminado.

Puertos de HBase comunes

El tipo de protocolo de todos los puertos de la tabla es TCP.

Parámetro	Puerto de código abierto predeterminado	Puerto personalizado predeterminado	Descripción de puertos
hbase.master.port	16000	21300	Puerto de HMaster RPC. Este puerto se utiliza para conectar el cliente de HBase a HMaster. **NOTA** El ID de puerto es un valor recomendado y se especifica en función del producto. El rango de puerto no está restringido en el código. - El puerto está habilitado de forma predeterminada durante la instalación: Sí - ¿El puerto está habilitado después del refuerzo de seguridad?: Sí
hbase.master.info.port	16010	21301	Puerto de HMaster HTTPS. Este puerto es utilizado por el cliente web remoto para conectarse a la interfaz de usuario de HMaster. **NOTA** El ID de puerto es un valor recomendado y se especifica en función del producto. El rango de puerto no está restringido en el código. - El puerto está habilitado de forma predeterminada durante la instalación: Sí - ¿El puerto está habilitado después del refuerzo de seguridad?: Sí

Parámetro	Puerto de código abierto predeterminado	Puerto personalizado predeterminado	Descripción de puertos
hbase.regionserver.port	16020	21302	Puerto de RegoinServer (RS) RPC. Este puerto se utiliza para conectar el cliente HBase a RegionServer. **NOTA** El ID de puerto es un valor recomendado y se especifica en función del producto. El rango de puerto no está restringido en el código. ● El puerto está habilitado de forma predeterminada durante la instalación: Sí ● ¿El puerto está habilitado después del refuerzo de seguridad?: Sí
hbase.regionserver.info.port	16030	21303	Puerto de HTTPS del servidor de Region. Este puerto es utilizado por el cliente web remoto para conectarse a la interfaz de usuario RegionServer. **NOTA** El ID de puerto es un valor recomendado y se especifica en función del producto. El rango de puerto no está restringido en el código. ● El puerto está habilitado de forma predeterminada durante la instalación: Sí ● ¿El puerto está habilitado después del refuerzo de seguridad?: Sí

Parámetro	Puerto de código abierto predeterminado	Puerto personalizado predeterminado	Descripción de puertos
hbase.thrift.info.port	9095	21304	Puerto de escucha de Thrift Server de Thrift Server Este puerto se utiliza para: Escuchar cuando el cliente está conectado **NOTA** El ID de puerto es un valor recomendado y se especifica en función del producto. El rango de puerto no está restringido en el código. ● El puerto está habilitado de forma predeterminada durante la instalación: Sí ● ¿El puerto está habilitado después del refuerzo de seguridad?: Sí
hbase.regionserver.thrift.port	9090	21305	Puerto de escucha de Thrift Server de RegionServer Este puerto se utiliza para: Escuchar cuando el cliente está conectado a RegionServer **NOTA** El ID de puerto es un valor recomendado y se especifica en función del producto. El rango de puerto no está restringido en el código. ● El puerto está habilitado de forma predeterminada durante la instalación: Sí ● ¿El puerto está habilitado después del refuerzo de seguridad?: Sí
hbase.rest.info.port	8085	21308	Puerto de la página web nativa de RegionServer RESTServer
-	21309	21309	Puerto de REST de RegionServer RESTServer

Puertos de HDFS comunes

El tipo de protocolo de todos los puertos de la tabla es TCP.

Parámetro	Puerto de código abierto predeterminado	Puerto personalizado predeterminado	Descripción de puertos
dfs.namenode.rpc.port	● 9820 (versions earlier than MRS 3.*x*) ● 8020 (MRS 3.*x* and later)	25000	Puerto de NameNode RPC Este puerto se utiliza para: 1. Comunicación entre el cliente HDFS y NameNode 2. Conexión entre el DataNode y el NameNode **NOTA** El ID de puerto es un valor recomendado y se especifica en función del producto. El rango de puerto no está restringido en el código. ● El puerto está habilitado de forma predeterminada durante la instalación: Sí ● ¿El puerto está habilitado después del refuerzo de seguridad?: Sí
dfs.namenode.http.port	9870	25002	Puerto de HDFS HTTP (NameNode) Este puerto se utiliza para: 1. Operaciones de punto de control de NameNode punto a punto. 2. Conexión del cliente web remoto a la interfaz de usuario de NameNode **NOTA** El ID de puerto es un valor recomendado y se especifica en función del producto. El rango de puerto no está restringido en el código. ● El puerto está habilitado de forma predeterminada durante la instalación: Sí ● ¿El puerto está habilitado después del refuerzo de seguridad?: Sí

Parámetro	Puerto de código abierto predeterminado	Puerto personalizado predeterminado	Descripción de puertos
dfs.namenode.https.port	9871	25003	Puerto de HDFS HTTPS (NameNode) Este puerto se utiliza para: 1. Operaciones de punto de control de NameNode punto a punto 2. Conexión del cliente web remoto a la interfaz de usuario de NameNode **NOTA** El ID de puerto es un valor recomendado y se especifica en función del producto. El rango de puerto no está restringido en el código. ● El puerto está habilitado de forma predeterminada durante la instalación: Sí ● ¿El puerto está habilitado después del refuerzo de seguridad?: Sí
dfs.datanode.ipc.port	9867	25008	Puerto de servidor de IPC de DataNode Este puerto se utiliza para: Conexión entre el cliente y DataNode para realizar operaciones de RPC. **NOTA** El ID de puerto es un valor recomendado y se especifica en función del producto. El rango de puerto no está restringido en el código. ● El puerto está habilitado de forma predeterminada durante la instalación: Sí ● ¿El puerto está habilitado después del refuerzo de seguridad?: Sí

Parámetro	Puerto de código abierto predeterminado	Puerto personalizado predeterminado	Descripción de puertos
dfs.datanode.port	9866	25009	Puerto de transmisión de datos de DataNode Este puerto se utiliza para: 1. Transmisión de datos desde el cliente de HDFS desde o hacia el DataNode 2. Transmisión de datos de DataNode punto a punto **NOTA** El ID de puerto es un valor recomendado y se especifica en función del producto. El rango de puerto no está restringido en el código. ● El puerto está habilitado de forma predeterminada durante la instalación: Sí ● ¿El puerto está habilitado después del refuerzo de seguridad?: Sí
dfs.datanode.http.port	9864	25010	Puerto de HTTP de DataNode Este puerto se utiliza para: Conexión a DataNode desde el cliente web remoto en modo de seguridad **NOTA** El ID de puerto es un valor recomendado y se especifica en función del producto. El rango de puerto no está restringido en el código. ● El puerto está habilitado de forma predeterminada durante la instalación: Sí ● ¿El puerto está habilitado después del refuerzo de seguridad?: Sí
dfs.datanode.https.port	9865	25011	Puerto de HTTPS de DataNode Este puerto se utiliza para: Conexión a DataNode desde el cliente web remoto en modo de seguridad **NOTA** El ID de puerto es un valor recomendado y se especifica en función del producto. El rango de puerto no está restringido en el código. ● El puerto está habilitado de forma predeterminada durante la instalación: Sí ● ¿El puerto está habilitado después del refuerzo de seguridad?: Sí

Parámetro	Puerto de código abierto predeterminado	Puerto personalizado predeterminado	Descripción de puertos
dfs.JournalNode.rpc.port	8485	25012	Puerto de RPC de JournalNode Este puerto se utiliza para: Comunicación con el cliente para acceder a múltiples tipos de información **NOTA** El ID de puerto es un valor recomendado y se especifica en función del producto. El rango de puerto no está restringido en el código. ● El puerto está habilitado de forma predeterminada durante la instalación: Sí ● ¿El puerto está habilitado después del refuerzo de seguridad?: Sí
dfs.journalnode.http.port	8480	25013	Puerto de HTTP de JournalNode Este puerto se utiliza para: Conexión a JournalNode desde el cliente web remoto en modo de seguridad **NOTA** El ID de puerto es un valor recomendado y se especifica en función del producto. El rango de puerto no está restringido en el código. ● El puerto está habilitado de forma predeterminada durante la instalación: Sí ● ¿El puerto está habilitado después del refuerzo de seguridad?: Sí
dfs.journalnode.https.port	8481	25014	Puerto de HTTPS de JournalNode Este puerto se utiliza para: Conexión a JournalNode desde el cliente web remoto en modo de seguridad **NOTA** El ID de puerto es un valor recomendado y se especifica en función del producto. El rango de puerto no está restringido en el código. ● El puerto está habilitado de forma predeterminada durante la instalación: Sí ● ¿El puerto está habilitado después del refuerzo de seguridad?: Sí

Parámetro	Puerto de código abierto predeterminado	Puerto personalizado predeterminado	Descripción de puertos
httpfs.http.port	14000	25018	Puerto de escucha del servidor HTTP HttpFS Este puerto se utiliza para: Conexión a HttpFS desde la API de REST remota **NOTA** El ID de puerto es un valor recomendado y se especifica en función del producto. El rango de puerto no está restringido en el código. ● El puerto está habilitado de forma predeterminada durante la instalación: Sí ● ¿El puerto está habilitado después del refuerzo de seguridad?: Sí

Puertos comunes de Hive

El tipo de protocolo de todos los puertos de la tabla es TCP.

Parámetro	Puerto de código abierto predeterminado	Puerto personalizado predeterminado	Descripción de puertos
templeton.port	9111	21055	Puerto utilizado para WebHCat para proporcionar el servicio REST Este puerto se utiliza para: Comunicación entre el cliente WebHCat y el servidor WebHCat ● El puerto está habilitado de forma predeterminada durante la instalación: Sí ● ¿El puerto está habilitado después del refuerzo de seguridad?: Sí

Parámetro	Puerto de código abierto predeterminado	Puerto personalizado predeterminado	Descripción de puertos
hive.server2.thrift.port	10000	21066	Puerto para HiveServer para proporcionar servicios de Thrift Este puerto se utiliza para: Comunicación entre el cliente HiveServer y HiveServer ● El puerto está habilitado de forma predeterminada durante la instalación: Sí ● ¿El puerto está habilitado después del refuerzo de seguridad?: Sí
hive.metastore.port	9083	21088	Puerto de MetaStore para proporcionar servicios de Thrift Este puerto se utiliza para: Comunicación entre el cliente MetaStore y MetaStore, es decir, comunicación entre HiveServer y MetaStore. ● El puerto está habilitado de forma predeterminada durante la instalación: Sí ● ¿El puerto está habilitado después del refuerzo de seguridad?: Sí
hive.server2.webui.port	10002	-	Puerto de Web UI de Hive Este puerto se utiliza para: comunicación de HTTPS/HTTP entre las solicitudes de Web y el servidor de Hive UI

Puertos comunes de Hue

El tipo de protocolo de todos los puertos de la tabla es TCP.

Parámetro	Puerto de código abierto predeterminado	Puerto personalizado predeterminado	Descripción de puertos
HTTP_PORT	8888	21200	Puerto para Hue para proporcionar servicios HTTPS Este puerto se utiliza para proporcionar servicios web en modo HTTPS, que se puede cambiar. ● El puerto está habilitado de forma predeterminada durante la instalación: Sí ● ¿El puerto está habilitado después del refuerzo de seguridad?: Sí

Puertos comunes de Kafka

El tipo de protocolo de todos los puertos de la tabla es TCP.

Parámetro	Puerto de código abierto predeterminado	Puerto personalizado predeterminado	Descripción de puertos
port	9092	21005	Puerto para que un broker reciba datos y obtenga servicios
ssl.port	9093	21008	Puerto SSL utilizado por un broker para recibir datos y obtener servicios
sasl.port	21007	21007	Puerto de autenticación de seguridad SASL proporcionado por un broker, que proporciona el servicio seguro de Kafka
sasl-ssl.port	21009	21009	Puerto utilizado por un broker para proporcionar un servicio cifrado basado en los protocolos SASL y SSL

Puertos comunes de Loader

El tipo de protocolo de todos los puertos de la tabla es TCP.

Parámetro	Puerto predeterminado	Descripción de puertos
LOADER_HTTPS_PORT	21351	Este puerto se utiliza para proporcionar las API de REST para la configuración y ejecución de trabajos de Loader. ● El puerto está habilitado de forma predeterminada durante la instalación: Sí ● ¿El puerto está habilitado después del refuerzo de seguridad?: Sí

Puertos de Manager común

El tipo de protocolo de todos los puertos de la tabla es TCP.

Parámetro	Puerto predeterminado (Versiones anteriores a MRS 3.x)	Descripción de puertos
-	8080	Puerto proporcionado por WebService para el acceso del usuario Este puerto se utiliza para acceder a la interfaz de usuario web a través de HTTP. ● El puerto está habilitado de forma predeterminada durante la instalación: Sí ● ¿El puerto está habilitado después del refuerzo de seguridad?: Sí
-	28443	Puerto proporcionado por WebService para el acceso del usuario Este puerto se utiliza para acceder a la interfaz de usuario web a través de HTTPS. ● El puerto está habilitado de forma predeterminada durante la instalación: Sí ● ¿El puerto está habilitado después del refuerzo de seguridad?: Sí

Puertos comunes de MapReduce

El tipo de protocolo de todos los puertos de la tabla es TCP.

Parámetro	Puerto de código abierto predeterminado	Puerto personalizado predeterminado	Descripción de puertos
mapreduce.jobhistory.webapp.port	19888	26012	Puerto de Web HTTP del servidor de JobHistory Este puerto se utiliza para: ver la página web del servidor de JobHistory **NOTA** El ID de puerto es un valor recomendado y se especifica en función del producto. El rango de puerto no está restringido en el código. ● El puerto está habilitado de forma predeterminada durante la instalación: Sí ● ¿El puerto está habilitado después del refuerzo de seguridad?: Sí
mapreduce.jobhistory.port	10020	26013	Puerto del servidor de JobHistory Este puerto se utiliza para: 1. Restauración de datos de tareas en el cliente MapReduce 2. Obtención del informe de tareas en el cliente de Job **NOTA** El ID de puerto es un valor recomendado y se especifica en función del producto. El rango de puerto no está restringido en el código. ● El puerto está habilitado de forma predeterminada durante la instalación: Sí ● ¿El puerto está habilitado después del refuerzo de seguridad?: Sí
mapreduce.jobhistory.webapp.https.port	19890	26014	Puerto de Web HTTPS del servidor JobHistory Este puerto se utiliza para ver la página web del servidor JobHistory. **NOTA** El ID de puerto es un valor recomendado y se especifica en función del producto. El rango de puertos no está restringido en el código. ● El puerto está habilitado de forma predeterminada durante la instalación: Sí ● ¿El puerto está habilitado después del refuerzo de seguridad?: Sí

Puertos comunes de Spark

El tipo de protocolo de todos los puertos de la tabla es TCP.

Parámetro	Puerto de código abierto predeterminado	Puerto personalizado predeterminado	Descripción de puertos
hive.server2.thrift.port	22550	22550	Puerto de JDBC thrift Este puerto se utiliza para: Comunicación de socket entre el cliente y el servidor Spark2.1.0 CLI/JDBC **NOTA** Si **hive.server2.thrift.port** está ocupado, se notifica una excepción que indica que el puerto está ocupado. ● El puerto está habilitado de forma predeterminada durante la instalación: Sí ● ¿El puerto está habilitado después del refuerzo de seguridad?: Sí
spark.ui.port	4040	22950	Puerto de Web UI de JDBC Este puerto se utiliza para: comunicación HTTPS/HTTP entre las solicitudes de web y el JDBC Server Web UI server **NOTA** El sistema verifica la configuración del puerto. Si el puerto no es válido, se utiliza el valor del puerto más 1 hasta que el valor calculado sea válido. (Se permite un número máximo de 16 intentos. **spark.port.maxRetries** especifica el número de intentos.) ● El puerto está habilitado de forma predeterminada durante la instalación: Sí ● ¿El puerto está habilitado después del refuerzo de seguridad?: Sí

Parámetro	Puerto de código abierto predeterminado	Puerto personalizado predeterminado	Descripción de puertos
spark.history.ui.port	18080	22500	Puerto de JobHistory Web UI Este puerto se utiliza para: comunicación de HTTPS/HTTP entre las solicitudes de Web y el Spark2.1.0 History Server **NOTA** El sistema verifica la configuración del puerto. Si el puerto no es válido, se utiliza el valor del puerto más 1 hasta que el valor calculado sea válido. (Se permite un número máximo de 16 intentos. **spark.port.maxRetries** especifica el número de intentos.) ● El puerto está habilitado de forma predeterminada durante la instalación: Sí ● ¿El puerto está habilitado después del refuerzo de seguridad?: Sí

Puertos comunes de Storm

El tipo de protocolo de todos los puertos de la tabla es TCP.

Parámetro	Puerto de código abierto predeterminado	Puerto personalizado predeterminado	Descripción de puertos
nimbus.thrift.port	6627	29200	Puerto para Nimbus para proporcionar servicios de thrift
supervisor.slots.ports	6700, 6701, 6702, 6703	29200-29499	Puerto para recibir solicitudes de servicio que se reenvían desde otros servidores

Parámetro	Puerto de código abierto predeterminado	Puerto personalizado predeterminado	Descripción de puertos
logviewer.https.port	29248	29248	Puerto para LogViewer para proporcionar servicios de HTTPS
ui.https.port	29243	29243	Puerto para Storm UI para proporcionar servicios de HTTPS (ui.https.port)

Puertos comunes de Yarn

El tipo de protocolo de todos los puertos de la tabla es TCP.

Parámetro	Puerto de código abierto predeterminado	Puerto personalizado predeterminado	Descripción de puertos
yarn.resourcemanager.webapp.port	8088	26000	Puerto de Web HTTP del servicio de ResourceManager

Parámetro	Puerto de código abierto predeterminado	Puerto personalizado predeterminado	Descripción de puertos
yarn.resourcemanager.webapp.https.port	8090	26001	Puerto de Web HTTPS del servicio de ResourceManager Este puerto se utiliza para acceder a las aplicaciones de web de Resource Manager en modo de seguridad. **NOTA** El ID de puerto es un valor recomendado y se especifica en función del producto. El rango de puertos no está restringido en el código. ● El puerto está habilitado de forma predeterminada durante la instalación: Sí ● ¿El puerto está habilitado después del refuerzo de seguridad?: Sí
yarn.nodemanager.webapp.port	8042	26006	Puerto de NodeManager Web HTTP
yarn.nodemanager.webapp.https.port	8044	26010	Puerto de NodeManager Web HTTPS Este puerto se utiliza para: Acceso a la aplicación web de NodeManager en modo de seguridad **NOTA** El ID de puerto es un valor recomendado y se especifica en función del producto. El rango de puertos no está restringido en el código. ● El puerto está habilitado de forma predeterminada durante la instalación: Sí ● ¿El puerto está habilitado después del refuerzo de seguridad?: Sí

Puertos comunes de ZooKeeper

El tipo de protocolo de todos los puertos de la tabla es TCP.

Parámetro	Puerto de código abierto predeterminado	Puerto personalizado predeterminado	Descripción de puertos
clientPort	2181	24002	Puerto de cliente de ZooKeeper Este puerto se utiliza para: Conexión entre el cliente y el servidor de ZooKeeper. **NOTA** El ID de puerto es un valor recomendado y se especifica en función del producto. El rango de puertos no está restringido en el código. ● El puerto está habilitado de forma predeterminada durante la instalación: Sí ● ¿El puerto está habilitado después del refuerzo de seguridad?: Sí

Puertos comunes de Kerberos

El tipo de protocolo de todos los puertos de la tabla es UDP.

Parámetro	Puerto predeterminado	Descripción de puertos
kdc_ports	21732	Puerto de servidor de Kerberos Este puerto se utiliza para: Realización de autenticación de Kerberos para componentes. Este parámetro puede usarse durante la configuración de confianza mutua entre clústeres. **NOTA** El ID de puerto es un valor recomendado y se especifica en función del producto. El rango de puertos no está restringido en el código. ● El puerto está habilitado de forma predeterminada durante la instalación: Sí ● ¿El puerto está habilitado después del refuerzo de seguridad?: Sí

Puertos comunes de OpenTSDB

El tipo de protocolo del puerto de la tabla es TCP.

Parámetro	Puerto predeterminado	Descripción de puertos
tsd.network.port	4242	Puerto de Web UI de OpenTSDB Este puerto se utiliza para: comunicación de HTTPS/HTTP entre las solicitudes de web y el servidor de OpenTSDB UI

Puertos comunes de Tez

El tipo de protocolo del puerto de la tabla es TCP.

Parámetro	Puerto predeterminado	Descripción de puertos
tez.ui.port	28888	Puerto de Web UI de Tez

Puertos comunes de KafkaManager

El tipo de protocolo del puerto de la tabla es TCP.

Parámetro	Puerto predeterminado	Descripción de puertos
kafka_manager_port	9099	Puerto de Web UI de KafkaManager

Puertos comunes de Presto

El tipo de protocolo del puerto de la tabla es TCP.

Parámetro	Puerto predeterminado	Descripción de puertos
http-server.http.port	7520	Puerto de HTTP para que Presto coordinator proporcione servicios a sistemas externos
http-server.https.port	7521	Puerto de HTTPS para que Presto coordinator proporcione servicios a sistemas externos
http-server.http.port	7530	Puerto de HTTP para que Presto worker proporcione servicios a sistemas externos
http-server.https.port	7531	Puerto HTTPS para que Presto worker proporcione servicios a sistemas externos

Puertos comunes de Flink

El tipo de protocolo del puerto de la tabla es TCP.

Parámetro	Puerto predeterminado	Descripción de puertos
jobmanager.web.port	32261-32325	Puerto de Web UI de Flink Este puerto se utiliza para: comunicación de HTTP/HTTPS entre las solicitudes de Client Web y Flink server

Puertos comunes de ClickHouse

El tipo de protocolo del puerto de la tabla es TCP.

Parámetro	Puerto de código abierto predeterminado	Puerto personalizado predeterminado	Descripción de puertos
tcp_port	9000	21423	Puerto TCP para acceder al cliente de servicio

Parámetro	Puerto de código abierto predeterminado	Puerto personalizado predeterminado	Descripción de puertos
http_port	8123	21421	Puerto HTTP para acceder al cliente de servicio
https_port	8443	21422	Puerto HTTPS para acceder al cliente de servicio
tcp_port_secure	9440	21427	Puerto de TCP With SSL para acceder al cliente de servicio. Este puerto solo está habilitado en modo de seguridad de forma predeterminada.

Puertos comunes de Impala

El tipo de protocolo del puerto de la tabla es TCP.

Parámetro	Puerto predeterminado	Descripción de puertos
--beeswax_port	21000	Puerto para comunicación de impala-shell
--hs2_port	21050	Puerto para comunicación de aplicaciones de Impala
--hs2_http_port	28000	Puerto utilizado por Impala para proporcionar el protocolo de HiveServer2 para sistemas externos

5.3 Acceso a través de Direct Connect

MRS le permite acceder a los clústeres MRS mediante Direct Connect. Direct Connect es una conexión de red dedicada de alta velocidad, baja latencia, estable y segura que conecta su centro de datos local a una VPC en la nube en línea. Amplía los servicios en la nube en línea y las instalaciones de IT existentes para crear un entorno de computación en la nube híbrida flexible y escalable.

Prerrequisitos

Direct Connect está disponible y se ha establecido la conexión entre el centro de datos local y la VPC en línea. Para obtener más información, consulte **¿Qué es Direct Connect?**

Acceso a un clúster MRS mediante Direct Connect

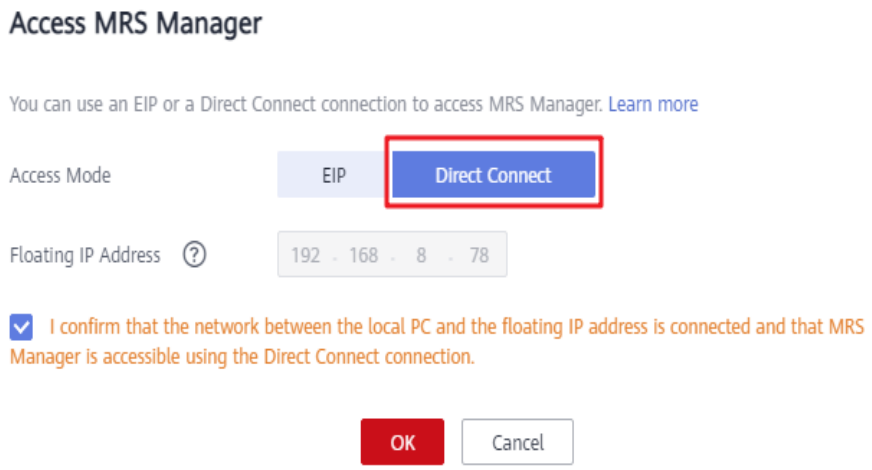
Paso 1 Inicie sesión en la consola de MRS.

Paso 2 Haga clic en el nombre del clúster para ingresar su página de detalles.

Paso 3 En la página de la pestaña **Dashboard** de la página de detalles del clúster, haga clic en **Access Manager** junto a **MRS Manager**.

Paso 4 Establezca **Access Mode** a **Direct Connect** y seleccione **I confirm that the network between the local PC and the floating IP address is connected and that MRS Manager is accessible using the Direct Connect connection**.

MRS asigna automáticamente la dirección IP flotante para acceder a MRS Manager. Antes de utilizar Direct Connect para acceder a MRS Manager, asegúrese de que se ha establecido la conexión entre el centro de datos local y la VPC en línea.



Paso 5 Haga clic en **OK**. Se muestra la página de inicio de sesión de MRS Manager. Introduzca el nombre de usuario **admin** y la contraseña establecida durante la creación del clúster.

----Fin

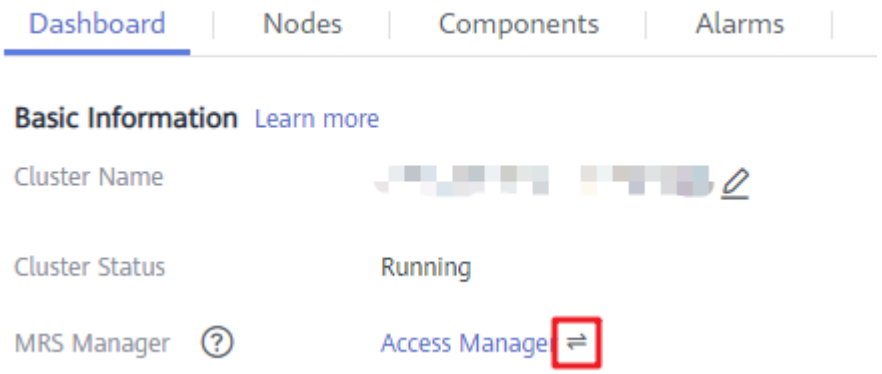
Cambio del modo de acceso de MRS Manager

Para facilitar las operaciones del usuario, la caché del navegador registra el modo de acceso del Manager seleccionado. Para cambiar el modo de acceso, realice los siguientes pasos:

Paso 1 Inicie sesión en la consola de MRS.

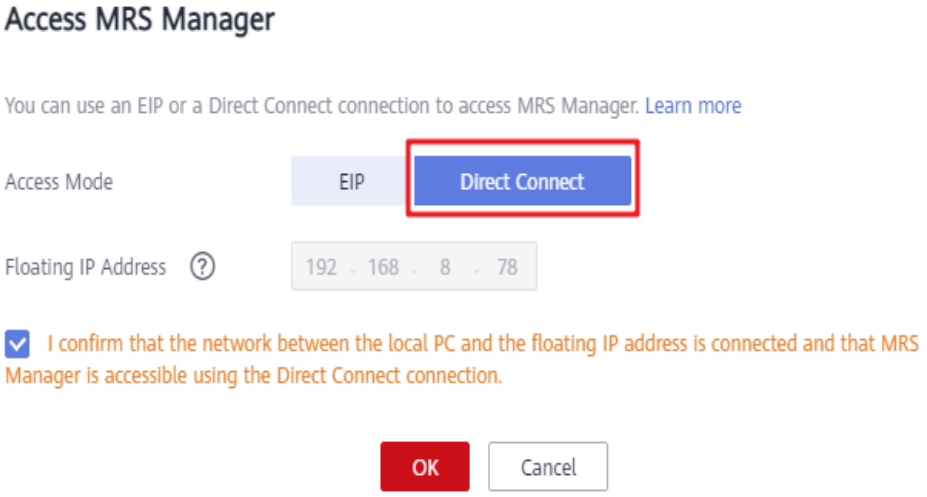
Paso 2 Haga clic en el nombre del clúster para ingresar su página de detalles.

Paso 3 En la página de la pestaña **Dashboard** de la página de detalles del clúster, haga clic en ⇌ junto a **MRS Manager**.



Paso 4 En la página mostrada, defina **Access Mode**.

- Para cambiar **EIP** a **Direct Connect**, asegúrese de que la red para las conexiones directas está disponible, establezca **Access Mode** en **Direct Connect** y seleccione **I confirm that the network between the local PC and the floating IP address is connected and that MRS Manager is accessible using the Direct Connect connection**. Haga clic en **OK**.



- Para cambiar **Direct Connect** a **EIP**, establezca **Access Mode** en **EIP** y configure el EIP haciendo referencia a **Acceder al Manager mediante una EIP**. Si se ha configurado una dirección IP pública para el clúster, haga clic en **OK** para acceder al MRS Manager mediante una EIP.

----Fin

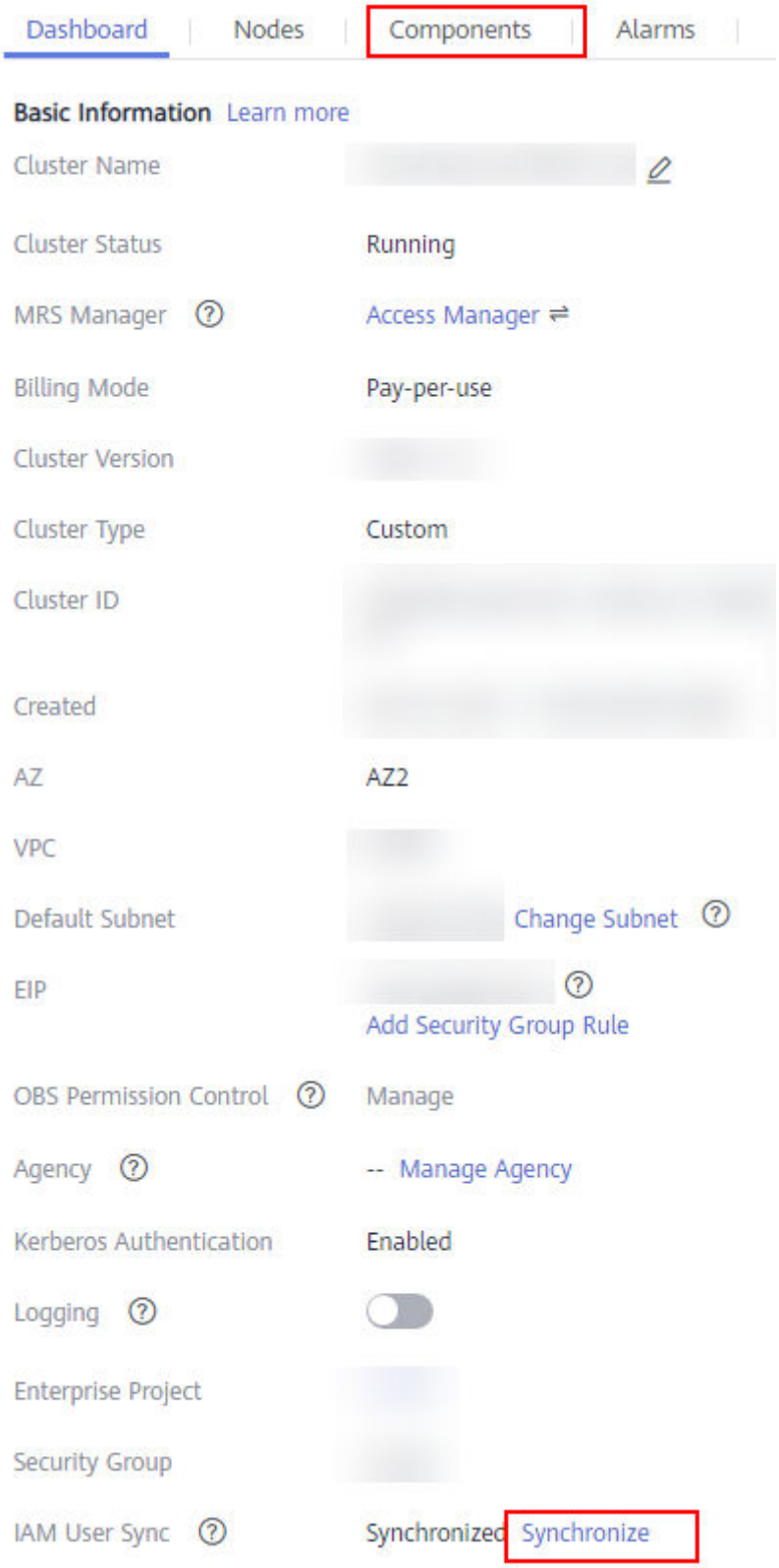
5.4 Acceso basado en EIP

Puede vincular una EIP a un clúster para acceder a las web UIs de los componentes de código abierto gestionados en el clúster MRS. Este método es simple y fácil de usar y se recomienda para acceder a las web UIs de los componentes de código abierto.

Vinculación de una EIP a un clúster y adición de una regla de grupo de seguridad

1. En la página **Dashboard**, haga clic en **Synchronize** en el lado derecho de **IAM User Sync** para sincronizar usuarios de IAM. Después de sincronizar los usuarios de IAM, la pestaña **Components** está disponible.

Figura 5-1 Sincronización de usuarios para acceder a la página de pestaña **Component**



2. Haga clic en **Access Manager** a la derecha de **MRS Manager**.
3. Se muestra la página para acceder a MRS Manager. Vincule una EIP y agregue una regla de grupo de seguridad. Realice las siguientes operaciones solo cuando acceda a las

interfaces de usuario web de los componentes de código abierto del clúster por primera vez.

a. Seleccione una EIP disponible en la lista desplegable de EIP para vincularlo. Si no hay EIP disponible, haga clic en **Manage EIP** para una EIP. Si una EIP se ha enlazado durante la creación del clúster, omita este paso.

b. Seleccione el grupo de seguridad al que pertenece la regla de grupo de seguridad que se va a agregar. El grupo de seguridad se configura cuando se crea el grupo.

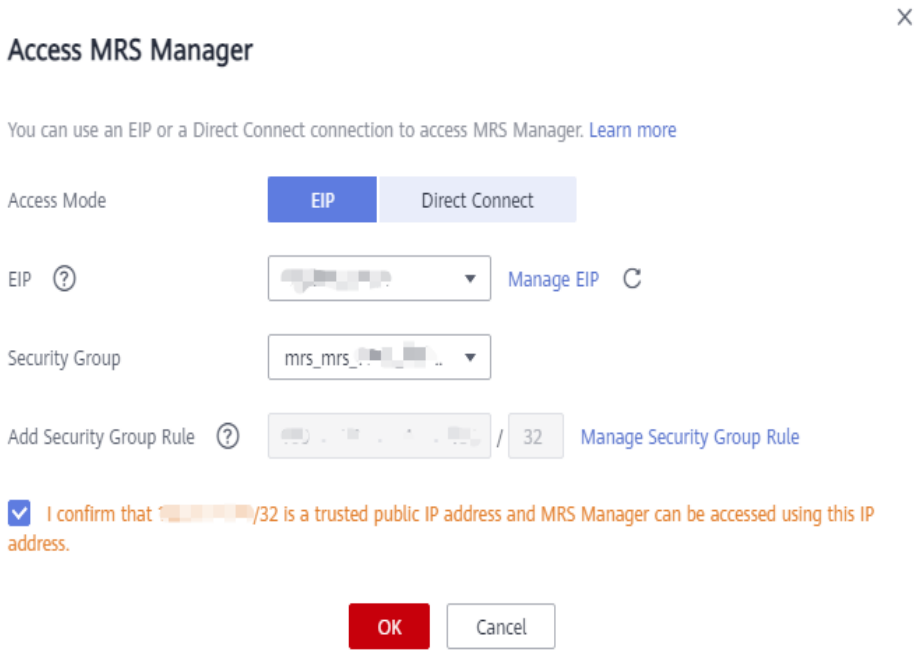
c. Agregue una regla de grupo de seguridad. De forma predeterminada, la dirección IP pública utilizada para acceder al puerto 9022 se completa en la regla. Si desea ver, modificar o eliminar una regla de grupo de seguridad, haga clic en **Manage Security Group Rule**.

NOTA

- Es normal que la dirección IP pública generada automáticamente sea diferente de la dirección IP local y no se requiera ninguna acción.
- Si el puerto 9022 es un puerto Knox, debe habilitar el permiso del puerto 9022 para acceder a Knox para acceder a los componentes de MRS.

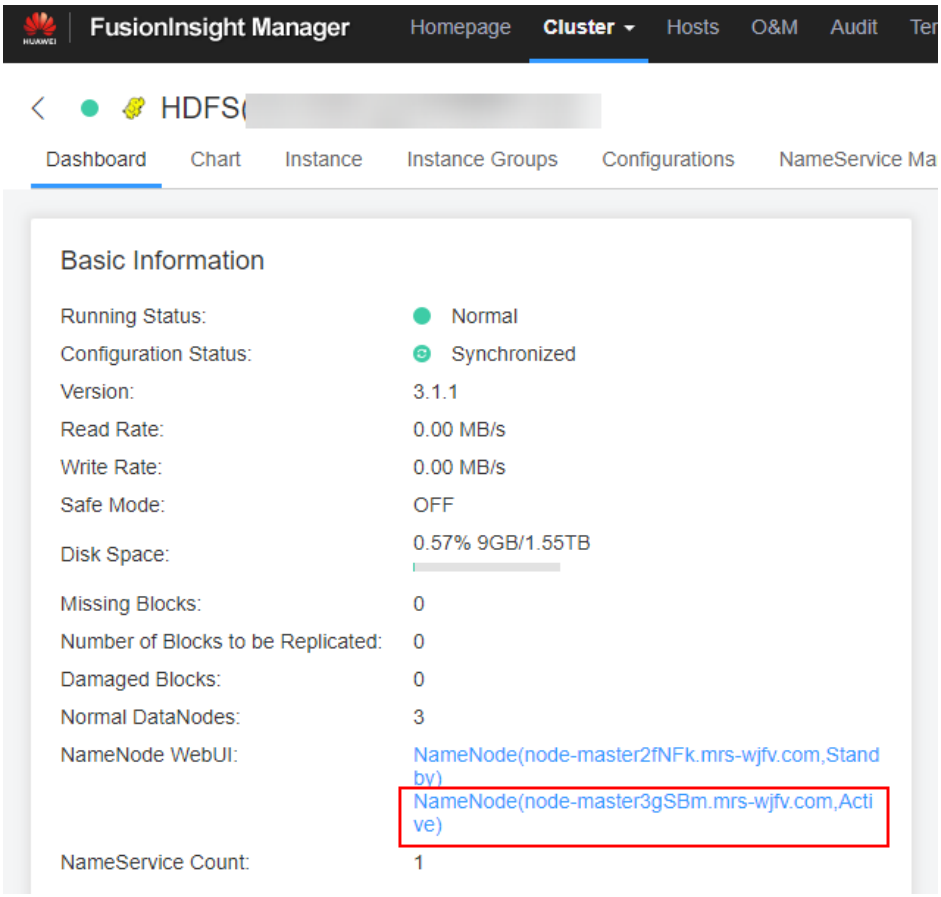
d. Marque la casilla de verificación que indica que **I confirm that xx.xx.xx.xx is a trusted public IP address and MRS Manager can be accessed using this IP address**.

Figura 5-2 Cómo acceder a MRS Manager



e. Haga clic en **OK**. Se muestra la página de inicio de sesión. Introduzca el nombre de usuario **admin** y la contraseña establecida durante la creación del clúster.

4. Inicie sesión en FusionInsight Manager y elija **Cluster** > **Services** > **HDFS**. En la página mostrada, haga clic en **NameNode(***Host name***, active)** para acceder a la web UI de HDFS. El NameNode de HDFS se utiliza como ejemplo. Para obtener más información sobre las web UI de otros componentes, consulte **Interfaz de usuario web de componentes de código abierto**.



5.5 Acceso mediante un ECS de Windows

MRS le permite acceder a las interfaces de usuario web de los componentes de código abierto a través de un ECS de Windows. Este método es complejo y se recomienda para clústeres MRS que no soportan la función EIP.

Paso 1 En la consola de gestión de MRS, haga clic en **Clusters**.

Paso 2 En la página **Active Clusters**, haga clic en el nombre del clúster especificado.

En la página de detalles del clúster, registre el **AZ**, **VPC**, **Cluster Manager IP Address** y **Security Group** del clúster.

NOTA

Para obtener la dirección IP del administrador del clúster, inicie sesión de forma remota en el nodo Master2 y ejecute el comando **ifconfig**. En la salida del comando, **eth0:wsom** indica la dirección IP del administrador del clúster. Registre el valor de **inet**. Si no se puede consultar la dirección IP del administrador de clústeres en el nodo Master2, cambie al nodo Master1 para consultar y registrar la dirección IP del administrador de clústeres. Si solo hay un nodo de Master, consulte y registre la dirección IP del administrador de clústeres del nodo de Master.

Paso 3 En la consola de gestión de ECS, cree un ECS.

- El **AZ**, **VPC** y **Security Group** del ECS deben ser los mismos que los del clúster al que se accede.
- Seleccione una imagen pública de Windows. Por ejemplo, seleccione la imagen estándar **Windows Server 2012 R2 Standard 64bit(40GB)**.

- Para obtener más información sobre otros parámetros de configuración, consulte **Compra de un ECS**.

  NOTA

  Si el grupo de seguridad del ECS es diferente de **Security Group** del clúster MRS, puede modificar la configuración mediante cualquiera de los métodos siguientes:

  - Cambie el grupo de seguridad del ECS al grupo de seguridad del clúster MRS. Para obtener más información, consulte **Cambio de un grupo de seguridad**.
  - Agregue dos reglas de grupo de seguridad a los grupos de seguridad de los nodos de Master y Core para permitir que el ECS tenga acceso al clúster. Establezca **Protocol** en **TCP** y **ports** de las dos reglas de grupo de seguridad en **28443** y **20009** respectivamente. Para obtener más información, consulte **Creación de un grupo de seguridad**.

Paso 4 En la consola de gestión de VPC, solicite una EIP y vincúlela al ECS.

Para obtener más información, consulte **Asignación de un EIP**.

Paso 5 Inicie sesión en el ECS.

La cuenta del sistema de Windows, la contraseña, la EIP y las reglas del grupo de seguridad son necesarias para iniciar sesión en el ECS. Para obtener más información, consulte **Iniciar sesión en un ECS de Windows**.

Paso 6 En el escritorio remoto de Windows, utilice el navegador para acceder al Manager.

La dirección de acceso de MRS Manager tiene el formato de **https://*Cluster Manager IP Address*:28443/web**. Introduzca el nombre y la contraseña del usuario del clúster MRS, por ejemplo, usuario **admin**.

NOTA

- Para obtener la dirección IP del administrador del clúster, inicie sesión de forma remota en el nodo Master2 y ejecute el comando **ifconfig**. En la salida del comando, **eth0:wsom** indica la dirección IP del administrador del clúster. Registre el valor de **inet**. Si no se puede consultar la dirección IP del administrador de clústeres en el nodo Master2, cambie al nodo Master1 para consultar y registrar la dirección IP del administrador de clústeres. Si solo hay un nodo de Master, consulte y registre la dirección IP del administrador de clústeres del nodo de Master.
- Si accede a MRS Manager con otros nombres de usuario del clúster de MRS, cambie la contraseña en su primer acceso. La nueva contraseña debe cumplir los requisitos de las políticas de complejidad de contraseñas actuales.
- De forma predeterminada, un usuario se bloquea después de introducir una contraseña incorrecta cinco veces consecutivas. El usuario se desbloquea automáticamente después de 5 minutos.

Paso 7 Visite las interfaces de usuario web de los componentes de código abierto haciendo referencia a las direcciones enumeradas en **Interfaz de usuario web de componentes de código abierto**.

----Fin

Tareas relacionadas

Configuración de la asignación entre nombres de nodos de clúster y direcciones IP

Paso 1 Inicie sesión en MRS Manager y elija **Host Management**.

Registre los nombres de host y las direcciones IP de gestión de todos los nodos del clúster.

Paso 2 En el entorno de trabajo, utilice el Bloc de notas para abrir el archivo **hosts** y agregar la asignación entre nombres de nodo y direcciones IP al archivo.

Rellene una fila para cada relación de asignación, como se muestra en la siguiente figura.

```
192.168.4.127 node-core-Jh3ER
192.168.4.225 node-master2-PaWVE
192.168.4.19 node-core-mtZ81
192.168.4.33 node-master1-zbYN8
192.168.4.233 node-core-7KoGY
```

Guarde las modificaciones.

----Fin

5.6 Creación de un canal de SSH para conectarse a un clúster de MRS y configurar el navegador

Escenario

Los usuarios y un clúster MRS están en redes diferentes. Como resultado, se necesita crear un canal SSH para enviar las solicitudes de los usuarios para acceder a sitios web al clúster MRS y reenviarlos dinámicamente a los sitios web de destino.

El sistema MAC no admite esta función. Para obtener más información sobre cómo acceder a MRS, consulte **Acceso basado en EIP**.

Prerrequisitos

- Ha preparado un cliente SSH para crear el canal SSH, por ejemplo, el cliente SSH de código abierto Git. Ha descargado e instalado el cliente.
- Ha creado un clúster y ha preparado un archivo de clave en formato PEM u obtenido la contraseña utilizada durante la creación del clúster.
- Los usuarios pueden acceder a Internet en el PC local.

Procedimiento

Paso 1 Inicie sesión en la consola de gestión de MRS y elija **Clusters** > **Active Clusters**.

Paso 2 Haga clic en el nombre del clúster de MRS especificado.

Registre el grupo de seguridad del clúster.

Paso 3 Agregue una regla de entrada al grupo de seguridad del nodo de Master para permitir el acceso de datos a la dirección IP del clúster MRS a través del **22** de puerto.

Para obtener más información, consulte **Adición de regla de grupo de seguridad**.

Paso 4 Consulte el nodo de gestión principal del clúster. Para obtener más información, consulte **Determinación de nodos de gestión activos y en espera**.

Paso 5 Vincule una dirección IP elástica al nodo de gestión principal.

Para obtener más información, consulte **Asignación de un EIP**.

Paso 6 Inicie Git Bash localmente y ejecute el siguiente comando para iniciar sesión en el nodo de gestión activo del clúster: **ssh root@*Elastic IP address*** or **ssh -i *Path of the key file* root@*Elastic IP address***.

Paso 7 Ejecute el siguiente comando para ver las configuraciones de reenvío de datos:

cat /etc/sysctl.conf | grep net.ipv4.ip_forward

- Si se muestra **net.ipv4.ip_forward=1**, se ha configurado la función de reenvío. Vaya a **Paso 9**.
- Si se muestra **net.ipv4.ip_forward=0**, la función de reenvío no se ha configurado. Vaya a **Paso 8**.
- Si **net.ipv4.ip_forward** no se puede consultar, este parámetro no se ha configurado. Ejecute el siguiente comando y, a continuación, vaya a **Paso 9**:

  echo "net.ipv4.ip_forward = 1" >> /etc/sysctl.conf

Paso 8 Modifique las configuraciones de reenvío en el nodo.

1. Ejecute el siguiente comando para cambiar a usuario **root**:

   sudo su - root

2. Ejecute los siguientes comandos para modificar las configuraciones de reenvío:

   echo 1 > /proc/sys/net/ipv4/ip_forward

   sed -i "s/net.ipv4.ip_forward=0/net.ipv4.ip_forward = 1/g" /etc/sysctl.conf

   sysctl -w net.ipv4.ip_forward=1

3. Ejecute el siguiente comando para modificar el archivo de configuración **sshd**:

   vi /etc/ssh/sshd_config

   Pulse **I** para entrar en el modo de edición. Localice **AllowTcpForwarding** y **GatewayPorts** y elimine las etiquetas de comentarios. Modifíquelos de la siguiente manera. Guarde los cambios y salga.

   ```
   AllowTcpForwarding yes
   GatewayPorts yes
   ```

4. Ejecute el siguiente comando para reiniciar el servicio sshd:

   service sshd restart

Paso 9 Ejecute el siguiente comando para ver la dirección IP flotante:

ifconfig

En la salida del comando, **eth0:FI_HUE** indica la dirección IP flotante de Hue y **eth0:wsom** especifica la dirección IP flotante de Manager. Registre el valor de **inet**.

Ejecute el comando **exit** para salir.

Paso 10 Ejecute el siguiente comando en el PC local para crear un canal de SSH que admita el reenvío dinámico de puertos:

ssh -i *Path of the key file* -v -ND *Local port* root@*Elastic IP address* or ***ssh -v -ND Local port root@Elastic IP address***. Después de ejecutar el comando, escriba la contraseña que estableció al crear el clúster.

En el comando, establezca **Local port** en el puerto local del usuario que no está ocupado. Se recomienda el puerto **8157**.

Después de crear el canal de SSH, agregue **-D** al comando y ejecute el comando para iniciar la función de reenvío dinámico de puertos. De forma predeterminada, la función de reenvío dinámico de puertos habilita un proceso de proxy SOCKS y monitorea el puerto local del usuario. Los datos del puerto se reenviarán al nodo de gestión primario utilizando el canal de SSH.

Paso 11 Ejecute el siguiente comando para configurar el proxy del navegador.

1. Vaya al directorio de instalación del cliente de Google Chrome en el PC local.
2. Presione **Shift** y haga clic con el botón derecho en el área en blanco, elija **Open Command Window Here** e introduzca el siguiente comando:

   chrome --proxy-server="socks5://localhost:8157" --host-resolver-rules="MAP * 0.0.0.0 , EXCLUDE localhost" --user-data-dir=c:/tmppath --proxy-bypass-list="*google*com,*gstatic.com,*gvt*.com,*:80"

   NOTA

   - En el comando anterior, **8157** es el puerto de proxy local configurado en **Paso 10**.
   - Si el sistema operativo local es Windows 10, inicie el Windows OS, haga clic en **Start** y escriba **cmd**. En la CLI mostrada, ejecute el comando en **Paso 11.2**. Si este método falla, haga clic en **Start**, escriba el comando en el cuadro de búsqueda y ejecute el comando de **Paso 11.2**.

Paso 12 En el cuadro de dirección del navegador, introduzca la dirección para acceder al Manager.

Formato de dirección: **https://***Floating IP address of FusionInsight Manager***:28443/web**

Es necesario introducir el nombre de usuario y la contraseña del clúster de MRS para acceder a clústeres con autenticación de Kerberos habilitada, por ejemplo, usuario **admin**. No son necesarios para acceder a clústeres con la autenticación de Kerberos deshabilitada.

Cuando acceda a Manager por primera vez, debe agregar la dirección a la lista de sitios de confianza.

Paso 13 Preparar la dirección de acceso al sitio web.

1. Obtenga el formato de dirección del sitio web y la instancia de rol según **Web UIs**.
2. Haga clic en **Services**.
3. Haga clic en el nombre del servicio especificado, por ejemplo, HDFS.
4. Haga clic en **Instance** y vea **Service IP Address** de **NameNode(Active)**.

Paso 14 En la barra de direcciones del navegador, introduzca la dirección del sitio web para acceder a ella.

Paso 15 Al cerrar la sesión del sitio web, termine y cierre el túnel de SSH.

----Fin

6 Acceder a Manager

6.1 Acceder a FusionInsight Manager (MRS 3.*x* o posterior)

Escenario

En MRS 3.*x* o posterior, FusionInsight Manager se utiliza para monitorear, configurar y gestionar clústeres. Después de instalar el clúster, puede utilizar la cuenta para iniciar sesión en FusionInsight Manager.

Actualmente, puede acceder al FusionInsight Manager utilizando los siguientes métodos:

- **Acceder al FusionInsight Manager mediante EIP**
- **Acceder al FusionInsight Manager mediante Direct Connect**
- **Acceder al FusionInsight Manager desde un ECS**

Puede cambiar los métodos de acceso entre **EIP** y **Direct Connect** en la consola MRS realizando los siguientes pasos:

Inicie sesión en la consola de gestión de MRS y haga clic en el clúster deseado. En la página mostrada, haga clic en ⇌ junto a **MRS Manager** en la pestaña **Dashboard** y cambie el método de acceso.

NOTA

Si no puede iniciar sesión en el WebUI del componente, acceda al FusionInsight Manager haciendo referencia a **Acceso al FusionInsight Manager desde un ECS**.

No se puede acceder al FusionInsight Manager cuando el clúster se encuentra en cualquiera de los siguientes estados:

Starting, Stopping, Stopped, Deleting, Deleted, and Frozen.

Acceder a FusionInsight Manager mediante EIP

Si la función de dirección EIP está habilitada para el clúster, realice los siguientes pasos:

Paso 1 Inicie sesión en la consola de gestión de MRS.

Paso 2 En el panel de navegación, elija **Clusters** >**Active Clusters**. Haga clic en el nombre del clúster de destino para acceder a la página de detalles del clúster.

Paso 3 Haga clic en **Manager** junto a **MRS Manager**. En el cuadro de diálogo que aparece, configure la información de EIP.

1. Si no hay ninguna EIP enlazada durante la creación del clúster de MRS, seleccione una EIP disponible en la lista desplegable situada a la derecha de **IEP**. Si ha enlazado un EIP al crear un clúster, vaya a **Paso 3.2**.

   NOTA

   - Si no hay EIP disponibles, haga clic en **Manage EIP** para uno. A continuación, seleccione la EIP de la lista desplegable.
   - Para desvincular o liberar un EIP después de usarlo, inicie sesión en la página **EIPs**, busque la fila que contiene el EIP de destino y haga clic en **Unbind** o elija **More** > **Release** en la columna **Operation**.
   - Si se ha creado una EIP pero no se puede encontrar durante la vinculación, la EIP puede haber estado vinculada a otra agrupación. En este caso, desvincule el EIP en la página **EIPs** y luego enlíquelo al clúster actual.

2. En el **Security Group**, seleccione el grupo de seguridad al que pertenece el clúster actual. El grupo de seguridad se configura durante la creación del clúster o se crea automáticamente por el clúster.

   NOTA

   - Al crear un clúster personalizado, puede configurar un grupo de seguridad creado de antemano o conservar el valor predeterminado **Auto create**. Cuando se crea rápidamente un clúster, el clúster crea automáticamente el grupo de seguridad.
   - Puede ver el nombre del grupo de seguridad en **Security Group** en la página de pestaña **Dashboard** del clúster.

3. Agregue una regla de grupo de seguridad. Por defecto, la regla completada se utiliza para acceder al EIP. Para habilitar varios segmentos de direcciones IP para acceder al Manager, consulte los pasos **Paso 6** a **Paso 9**. Si desea ver, modificar o eliminar una regla de grupo de seguridad, haga clic en **Manage Security Group Rule**.
4. Seleccione la información que desea confirmar y haga clic en **OK**.

   NOTA

   Haga clic en ⇌ a la derecha de **Access Manager** para cambiar el modo de acceso del FusionInsight Manager. Para obtener más información acerca de cómo acceder al FusionInsight Manager mediante **Direct Connect**, consulte **Acceso al FusionInsight Manager mediante Direct Connect**.

Paso 4 Haga clic en **OK**. Se muestra la página de inicio de sesión de Manager.

Paso 5 Ingrese el nombre de usuario predeterminado **admin** y el conjunto de contraseñas durante la creación del clúster, y haga clic en **Log In**. Se muestra la página de Manager.

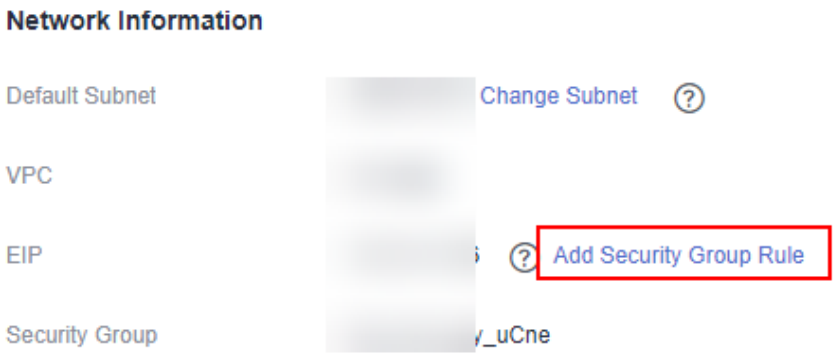
Paso 6 En la consola de gestión de MRS, elija **Clusters** > **Active Clusters**. Haga clic en el nombre del clúster de destino para acceder a la página de detalles del clúster.

NOTA

Para conceder a otros usuarios el permiso de acceso al Manager, realice **Paso 6** a **Paso 9** para agregar las direcciones IP públicas de los usuarios al intervalo de direcciones IP de confianza.

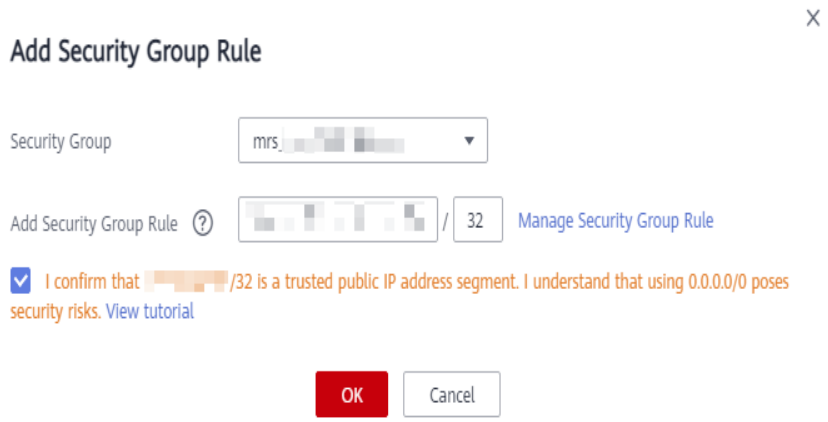
Paso 7 Haga clic en **Add Security Group Rule** junto a **EIP**.

Figura 6-1 Detalles del clúster



Paso 8 En la página **Add Security Group Rule**, agregue el segmento de direcciones IP para que los usuarios accedan a la red pública y seleccione **I confirm that *public network IP*/*port* is a trusted public IP address. I understand that using 0.0.0.0/0. poses security risks**. Consulte **Figura 6-2**.

Figura 6-2 Adición de una regla de grupo de seguridad



De forma predeterminada, se rellena la dirección IP utilizada para acceder a la red pública. Puede cambiar el segmento de dirección IP según sea necesario. Para habilitar varios segmentos de direcciones IP, repita los pasos **Paso 6** a **Paso 9**. Si desea ver, modificar o eliminar una regla de grupo de seguridad, haga clic en **Manage Security Group Rule**.

Paso 9 Haga clic en **OK**.

----Fin

Acceso al FusionInsight Manager mediante Direct Connect

Debe asegurarse de que Direct Connect esté disponible y de que se haya establecido la conexión entre el centro de datos local y la VPC en línea. Para obtener más información, consulte **¿Qué es Direct Connect?**

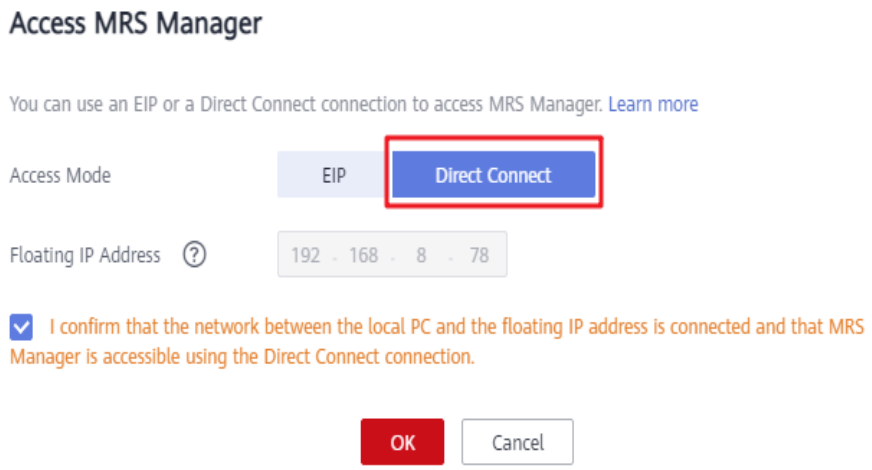
Paso 1 Inicie sesión en la consola de MRS.

Paso 2 Haga clic en el nombre del clúster para ingresar su página de detalles.

Paso 3 En la página de la pestaña **Dashboard** de la página de detalles del clúster, haga clic en **Access Manager** junto a **MRS Manager**.

Paso 4 Establezca **Access Mode** a **Direct Connect** y seleccione **I confirm that the network between the local PC and the floating IP address is connected and that MRS Manager is accessible using the Direct Connect connection**.

MRS asigna automáticamente la dirección IP flotante para acceder a MRS Manager. Antes de utilizar Direct Connect para acceder a MRS Manager, asegúrese de que se ha establecido la conexión entre el centro de datos local y la VPC en línea.



Paso 5 Haga clic en **OK**. Se muestra la página de inicio de sesión de MRS Manager. Introduzca el nombre de usuario **admin** y la contraseña establecida durante la creación del clúster.

----Fin

Acceso al FusionInsight Manager desde un ECS

Paso 1 En la consola de gestión de MRS, haga clic en **Clusters**.

Paso 2 En la página **Active Clusters**, haga clic en el nombre del clúster especificado.

Registre **AZ**, **VPC**, **MRS ManagerSecurity Group** del clúster.

Paso 3 En la página principal de la consola de gestión, elija **Service List** > **Elastic Cloud Server** para cambiar a la consola de gestión de ECS y crear un ECS.

- El **AZ**, **VPC** y **Security Group** del ECS deben ser los mismos que los del clúster al que se accede.
- Seleccione una imagen pública de Windows. Por ejemplo, una imagen estándar **Windows Server 2012 R2 Standard 64bit(40GB)**.
- Para obtener más información sobre otros parámetros de configuración, consulte **Compra de un ECS con configuraciones personalizadas**.

NOTA

Si el grupo de seguridad del ECS es diferente de **Default Security Group** del nodo Master, puede modificar la configuración utilizando cualquiera de los métodos siguientes:

- Cambie el grupo de seguridad del ECS al grupo de seguridad predeterminado del nodo Master. Para obtener más información, consulte **Cambio de un grupo de seguridad**.
- Agregue dos reglas de grupo de seguridad a los grupos de seguridad de los nodos de Master y Core para permitir que el ECS tenga acceso al clúster. Establezca **Protocol** en **TCP**, **Ports** de las dos reglas de grupo de seguridad en **28443** y **20009** respectivamente. Para obtener más información, consulte **Creación de un grupo de usuario**.

Si aparece "Failed to add security group rules.", compruebe si la cuota de grupo de seguridad es suficiente. Si se necesitan más cuotas, aumente las cuotas o elimine las reglas de grupo de seguridad que ya no se utilicen.

Paso 4 En la consola de gestión de VPC, solicite una EIP y vincúlela al ECS.

Para obtener más información, consulte **Asignación de un EIP**.

Paso 5 Inicie sesión en el ECS.

La cuenta del sistema de Windows, la contraseña, la EIP y las reglas del grupo de seguridad son necesarias para iniciar sesión en el ECS. Para obtener más información, consulte **Iniciar sesión en un Windows ECS**.

Paso 6 En el escritorio remoto de Windows, utilice el navegador para acceder al Manager.

La dirección para acceder al Manager es la dirección de la página **MRS Manager**. Introduzca el nombre y la contraseña del usuario del clúster, por ejemplo, usuario **admin**.

NOTA

- Si accede a Manager con otros nombres de usuario del clúster, cambie la contraseña en el primer acceso. La nueva contraseña debe cumplir los requisitos de las políticas de complejidad de contraseñas actuales. Para obtener más información, póngase en contacto con el administrador.
- De forma predeterminada, un usuario se bloquea después de introducir una contraseña incorrecta cinco veces consecutivas. El usuario se desbloquea automáticamente después de 5 minutos.

Paso 7 Cierre la sesión del FusionInsight Manager. Para cerrar la sesión en Manager, mueva el cursor a en la esquina superior derecha y haga clic en **Log Out**.

----Fin

6.2 Acceso a MRS Manager (MRS 2.*x* o anterior)

Escenario

MRS utiliza Manager para supervisar, configurar y gestionar clústeres. Puede acceder al Administrador haciendo clic en **Access Manager** en la página de pestaña **Dashboard** del clúster MRS e ingresando el nombre de usuario **admin** y la contraseña configurada durante la creación del clúster en la página de inicio de sesión que se muestra.

NOTA

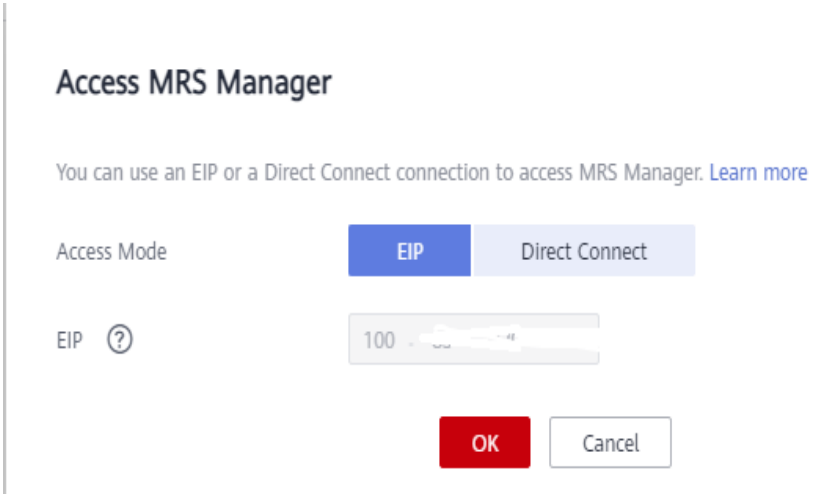
No se puede acceder al Manager cuando el clúster se encuentra en cualquiera de los siguientes estados: Starting, Stopping, Stopped, Deleting, Deleted, y Frozen.

Acceder al Manager mediante una EIP

Paso 1 Inicie sesión en la consola de gestión de MRS.

Paso 2 En el panel de navegación, elija **Clusters** >**Active Clusters**. Haga clic en el nombre del clúster de destino para acceder a la página de detalles del clúster.

Paso 3 Haga clic en **Access Manager** junto a **MRS Manager**. En el cuadro de diálogo que se muestra, establezca **Access Mode** en **EIP**. Para obtener más información acerca de **Direct Connect**, consulte **Acceso a través de Direct Connect**.



1. Si no hay ninguna EIP enlazada durante la creación del clúster de MRS, seleccione una EIP disponible en la lista desplegable situada a la derecha de **IEP**. Si ha enlazado un EIP al crear un clúster, vaya a **Paso 3.2**.

   NOTA

   - Si no hay EIP disponibles, haga clic en **Manage EIP** para uno. A continuación, seleccione la EIP de la lista desplegable.
   - Para desvincular o liberar un EIP después de usarlo, inicie sesión en la página **EIPs**, busque la fila que contiene el EIP de destino y haga clic en **Unbind** o elija **More** > **Release** en la columna **Operation**.
   - Si se ha creado una EIP pero no se puede encontrar durante la vinculación, la EIP puede haber estado vinculada a otra agrupación. En este caso, desvincule el EIP en la página **EIPs** y luego vincúlelo al clúster actual.

2. En el **Security Group**, seleccione el grupo de seguridad al que pertenece el clúster actual. El grupo de seguridad se configura durante la creación del clúster o se crea automáticamente por el clúster.

   NOTA

   - Al crear un clúster personalizado, puede configurar un grupo de seguridad creado de antemano o conservar el valor predeterminado **Auto create**. Cuando se crea rápidamente un clúster, el clúster crea automáticamente el grupo de seguridad.
   - Puede ver el nombre del grupo de seguridad en **Security Group** en la página de pestaña **Dashboard** del clúster.

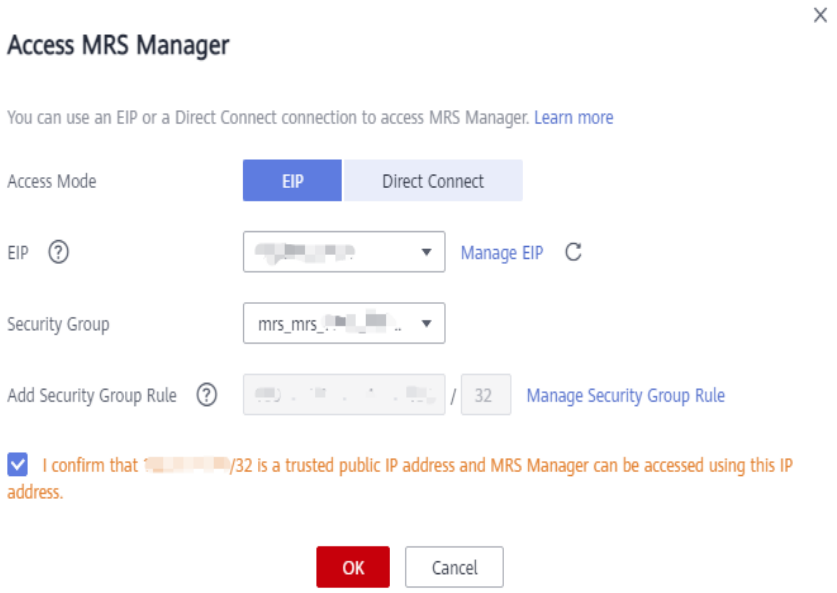
3. Agregue una regla de grupo de seguridad. De forma predeterminada, la dirección IP pública utilizada para acceder al puerto 9022 se completa en la regla. Para habilitar varios segmentos de direcciones IP para acceder al MRS Manager, consulte **Paso 6** a **Paso 9**. Si desea ver, modificar o eliminar una regla de grupo de seguridad, haga clic en **Manage Security Group Rule**.

NOTA

- Es normal que la dirección IP pública generada automáticamente sea diferente de la dirección IP local y no se requiera ninguna acción.
- Si el puerto 9022 es un puerto Knox, debe habilitar el permiso del puerto 9022 para acceder a Knox para acceder a MRS Manager.

4. Marque la casilla de verificación que indica que **I confirm that xx.xx.xx.xx is a trusted public IP address and MRS Manager can be accessed using this IP address**.

Figura 6-3 Vinculación de una EIP



Paso 4 Haga clic en **OK**. Aparecerá en pantalla la página de inicio de sesión de MRS Manager.

Paso 5 Ingrese el nombre de usuario predeterminado **admin** y el conjunto de contraseñas durante la creación del clúster, y haga clic en **Log In**. Se muestra la página MRS Manager.

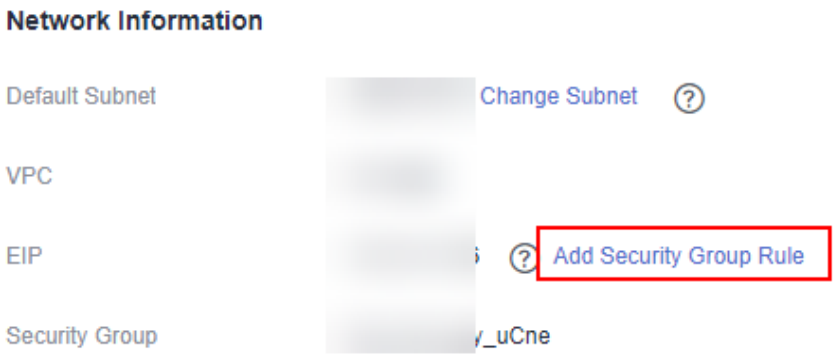
Paso 6 En la consola de gestión de MRS, elija **Clusters** > **Active Clusters** y haga clic en el nombre del clúster de destino para acceder a la página de detalles del clúster.

NOTA

Para asignar permisos de acceso de MRS Manager a otros usuarios, siga las instrucciones de **Paso 6** a **Paso 9** para agregar las direcciones IP públicas de los usuarios al rango de confianza.

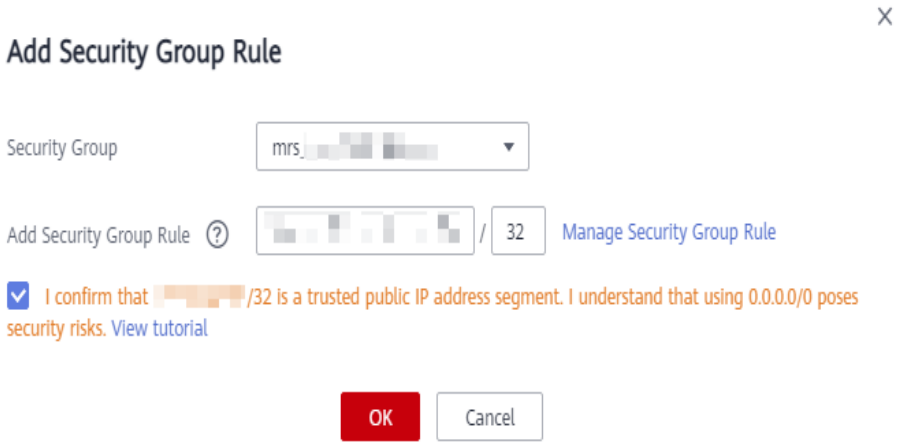
Paso 7 Haga clic en **Add Security Group Rule** junto a **EIP**.

Figura 6-4 Detalles del clúster



Paso 8 En la página **Add Security Group Rule**, agregue el segmento de dirección IP para que los usuarios accedan a la red pública y seleccione **I confirm that the authorized object is a trusted public IP address range. Do not use 0.0.0.0/0. Otherwise, security risks may arise**. Consulte **Figura 6-5**.

Figura 6-5 Incorporación de una regla de grupo de seguridad



De forma predeterminada, se rellena la dirección IP utilizada para acceder a la red pública. Puede cambiar el segmento de dirección IP según sea necesario. Para habilitar varios segmentos de direcciones IP, repita los pasos **Paso 6** a **Paso 9**. Si desea ver, modificar o eliminar una regla de grupo de seguridad, haga clic en **Manage Security Group Rule**.

Paso 9 Haga clic en **OK**.

----Fin

Acceso a MRS Manager usando un ECS

Paso 1 En la consola de gestión de MRS, haga clic en **Clusters**.

Paso 2 En la página **Active Clusters**, haga clic en el nombre del clúster especificado.

Registre el **AZ**, **VPC**, y **Security Group** del clúster.

Paso 3 En la consola de gestión de ECS, cree un ECS.

- El **AZ**, **VPC** y **Security Group** del ECS deben ser los mismos que los del clúster al que se accede.
- Seleccione una imagen pública de Windows. Por ejemplo, seleccione la imagen estándar **Windows Server 2012 R2 Standard 64bit(40GB)**.
- Para obtener más información acerca de otros parámetros de configuración, consulte **Compra de un ECS**.

NOTA

Si el grupo de seguridad del ECS es diferente de **Grupo de seguridad predeterminado** del clúster MRS, puede modificar la configuración mediante cualquiera de los métodos siguientes:

- Cambie el grupo de seguridad predeterminado del ECS al grupo de seguridad del clúster MRS. Para obtener más información, consulte **Cambio de un grupo de seguridad**.
- Agregue dos reglas de grupo de seguridad a los grupos de seguridad de los nodos de Master y Core para permitir que el ECS tenga acceso al clúster. Establezca **Protocol** en **TCP** y **ports** de las dos reglas de grupo de seguridad en **28443** y **20009** respectivamente. Para obtener más información, consulte **Creación de un grupo de seguridad**.

Paso 4 En la consola de gestión de VPC, solicite una EIP y vincúlela al ECS.

Para obtener más información, consulte **Asignación de un EIP**.

Paso 5 Inicie sesión en el ECS.

La cuenta del sistema de Windows, la contraseña, la EIP y las reglas del grupo de seguridad son necesarias para iniciar sesión en el ECS. Para obtener más información, consulte **Iniciar sesión en un Windows ECS**.

Paso 6 En el escritorio remoto de Windows, utilice el navegador para acceder al Manager.

Por ejemplo, puede utilizar Internet Explorer 11 en el Windows 2012 OS.

La dirección de acceso del Manager tiene el formato **https://***Cluster Manager IP Address***:28443/web**. Introduzca el nombre y la contraseña del usuario del clúster MRS, por ejemplo, usuario **admin**.

NOTA

- Para obtener la dirección IP del administrador del clúster, inicie sesión de forma remota en el nodo Master2 y ejecute el comando **ifconfig**. En la salida del comando, **eth0:wsom** indica la dirección IP del administrador del clúster. Registre el valor de **inet**. Si no se puede consultar la dirección IP del administrador de clústeres en el nodo Master2, cambie al nodo Master1 para consultar y registrar la dirección IP del administrador de clústeres. Si solo hay un nodo de Master, consulte y registre la dirección IP del administrador de clústeres del nodo de Master.
- Si accede a MRS Manager con otros nombres de usuario del clúster de MRS, cambie la contraseña en su primer acceso. La nueva contraseña debe cumplir los requisitos de las políticas de complejidad de contraseñas actuales.
- De forma predeterminada, un usuario se bloquea después de introducir una contraseña incorrecta cinco veces consecutivas. El usuario se desbloquea automáticamente después de 5 minutos.

Paso 7 Cierre la sesión del FusionInsight Manager. Para cerrar la sesión en Manager, mueva el cursor a  en la esquina superior derecha y haga clic en **Log Out**.

----Fin

Cambio de una EIP para un clúster

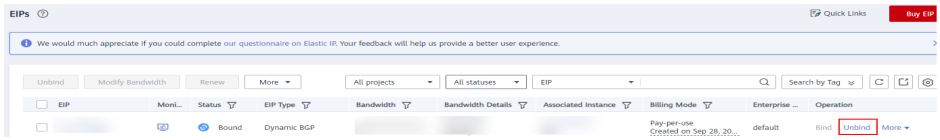
Paso 1 En la consola de gestión de MRS, elija **Clusters** > **Active Clusters** y haga clic en el nombre del clúster de destino para acceder a la página de detalles del clúster.

Paso 2 Ver las EIP

Paso 3 Inicie sesión en la consola de gestión de VPC.

Paso 4 Elija **Elastic IP and Bandwidth** > **EIPs**.

Paso 5 Busque la EIP enlazada al clúster de MRS y haga clic en **Unbind** en la columna **Operation** para desvincular la EIP del clúster de MRS.



Paso 6 Inicie sesión en la consola de gestión de MRS, elija **Clusters** > **Active Clusters** y haga clic en el nombre del clúster de destino para acceder a la página de detalles del clúster.

EIP en la página de detalles del clúster se muestra como **Unbound**.

Paso 7 Haga clic en **Access Manager** junto a **MRS Manager**. En el cuadro de diálogo que se muestra, establezca **Access Mode** en **EIP**.

Paso 8 Seleccione una nueva EIP en la lista desplegable de EIP y configure otros parámetros. Para obtener más información, consulte **Acceder al Manager mediante una EIP**.

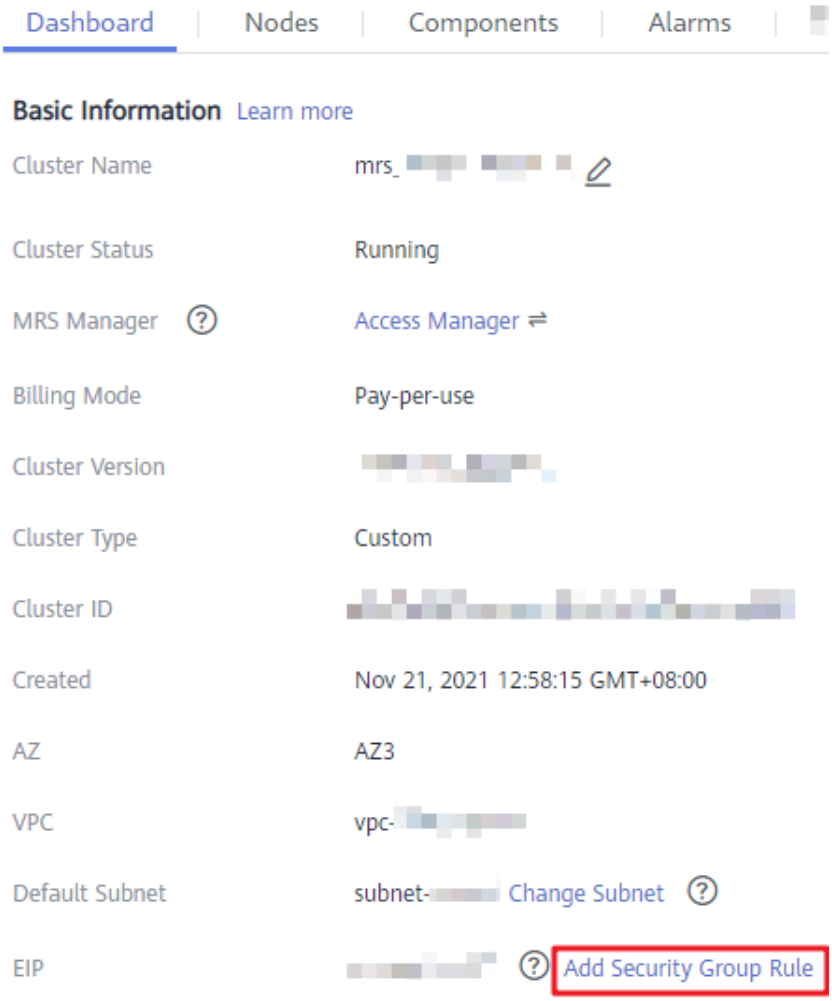
----Fin

Otorgar el permiso para acceder a MRS Manager a otros usuarios

Paso 1 En la consola de gestión de MRS, elija **Clusters** > **Active Clusters** y haga clic en el nombre del clúster de destino para acceder a la página de detalles del clúster.

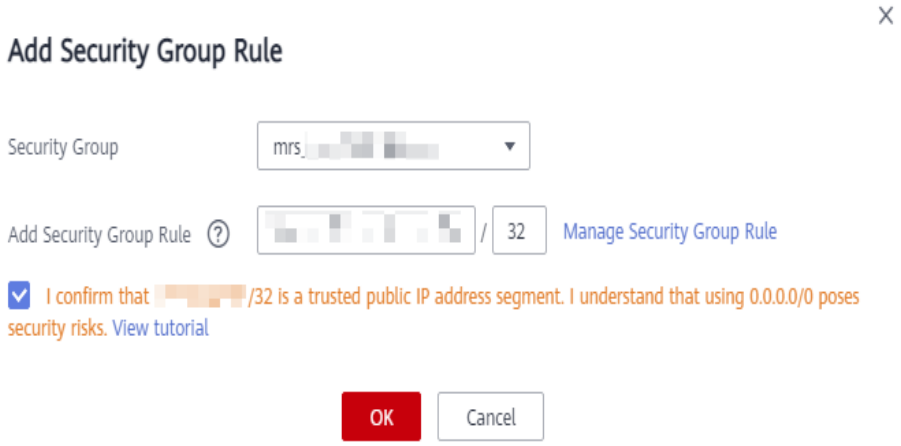
Paso 2 Haga clic en **Add Security Group Rule** a la derecha de **EIP**, como se muestra en **Figura 6-6**.

Figura 6-6 Detalles del clúster



Paso 3 En la página **Add Security Group Rule**, agregue el segmento de dirección IP para que los usuarios accedan a la red pública y seleccione **I confirm that the authorized object is a trusted public IP address range. Do not use 0.0.0.0/0. Otherwise, security risks may arise**. Consulte **Figura 6-7**.

Figura 6-7 Incorporación de una regla de grupo de seguridad



De forma predeterminada, se rellena la dirección IP utilizada para acceder a la red pública. Puede cambiar el segmento de dirección IP según sea necesario. Para habilitar varios segmentos de direcciones IP, repita los pasos **Paso 1** a **Paso 4**. Si desea ver, modificar o eliminar una regla de grupo de seguridad, haga clic en **Manage Security Group Rule**.

Paso 4 Haga clic en **OK**.

----Fin

7 Guía de operación del FusionInsight Manager (aplicable a 3.x)

7.1 Página de inicio

7.1.1 Descripción

Después de iniciar sesión en FusionInsight Manager, se muestra **Homepage** de forma predeterminada. En esta página, la pestaña **Summary** muestra los estados de servicio y los informes de estado de supervisión de cada clúster, y la pestaña **Alarm Analysis** muestra las estadísticas y el análisis de las alarmas principales.

- A la derecha de la página de inicio, puede ver el número de alarmas de diferentes gravedades, el número de tareas en ejecución, el usuario actual y la información de ayuda.

  Figura 7-1 Información de estado del clúster

  – Haga clic en para ver el nombre de la tarea, el clúster, el estado, el progreso, la hora de inicio y la hora de finalización de las últimas 100 tareas de operación de **Task Management Center**.

    NOTA

    Para una tarea de inicio, parada, reinicio o reinicio continuo, puede cancelarla haciendo clic en el nombre de la tarea en la lista de tareas, haciendo clic en **Abort** y, a continuación, escribiendo la contraseña de administrador del sistema en el cuadro de diálogo que se muestra. Una tarea abortada ya no se ejecuta.

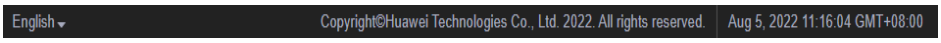
  – Haga clic en para obtener información de ayuda.

Tabla 7-1 Información de ayuda

Concepto	Descripción
Acerca de	Proporciona información sobre la versión del FusionInsight Manager.

- La barra de tareas en la parte inferior de la página principal muestra las opciones de idioma del FusionInsight Manager y la información de hora y zona horaria del clúster actual. Puede cambiar el idioma del sistema según sea necesario.

  Figura 7-2 Barra de tareas en la parte inferior de la página de inicio

Área de vista previa del estado del servicio

El número de hosts disponibles y el número de servicios instalados en cada clúster se muestran a la izquierda de la página de inicio. Puede hacer clic en para ampliar toda la información del servicio del clúster y ver el estado y las alarmas de cada servicio.

Haga clic en para realizar operaciones básicas de gestión de O&M en el clúster actual. Para obtener más información, consulte **Tabla 7-2**.

El icono a la izquierda de cada nombre de servicio indica que el servicio se está ejecutando correctamente; el icono indica que el servicio actual no se inicia; y el icono indica que el servicio actual no se ha iniciado.

También puede comprobar si se han generado alarmas para el servicio a la derecha del nombre del servicio. Si se han generado alarmas, se muestran las gravedades de alarma y el número de alarmas.

Para los componentes que admiten varios servicios, si se han instalado varios servicios en el mismo clúster, el número de servicios instalados se muestra a la derecha de cada componente.

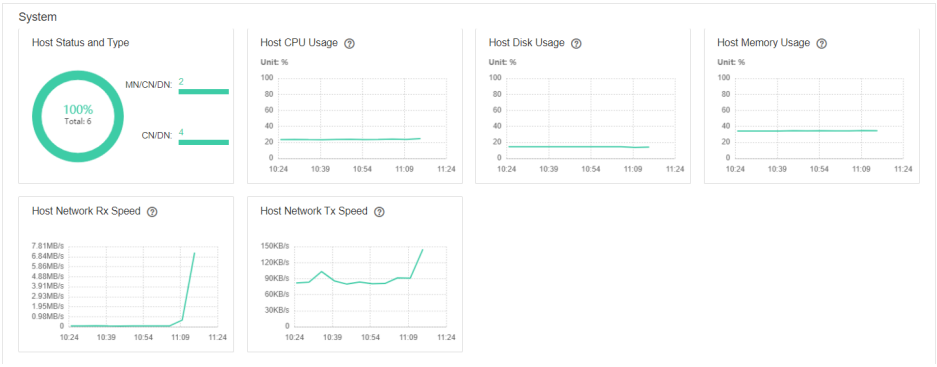
El icono que aparece a la derecha del nombre del servicio indica que la configuración del servicio ha caducado.

Área de Informe de estado de monitoreo

El área del gráfico se encuentra a la derecha de la página de inicio, que muestra informes clave de métricas de monitoreo, como el estado de todos los hosts del clúster, el uso de la CPU del host y el uso de la memoria del host. Puede personalizar los informes de monitoreo para que se muestren en esta área. Para obtener más información sobre cómo gestionar las métricas de monitoreo, consulte **Gestión de informes de métricas de monitoreo**.

Puede ver el origen de datos de un gráfico de monitoreo en la esquina inferior izquierda del gráfico. Puede ampliar un informe de monitoreo para ver los valores de los gráficos con mayor claridad o cerrar el informe de monitoreo.

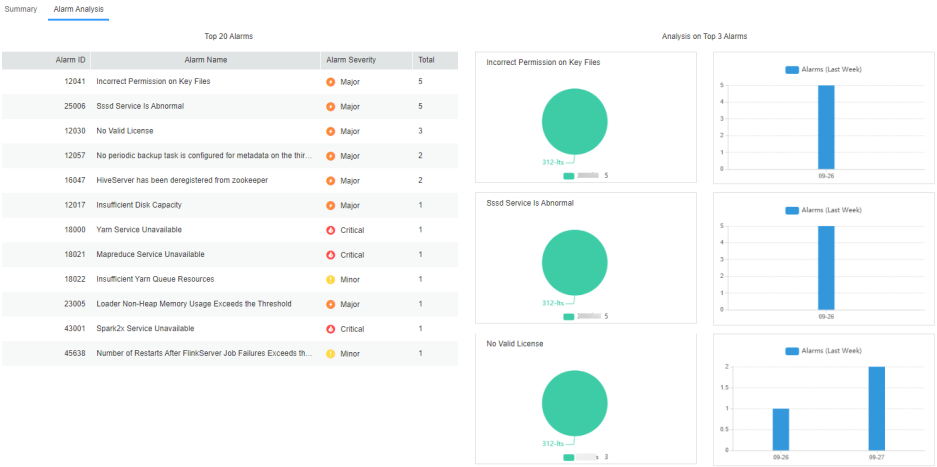
Figura 7-3 Informe de estado de monitoreo



Análisis de alarmas

En la página de pestaña **Alarm Analysis**, puede ver la tabla **Top 20 Alarms** y el gráfico **Analysis on Top 3 Alarms**. Puede hacer clic en un nombre de alarma en la tabla **Top 20 Alarms** para ver únicamente la información de análisis de esta alarma. El análisis de alarmas le permite ver las alarmas superiores y su tiempo de ocurrencia para que pueda manejar las alarmas en consecuencia, mejorando la estabilidad del sistema.

Figura 7-4 Página de pestaña de análisis de alarma



7.1.2 Gestión de informes de métricas de monitoreo

Escenario

En FusionInsight Manager, puede personalizar los elementos de monitoreo para que se muestren en la página de inicio y exportar datos de monitoreo.

NOTA

El intervalo en el eje horizontal del gráfico varía en función del período de tiempo especificado. Las normas de monitoreo de datos son las siguientes:

- **0 a 25 horas**: El intervalo es de 5 minutos. El clúster debe haber estado instalado durante al menos 10 minutos y se guardan los datos de monitoreo de un máximo de 15 días.
- **25 a 150 horas**: El intervalo es de 30 minutos. El clúster debe haber estado instalado durante al menos 30 minutos y se guardan los datos de monitoreo de un máximo de 3 meses.
- **150 a 300 horas**: El intervalo es de 1 hora. El clúster debe haber estado instalado durante al menos 1 hora y se guardan los datos de monitoreo de un máximo de 3 meses.
- **300 horas a 300 días**: El intervalo es de 1 día. El clúster debe haber estado instalado durante al menos 1 día y se guardan los datos de monitoreo de un máximo de 6 meses.
- **Más de 300 días**: El intervalo es de 7 días. El clúster debe haber estado instalado durante más de 7 días y se guardan los datos de monitoreo de un máximo de 1 año.
- Si el uso del disco de la partición donde reside GaussDB supera el 80%, se eliminarán los datos de monitoreo en tiempo real y los datos de monitoreo cuyo intervalo es de 5 minutos.
- **Recursos de almacenamiento (HDFS) en recursos de tenant (0 a 300 horas)**: El intervalo es de 1 hora. El clúster debe haber estado instalado durante al menos 1 hora y se guardan los datos de monitoreo de un máximo de 3 meses.

Personalización de un informe de métrica de monitoreo

Paso 1 Inicie sesión en FusionInsight Manager.

Paso 2 Elija **Homepage**.

Paso 3 En la esquina superior derecha del área del gráfico, haga clic en ▼ y elija **Customize** en el menú que se muestra.

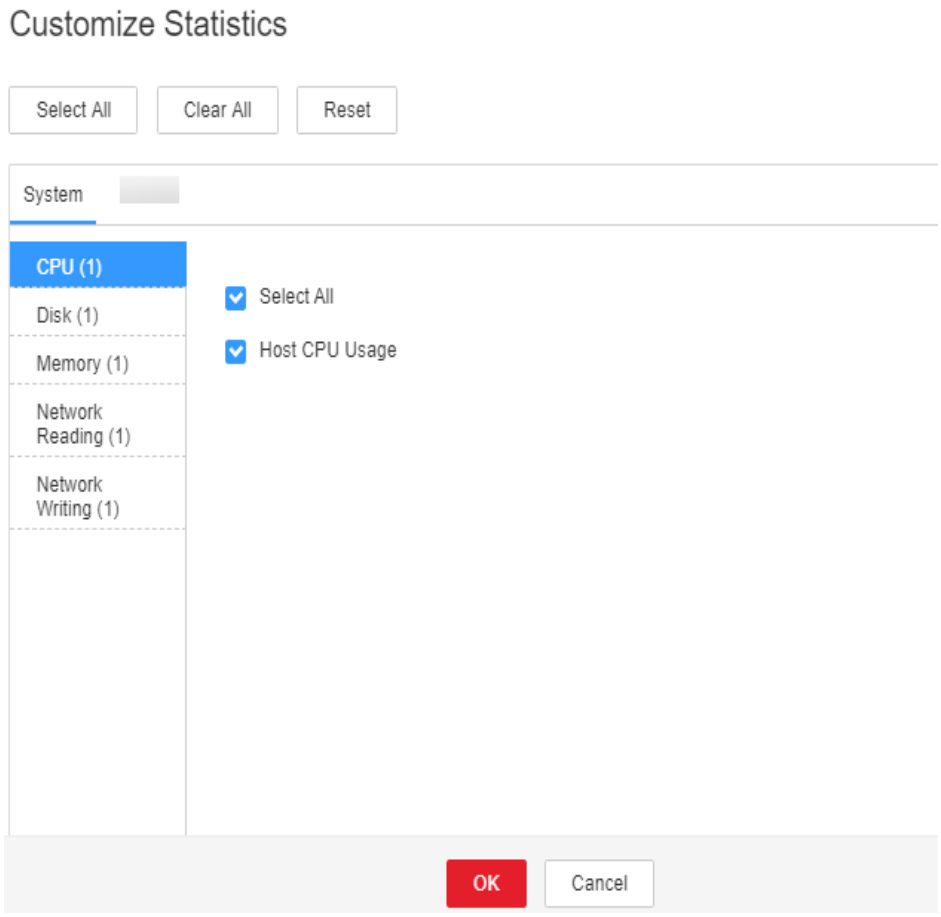
NOTA

Los datos de monitorización de la última hora se muestran en un intervalo de 5 minutos. Después de entrar en la página **Real-time Monitoring**, puede ver que los datos de monitoreo en tiempo real se muestran a la derecha del gráfico de monitoreo en un intervalo de 5 minutos.

Paso 4 En el panel izquierdo del cuadro de diálogo **Customize Statistics**, seleccione un recurso para monitorear.

Paso 5 Seleccione una o varias métricas de monitoreo en el panel derecho.

Figura 7-5 Personalización de un informe de métrica de monitoreo



Paso 6 Haga clic en **OK**.

----Fin

Exportación de todos los datos de monitoreo

Paso 1 Inicie sesión en FusionInsight Manager.

Paso 2 Elija **Homepage**.

Paso 3 En la esquina superior derecha del área del gráfico, seleccione un intervalo de tiempo para obtener los datos de monitoreo, por ejemplo, **1w**.

Los datos en tiempo real se muestran de forma predeterminada, que no se pueden exportar.

Puede hacer clic en para personalizar un intervalo de tiempo.

Figura 7-6 Personalización de un intervalo de tiempo

Paso 4 En la esquina superior derecha del área del gráfico, haga clic en y elija **Export** en el menú que se muestra.

----Fin

Exportación de datos de monitoreo de un elemento de monitoreo especificado

Paso 1 Inicie sesión en FusionInsight Manager.

Paso 2 Elija **Homepage**.

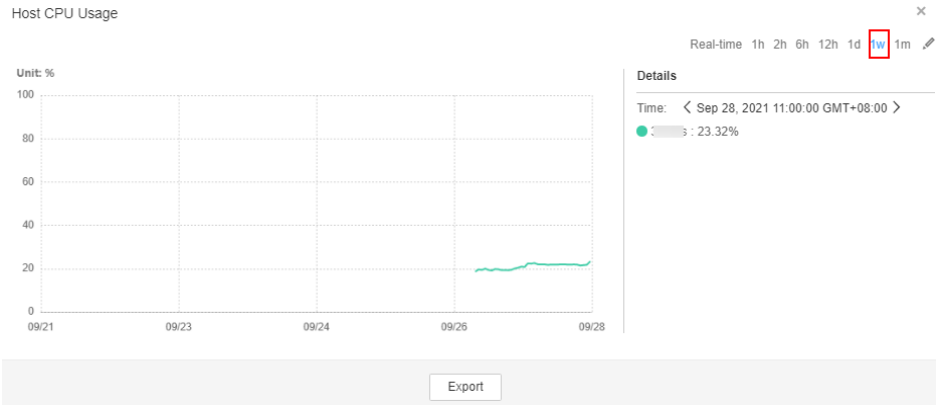
Paso 3 Haga clic en en la esquina superior derecha de cualquier panel de informes de monitoreo en el área de gráficos del clúster de destino.

Paso 4 Seleccione un intervalo de tiempo para obtener datos de monitorización, por ejemplo, **1w**.

Los datos en tiempo real se muestran de forma predeterminada, que no se pueden exportar.

Puede hacer clic en para personalizar un intervalo de tiempo.

Figura 7-7 Personalización de un intervalo de tiempo para un elemento de monitoreo especificado



Paso 5 Haga clic en **Export**.

----Fin

7.1.3 Consulta de la versión de FusionInsight Manager

Al ver la versión de FusionInsight Manager, puede prepararse para la actualización del sistema y el mantenimiento de rutina.

- Utilizar la interfaz gráfica de usuario:

  Inicie sesión en FusionInsight Manager. En la página de inicio, haga clic en en la esquina superior derecha y elija **About** en la lista desplegable. En el cuadro de diálogo que se muestra, vea la versión del FusionInsight Manager.

  Figura 7-8 Ver la versión

- Uso de CLI
  a. Inicie sesión en el nodo de gestión activa de FusionInsight Manager como usuario **root**.
  b. Ejecute los siguientes comandos para comprobar la versión y la información de la plataforma del FusionInsight Manager:

     su - omm

     cd ${BIGDATA_HOME}/om-server/om/sbin/pack

     ./queryManager.sh

     Se muestra la siguiente información:

```
    Version
Package                                                         Cputype
    ***
FusionInsight_Manager_***                                       x86_64
```

NOTA

*** indica el número de versión. Reemplácelo con el número de versión real.

7.2 Clúster

7.2.1 Gestión de clúster

7.2.1.1 Descripción

Panel

Inicie sesión en FusionInsight Manager y elija **Cluster** > *Name of the desired cluster* > **Dashboard** para ver el estado del clúster actual.

En la página de pestaña **Dashboard**, puede iniciar, detener, realizar un reinicio continuo de, sincronizar configuraciones y realizar otras operaciones básicas en el clúster actual.

Figura 7-9 Panel

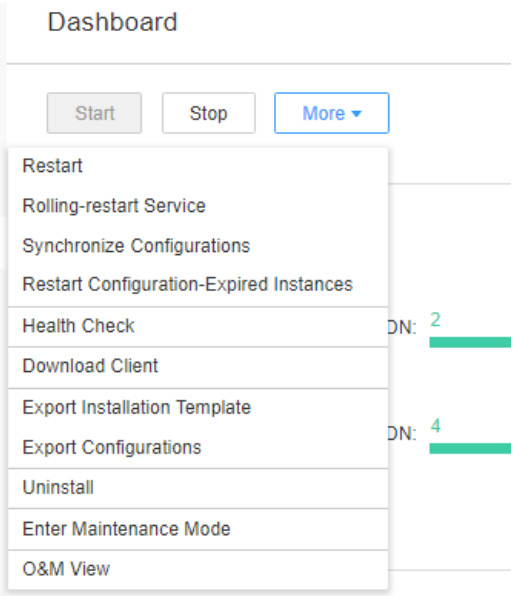


Tabla 7-2 Operaciones de mantenimiento y gestión

Portal de UI	Descripción
Start	Inicia todos los servicios del clúster.
Stop	Detiene todos los servicios del clúster.
More > **Restart**	Reinicia todos los servicios del clúster.
More > **Rolling-restart Service**	Reinicia todos los servicios del clúster uno a la vez sin interrumpir las cargas de trabajo. Para obtener más información sobre cómo realizar un reinicio continuo, consulte **Realización de un reinicio continuo de un clúster**.
More > **Synchronize Configurations**	Habilita nuevos parámetros de configuración para todos los servicios del clúster.
More > **Restart Configuration-Expired Instances**	Reinicia las instancias caducadas para todos los servicios del clúster. Para obtener más información, consulte **Gestión de configuraciones caducadas**.
More > **Health Check**	Realiza una comprobación de estado en los nodos de OMS, todos los servicios y el resto de nodos del clúster. Hay tres tipos de elementos de comprobación: estado de ejecución, alarmas relacionadas y métricas de monitoreo personalizadas. Los resultados de la comprobación de estado no siempre son los mismos que los valores de **Running Status** mostrados en la GUI. Puede exportar los resultados de la comprobación haciendo clic en **Export** en la esquina superior izquierda de la lista de comprobación. Si se detecta algún problema, puede hacer clic en **View Help** para buscar un método de solución de problemas.
More > **Download Client**	Descarga el cliente predeterminado. Para obtener más información, consulte **Descarga del cliente**.
More > **Export Installation Template**	Exporta por lotes todas las configuraciones de instalación del clúster, como el modo de autenticación del clúster, la información del nodo y la configuración del servicio. Puede utilizar esta función cuando necesite volver a instalar el clúster en el mismo entorno.
More > **Export Configurations**	Configuraciones de exportación por lotes de todos los servicios del clúster.
More > **Enter Maintenance Mode** and **More** > **Exit Maintenance Mode**	Entra o sale del modo de mantenimiento del clúster.
More > **O&M View**	Permite ver los servicios o hosts que están en modo de mantenimiento.

7.2.1.2 Realización de un reinicio continuo de un clúster

Escenario

Un reinicio continuo es reiniciar por lotes todos los servicios de un clúster después de que se modifiquen o actualicen sin interrumpir las cargas de trabajo.

Puede realizar un reinicio continuo de un clúster según sea necesario.

NOTA

- Algunos servicios de un clúster no admiten el reinicio continuo. Estos servicios se reinician en modo normal durante el reinicio continuo del clúster. Como resultado, las cargas de trabajo pueden interrumpirse. Por lo tanto, debe determinar si se debe realizar esta operación como se le solicite.
- Las configuraciones que deben surtir efecto inmediatamente, por ejemplo, las configuraciones de puertos de servidor, deben reiniciarse en modo normal.

Impacto en el sistema

Un reinicio continuo tarda más tiempo y puede afectar el rendimiento y el rendimiento del servicio.

Procedimiento

Paso 1 Inicie sesión en FusionInsight Manager.

Paso 2 Elija **Cluster** > *Name of the target cluster* > **Dashboard**. En esta página de pestaña, elija **More** >**Rolling-restart Service**.

Paso 3 En el cuadro de diálogo que se muestra, introduzca la contraseña del usuario de inicio de sesión actual y haga clic en **OK**.

Paso 4 Configure los parámetros según los requisitos del sitio.

Figura 7-10 Clúster de reinicio continuo

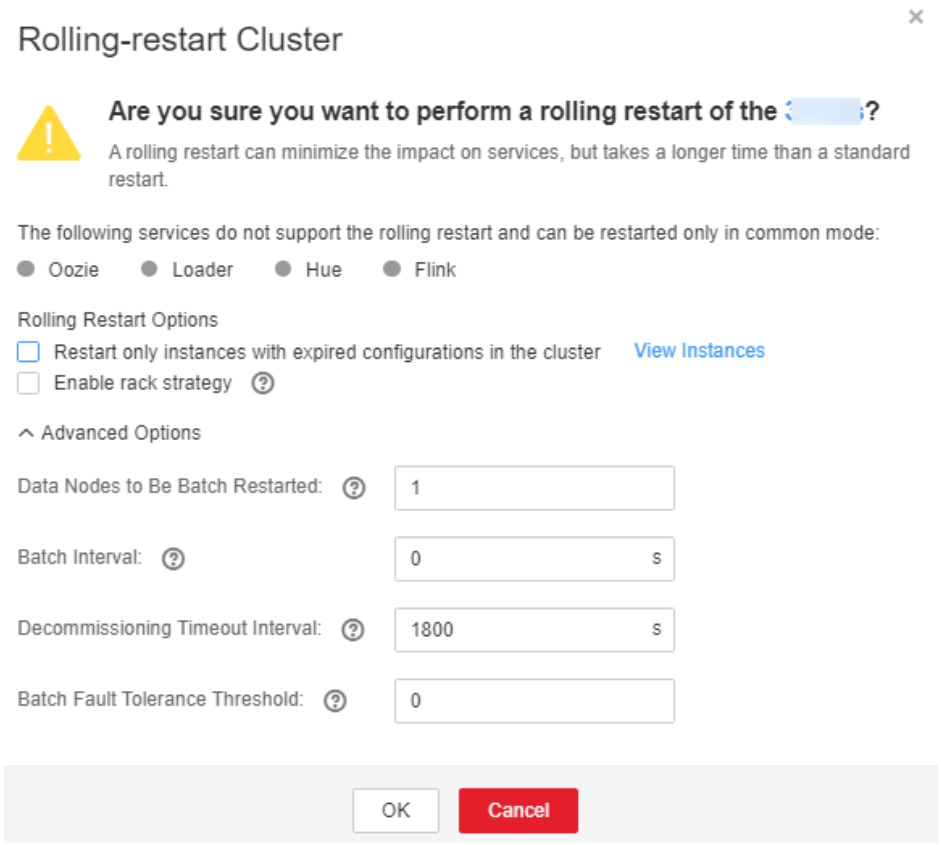


Tabla 7-3 Parámetros del reinicio secuencial

Parámetro	Descripción
Restart only instances with expired configurations in the cluster	Si desea reiniciar solo las instancias modificadas en un clúster
Enable rack strategy	Si se debe habilitar la estrategia de reinicio continuo de rack simultáneos. Este parámetro solo tiene efecto para los roles que cumplen con la estrategia de reinicio continuo de rack. (Los roles admiten el reconocimiento de rack y las instancias de los roles pertenecen a dos o más racks.) **NOTA** Este parámetro es configurable solo cuando se realiza un reinicio continuo en HDFS o YARN.

Parámetro	Descripción
Data Nodes to Be Batch Restarted	Número de instancias que se reinician en cada lote cuando se utiliza la estrategia de reinicio continuo por lotes. El valor predeterminado es **1**. **NOTA** ● Este parámetro solo es válido cuando se utiliza la estrategia de reinicio continuo por lotes y el tipo de instancia es de DataNode. ● Este parámetro no es válido cuando se habilita la estrategia de rack. En este caso, el clúster utiliza el número máximo de instancias (20 de forma predeterminada) configuradas en la estrategia de rack como el número máximo de instancias que se reinician simultáneamente en un rack. ● Este parámetro es configurable solo cuando se realiza un reinicio continuo en HDFS, HBase, YARN, Kafka, Storm, o Flume. ● Este parámetro para el RegionServer de HBase no se puede configurar manualmente. En su lugar, se ajusta automáticamente en función del número de nodos de RegionServer. Específicamente, si el número de nodos de RegionServer es menor que 30, el valor del parámetro es de **1**. Si el número es mayor o igual que 30 y menor que 300, el valor del parámetro es **2**. Si el número es mayor o igual a 300, el valor del parámetro es 1% del número (redondeado hacia abajo).
Batch Interval	Intervalo entre dos lotes de instancias que se van a reiniciar. El valor predeterminado es **0**.
Decommissioning Timeout Interval	Intervalo de desmantelamiento para instancias de rol durante un reinicio continuo. El valor predeterminado es **1800s**. Algunos roles (como HiveServer y JDBCServer) dejan de proporcionar servicios antes del reinicio continuo. Las instancias detenidas no se pueden conectar a nuevos clientes. Las conexiones existentes se completarán después de un período de tiempo. Un intervalo de tiempo de espera adecuado puede garantizar la continuidad del servicio. **NOTA** Este parámetro solo se puede configurar cuando se realiza un reinicio continuo en Hive o Spark2x.
Batch Fault Tolerance Threshold	Tiempos de tolerancia cuando el reinicio continuo de las instancias no se ejecuta por lotes. El valor predeterminado es **0**, que indica que la tarea de reinicio continuo finaliza después de que cualquier lote de instancias no se reinicie.

NOTA

Los parámetros avanzados, como **Data Nodes to Be Batch Restarted**, **Batch Interval** y **Batch Fault Tolerance Threshold** deben configurarse correctamente en función de los requisitos del sitio. De lo contrario, los servicios pueden verse interrumpidos o el rendimiento del clúster puede verse gravemente afectado.

Ejemplo:

- Si **Data Nodes to Be Batch Restarted** se establece en un valor innecesariamente grande, un gran número de instancias se reinician simultáneamente. Como resultado, los servicios se interrumpen o el rendimiento del clúster se ve gravemente afectado debido a que hay muy pocas instancias de trabajo.
- Si **Batch Fault Tolerance Threshold** es demasiado grande, los servicios se interrumpirán porque el siguiente lote de instancias se reiniciará después de que un lote de instancias no se reinicie.

Paso 5 Haga clic en **OK**.

----Fin

7.2.1.3 Gestión de configuraciones caducadas

Escenario

Si se necesita entregar una nueva configuración a todos los servicios del clúster, o **Configuration Status** de varios servicios cambia a **Expired** o **Failed** después de modificar una configuración, los parámetros de configuración de estos servicios no se sincronizan y no tienen efecto. En este caso, sincronice las configuraciones y reinicie las instancias de servicio relacionadas para el clúster de modo que los nuevos parámetros surtan efecto para todos los servicios.

Si la configuración de los servicios en el clúster se ha sincronizado pero no tiene efecto, debe reiniciar las instancias cuya configuración ha caducado.

Impacto en el sistema

- Después de sincronizar la configuración del clúster, debe reiniciar los servicios cuya configuración ha caducado. Estos servicios no están disponibles durante el reinicio.
- Las instancias cuya configuración ha caducado no están disponibles durante el reinicio.

Procedimiento

Sincronizar la configuración.

Paso 1 Inicie sesión en FusionInsight Manager.

Paso 2 Elija **Cluster** >*Name of the desired cluster* >**Dashboard**.

Paso 3 En esta página, elija **More** > **Synchronize Configuration**.

Paso 4 En el cuadro de diálogo que se muestra, haga clic en **OK**.

----Fin

Reiniciar instancias de configuración caducadas.

Paso 1 Elija **More** > **Restart Configuration-Expired Instances**.

Paso 2 En el cuadro de diálogo que se muestra, introduzca la contraseña del usuario de inicio de sesión actual y haga clic en **OK**.

Paso 3 En el cuadro de diálogo que se muestra, haga clic en **OK**.

Puede hacer clic en **View Instance** para abrir la lista de todas las instancias caducadas y confirmar que se han reiniciado.

----Fin

7.2.1.4 Descarga del cliente

Escenario

Utilice el cliente predeterminado proporcionado por los clústeres de para gestionar el clúster, ejecutar servicios y realizar un desarrollo secundario. Antes de utilizar este cliente, necesita descargar su paquete de software.

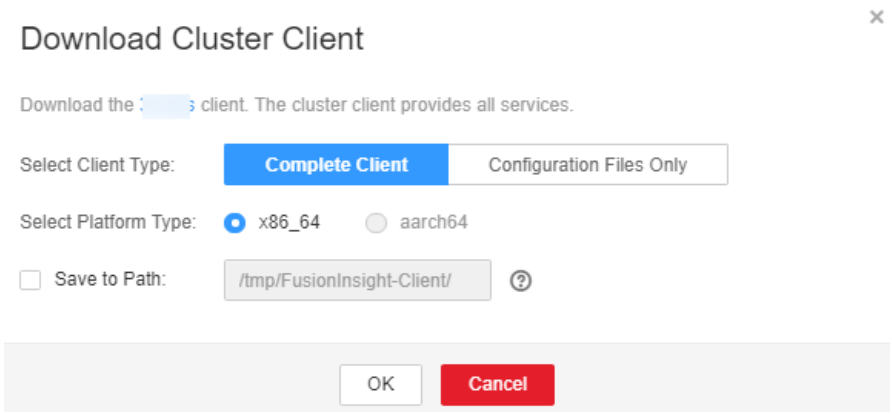
Procedimiento

Paso 1 Inicie sesión en FusionInsight Manager.

Paso 2 Elija **Cluster** >*Name of the desired cluster* >**Dashboard**. En la página que se muestra, elija **More** >**Download Client**.

Aparece el cuadro de diálogo **Download Cluster Client**.

Figura 7-11 Descargar el cliente de clúster



Paso 3 Seleccione un tipo de cliente para **Select Client Type**.

- **Complete Client**: el paquete contiene scripts, archivos de compilación y archivos de configuración.
- **Configuration Files Only**: el paquete contiene solo los archivos de configuración del cliente.

  Este tipo es aplicable a las tareas de desarrollo de aplicaciones. Por ejemplo, después de descargar e instalar un cliente completo, el administrador del clúster modifica la configuración del servicio en FusionInsight Manager y los desarrolladores deben actualizar los archivos de configuración del cliente.

> NOTA
>
> Establezca **Select Platform Type** en **x86_64** o **aarch64**. Para ejecutar el cliente en nodos x86, seleccione **x86_64**; para ajustar el cliente en nodos de TaiShan seleccione **aarch64**. De forma predeterminada, debe seleccionar un cliente que tenga la misma arquitectura que sus servidores.

Paso 4 Determine si desea generar un archivo de paquete de software cliente en el nodo del clúster.

- En caso afirmativo, seleccione **Save to Path** y haga clic en **OK** para generar el archivo cliente.

  El archivo generado se almacena en el directorio **/tmp/FusionInsight-Client** del nodo de gestión activo de forma predeterminada. También puede almacenar el archivo cliente en otros directorios, y el usuario **omm** tiene los permisos de lectura, escritura y ejecución en el directorio. Si el archivo cliente ya existe en la ruta de acceso, se reemplazará el archivo cliente existente.

  Una vez generado el archivo, copie el paquete obtenido en otro directorio, por ejemplo **/opt/Bigdata/hadoopclient** como usuario **omm** o usuario de instalación cliente.
- Si no, haga clic en **OK** para descargar el archivo cliente en el host local.

  El sistema comienza a descargar el paquete de software del cliente.

----Fin

7.2.1.5 Modificación de atributos de clúster

Escenario

Consultar los atributos básicos del clúster en FusionInsight Manager.

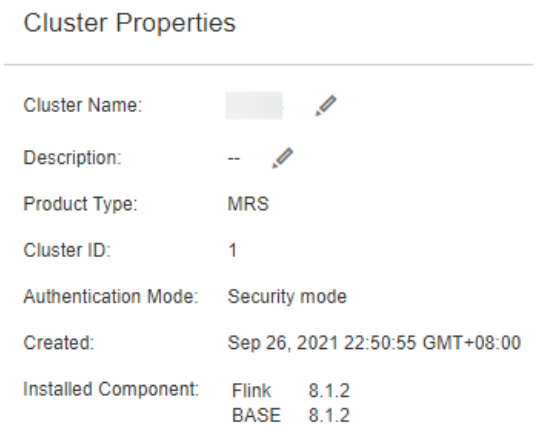
Procedimiento

Paso 1 Inicie sesión en FusionInsight Manager.

Paso 2 Elija **Cluster** > *Name of the desired cluster* > **Cluster Properties**.

De forma predeterminada, puede ver el nombre del clúster, la descripción del clúster, el tipo de producto, el ID del clúster, el modo de autenticación, la hora de creación y los componentes instalados.

Figura 7-12 Página de propiedades de clúster



Paso 3 Cambie el nombre del clúster.

1. Haga clic en e introduzca un nuevo nombre.

   Introduzca de 2 a 199 caracteres. Solo se permiten letras, dígitos, guiones bajos (_), guiones (-) y espacios, y el nombre no puede comenzar con un espacio.

2. Haga clic en **OK** para que el nuevo nombre del clúster surta efecto.

Paso 4 Modifique la descripción del clúster.

1. Haga clic en e introduzca una nueva descripción.

   Introduzca un máximo de 199 caracteres. Solo se permiten letras, dígitos, comas (,), puntos (.), guiones bajos (_), espacios y caracteres de nueva línea (\n).

2. Haga clic en **OK** para que la nueva descripción surta efecto.

----Fin

7.2.1.6 Gestión de configuraciones de clúster

Escenario

FusionInsight Manager le permite ver los cambios de los parámetros de configuración de servicios en un clúster con un solo clic, lo que le ayuda a localizar rápidamente las fallas y a mejorar la eficiencia de la gestión de la configuración.

Puede ver rápidamente todos los valores no predeterminados de cada servicio en el clúster, valores no uniformes entre instancias del mismo rol, registros históricos de modificaciones de configuración del clúster y parámetros caducados en el clúster en la página de configuración.

Procedimiento

Paso 1 Inicie sesión en FusionInsight Manager.

Paso 2 Elija **Cluster** >*Name of the desired cluster* >**Configurations**.

Paso 3 Seleccione una página de operación basada en el escenario.

- Para ver todos los valores no predeterminados:
  a. Haga clic en **All Non-default Values**. El sistema muestra los parámetros cuyos valores son diferentes de los valores predeterminados configurados para cada servicio, rol o instancia del clúster actual.

     Puede hacer clic en junto a un valor de parámetro para restaurar rápidamente el valor predeterminado. Puede hacer clic en para ver los registros históricos de modificación del parámetro.

     Si hay un gran número de parámetros que configurar, puede filtrar los parámetros en el cuadro de filtro en la esquina superior derecha de la página o introducir palabras clave en el cuadro de búsqueda.

  b. Para cambiar los valores de los parámetros, cambie los valores de acuerdo con la descripción del parámetro y haga clic en **Save**. En el cuadro de diálogo que se muestra, haga clic en **OK**.
- Para ver todos los valores no uniformes:

a. Haga clic en **All Non-uniform Values**. El sistema muestra parámetros con diferentes configuraciones de rol, servicio, grupo de instancia o instancia en el clúster actual.

   Puede hacer clic en  junto a un valor de parámetro y ver las diferencias en el cuadro de diálogo que se muestra.

b. Para cambiar el valor de un parámetro, haga clic en  para cancelar la diferencia de configuración o ajuste manualmente el valor del parámetro, haga clic en **OK** y, a continuación, haga clic en **Save**. En el cuadro de diálogo que se muestra, haga clic en **OK**.

- Para comprobar las configuraciones caducadas:

  a. Haga clic en **Expired Configurations**. Se muestran los elementos de configuración caducados en el clúster actual.

  b. Puede filtrar servicios utilizando el cuadro de filtro de servicios en la parte superior de la página para ver las configuraciones caducadas de diferentes servicios. También puede introducir palabras clave en el cuadro de búsqueda.

  c. Los elementos de configuración caducados no surten efecto completamente. Reinicie los servicios o instancias cuyas configuraciones hayan caducado de manera oportuna.

- Para ver los registros de configuración históricos:

  a. Haga clic en **Historical Configurations**. Se muestran los registros históricos de cambios de configuración del clúster actual. Puede ver detalles sobre los cambios en los valores de los parámetros, incluidos el servicio al que pertenece el parámetro, los valores de los parámetros antes y después de la modificación y los archivos de parámetros.

  b. Para restaurar un cambio de configuración, haga clic en **Restore Configuration** en la columna **Operation** del registro de destino. En el cuadro de diálogo que se muestra, haga clic en **OK**.

NOTA

Algunos elementos de configuración solo tienen efecto después de reiniciar los servicios correspondientes. Una vez guardadas las configuraciones, reinicie los servicios o instancias cuyas configuraciones hayan caducado de manera oportuna.

----Fin

7.2.1.7 Gestión de grupos de servicios estáticos

7.2.1.7.1 Recursos de servicio estático

Descripción

Un clúster asigna recursos de servicio estáticos a servicios Flume, HBase, HDFS, IoTDB, Kafka (Kafka admite grupos de servicios estáticos solo en MRS 3.2.0 o posterior), e YARN. El volumen total de recursos informáticos asignados a cada servicio es fijo y son estáticos. Un tenant puede utilizar o compartir exclusivamente un servicio para obtener los recursos necesarios para ejecutar este servicio.

Grupo de servicio estática

Los grupos de servicios estáticos se utilizan para especificar configuraciones de recursos de servicio.

Los grupos de servicios estáticos gestionan de forma centralizada los recursos que puede utilizar cada servicio.

- Limita el número total de recursos que pueden utilizar cada servicio. Específicamente, el número total de recursos de CPU, E/S y memoria se puede configurar en los nodos donde los servicios Flume, HBase, HDFS, e YARN se despliegan.
- Aísla los recursos de los servicios de un clúster de los de otros servicios. De esta manera, la carga de un servicio tiene un impacto muy limitado en otros servicios.

Mecanismo de programación

El mecanismo de planificación de recursos dinámicos basado en el tiempo permite configurar diferentes volúmenes de recursos estáticos para servicios en diferentes momentos, optimizando los entornos de ejecución de servicios y mejorando la eficiencia del clúster.

En un entorno de clúster complejo, varios servicios comparten recursos en el clúster, pero el período de servicio de recursos de cada servicio puede ser diferente.

A continuación se utiliza un cliente bancario como ejemplo:

- El servicio de consultas de HBase es pesado durante el día.
- El servicio de consultas es ligero, pero el servicio de análisis Hive es pesado por la noche.

Si se asignan recursos fijos a cada servicio, pueden producirse los siguientes problemas:

- El servicio de consultas no puede obtener recursos suficientes mientras los recursos del servicio de análisis estén inactivos durante el día.
- El servicio de análisis no puede obtener recursos suficientes mientras los recursos del servicio de consulta estén inactivos por la noche.

Como resultado, la utilización de recursos del clúster es baja y la capacidad del servicio es débil. Resuelva el problema de las siguientes maneras:

- Es necesario configurar suficientes recursos para HBase durante el día.
- Es necesario configurar suficientes recursos para Hive por la noche.

El mecanismo de programación dinámica basado en el tiempo puede utilizar eficientemente recursos y ejecutar tareas.

7.2.1.7.2 Configuración de recursos estáticos de clúster

Escenario

Puede ajustar la base de recursos en FusionInsight Manager y personalizar los grupos de configuración de recursos si necesita controlar los recursos de servicio utilizados en cada nodo de un clúster o las cuotas de CPU o E/S disponibles en cada nodo en diferentes segmentos de tiempo.

Impacto en el sistema

- Después de configurar un grupo de servicios estático, el estado de configuración de los servicios afectados se muestra como **Expired**. Necesita reiniciar los servicios. Los servicios no están disponibles durante el reinicio.
- Después de configurar un grupo de servicios estático, el número máximo de recursos utilizados por cada instancia de servicio e rol no puede exceder el límite superior.

Procedimiento

Modificar la base de ajuste de recursos

Paso 1 En FusionInsight Manager, seleccione **Cluster**, haga clic en el nombre del clúster de destino y elija **Static Service Pool Configurations**.

Paso 2 Haga clic en **Configuration** en la esquina superior derecha. Se muestra la página para configurar grupos de recursos.

Paso 3 Cambie los valores de **CPU (%)** y **Memory (%)** en el área **System Resource Adjustment Base**.

La modificación de la base de ajuste de recursos del sistema cambia el uso máximo de CPU y memoria física en los nodos por servicios. Si se despliegan varios servicios en el mismo nodo, el uso máximo de recursos físicos de todos los servicios no puede exceder el uso ajustado de CPU o memoria.

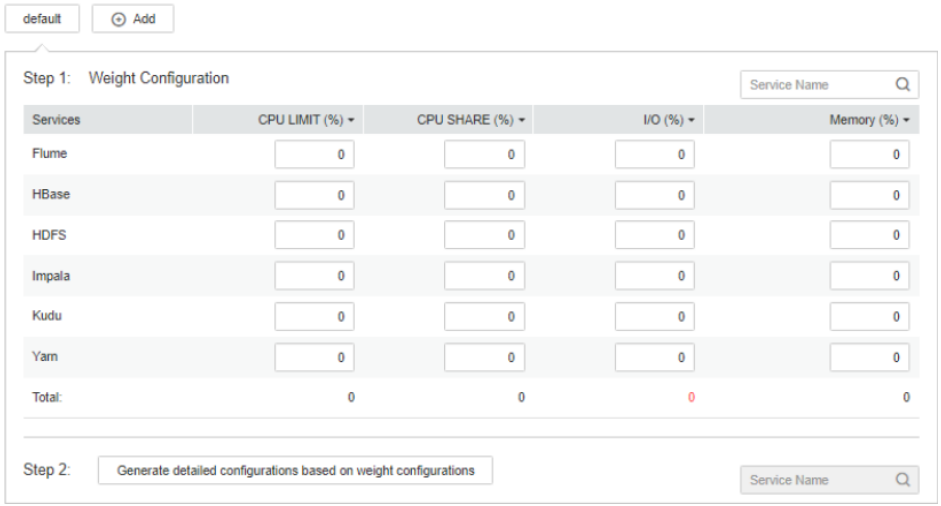
Paso 4 Haga clic en **Next**.

Para volver a modificar los parámetros, haga clic en **Previous**.

Modificar el grupo de configuración de recursos predeterminado

Paso 5 Haga clic en **default**. En la tabla **Configure weight**, establezca **CPU LIMIT(%)**, **CPU SHARE(%)**, **I/O(%)** y **Memory(%)** para cada servicio.

Figura 7-13 Configuración de ponderación



NOTA

- La suma de **CPU LIMIT(%)** y **CPU SHARE(%)** utilizados por todos los servicios puede superar el 100%.
- La suma de **I/O(%)** utilizados por todos los servicios puede superar el 100%, pero no puede ser 0.
- La suma de **Memory(%)** utilizados por todos los servicios puede ser mayor, menor o igual al 100%.
- **Memory(%)** no puede tener efecto dinámicamente y solo se puede modificar en el grupo de configuración predeterminado.
- **CPU LIMIT(%)** se utiliza para configurar la relación entre el número de núcleos de CPU que puede usar un servicio y los que pueden asignarse a nodos relacionados.
- **CPU SHARE(%)** se utiliza para configurar la relación entre el tiempo en que un servicio usa un núcleo de CPU y el tiempo en que otros servicios usan el núcleo de CPU. Es decir, la relación de tiempo cuando múltiples servicios compiten por el mismo núcleo de CPU.

Paso 6 Haga clic en **Generate detailed configurations based on weight configurations**. FusionInsight Manager genera los valores reales de los parámetros de la tabla de configuración de ponderación predeterminada basándose en los recursos de hardware del clúster y la información de asignación.

Paso 7 Haga clic en **OK**.

En el cuadro de diálogo que se muestra, haga clic en **OK**.

Agregar un grupo de configuración de recursos personalizado

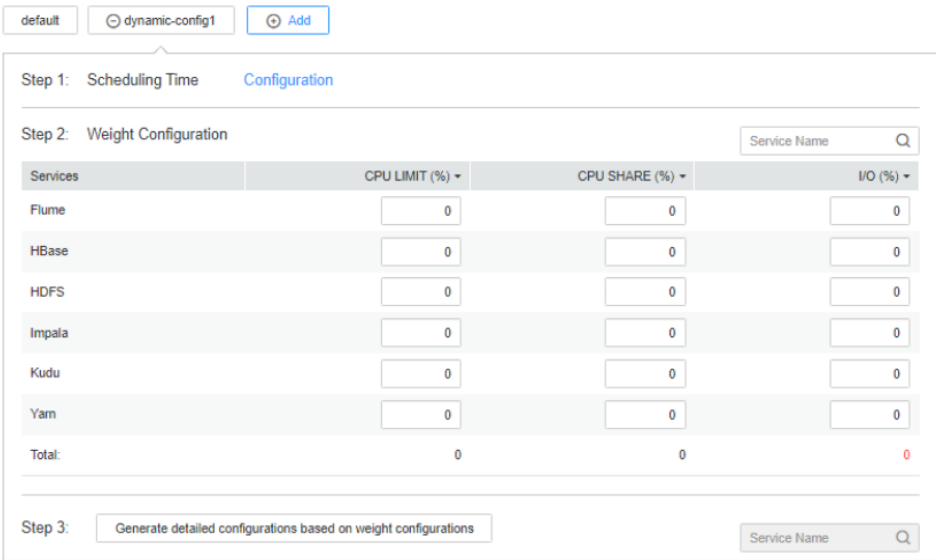
Paso 8 Determine si se deben ajustar automáticamente las configuraciones de recursos en diferentes segmentos de tiempo.

- En caso afirmativo, vaya a **Paso 9**.
- Si no, utilice las configuraciones predeterminadas y no se requiere ninguna acción adicional.

Paso 9 Haga clic en **Configuration**, cambie los valores base del ajuste de recursos del sistema y haga clic en **Next**.

Paso 10 Haga clic en **Add** para agregar un grupo de configuración de recursos.

Figura 7-14 Agregar un grupo de configuración de recursos



Paso 11 En **Step 1: Scheduling Time**, haga clic en **Configuration**.

Se muestra la página para configurar la política de tiempo.

Modifique los siguientes parámetros en función de los requisitos de servicio y haga clic en **OK**.

- **Repeat**: Si se selecciona este parámetro, la configuración de recursos personalizada se aplica repetidamente en función del período de programación. Si este parámetro no está seleccionado, establezca la fecha y la hora en que se puede aplicar la configuración del grupo de recursos.
- **Repeat Policy**: Los valores disponibles son **Daily**, **Weekly** y **Monthly**. Este parámetro sólo es válido cuando se selecciona **Repeat**.
- **On**: indica el período de tiempo entre la hora de inicio y la hora de finalización cuando se aplica la configuración de recursos. Establezca un rango de tiempo único. Si el intervalo de tiempo se superpone con el de un grupo existente de configuración de recursos, el intervalo de tiempo no se puede guardar.

NOTA

- El grupo predeterminado de configuración de recursos tiene efecto en todos los segmentos de tiempo indefinidos.
- El grupo de recursos recién agregado es un conjunto de parámetros que tiene efecto dinámicamente en un intervalo de tiempo especificado.
- El grupo de recursos recién agregado se puede eliminar. Se puede agregar un máximo de cuatro grupos de configuración de recursos que tengan efecto dinámicamente.
- Seleccione una política de repetición. Si la hora de finalización es anterior a la hora de inicio, la configuración de recursos finaliza al día siguiente de forma predeterminada. Por ejemplo, si un período de validez oscila entre las 22:00 y las 06:00, la configuración de recursos personalizada tiene efecto entre las 22:00 del día actual y las 06:00 del día siguiente.
- Si los tipos de política de repetición de varios grupos de configuración son diferentes, los intervalos de tiempo pueden superponerse. Los tipos de política se enumeran de la siguiente manera por prioridad de menor a mayor: diario, semanal y mensual. Lo siguiente es un ejemplo. Hay dos grupos de configuración de recursos que utilizan las políticas mensuales y diarias, respectivamente. Sus intervalos de tiempo de aplicación en un día se superponen de la siguiente manera: de 04:00 a 07:00 y de 06:00 a 08:00. En este caso, prevalece la configuración del grupo que utiliza la política mensual.
- Si los tipos de política de repetición de varios grupos de configuración de recursos son los mismos, los intervalos de tiempo de diferentes fechas pueden superponerse. Por ejemplo, si hay dos grupos de programación semanales, puede establecer el mismo intervalo de tiempo en un día diferente para ellos, como de 04:00 a 07:00, el lunes y el miércoles, respectivamente.

Paso 12 Modifique la configuración de recursos de cada servicio en **Step 2: Weight Configuration**.

Paso 13 Haga clic en **Generate detailed configuration**. FusionInsight Manager genera los valores reales de los parámetros de la tabla de configuración de ponderación predeterminada basándose en los recursos de hardware del clúster y la información de asignación.

Paso 14 Haga clic en **OK**.

En el cuadro de diálogo que se muestra, haga clic en **OK**.

----Fin

7.2.1.7.3 Consulta de recursos estáticos de clúster

Escenario

La plataforma de gestión de big data puede gestionar y aislar los recursos de servicio que no se ejecutan en YARN mediante grupos de recursos de servicio estáticos. El sistema admite el ajuste automático basado en el tiempo de los grupos de recursos de servicio estático. Esto permite que el clúster ajuste automáticamente los valores de los parámetros en diferentes períodos para garantizar una utilización más eficiente de los recursos.

Los administradores del sistema pueden ver los indicadores de monitoreo de los recursos utilizados por cada servicio en el grupo de servicios estático en FusionInsight Manager. Los indicadores de seguimiento son los siguientes:

- Uso de los servicios de CPU
- Velocidad total de lectura de E/S en disco de los servicios
- Tasa total de escritura de E/S en disco de los servicios
- Total de la memoria utilizada de los servicios

NOTA

Después de activar la función multi-tenant, el uso de CPU, E/S y memoria de todas las instancias de HBase se puede gestionar de forma centralizada.

Procedimiento

Paso 1 En FusionInsight Manager, seleccione **Cluster**, haga clic en el nombre del clúster de destino y elija **Static Service Pool Configurations**.

Paso 2 En la lista de grupos de configuración, haga clic en un grupo de configuración, por ejemplo, **default**.

Paso 3 Compruebe los valores base del ajuste de recursos del sistema.

- **System Resource Adjustment Base** indica el volumen máximo de recursos que puede utilizar cada nodo del clúster. Si un nodo solo tiene un servicio, el servicio ocupa exclusivamente los recursos disponibles en el nodo. Si un nodo tiene varios servicios, todos los servicios comparten los recursos disponibles en el nodo.
- **CPU** indica el número máximo de CPUs que pueden utilizar los servicios en un nodo.
- **Memory** indica la memoria máxima que pueden utilizar los servicios en un nodo.

Paso 4 En **Chart**, vea los datos de métricas del uso de recursos del servicio de clúster.

NOTA

- Puede hacer clic en **Add Service to Chart** para agregar datos de recursos de servicios estáticos de servicios específicos (hasta 12 servicios) al gráfico.
- Para obtener más información sobre cómo gestionar un gráfico, consulte **Gestión de informes de métricas de monitoreo**.

----Fin

7.2.1.8 Gestión de clientes

7.2.1.8.1 Gestión de un cliente

Escenario

FusionInsight Manager admite la gestión unificada de la información de instalación del cliente de clúster. Después de que un usuario descarga e instala un cliente, FusionInsight Manager registra automáticamente información sobre el cliente instalado (registrado) para facilitar la consulta y la gestión. Además, puede agregar o modificar manualmente la información sobre los clientes que no se registran automáticamente, por ejemplo, los clientes instalados en versiones anteriores.

Procedimiento

Ver información de cliente.

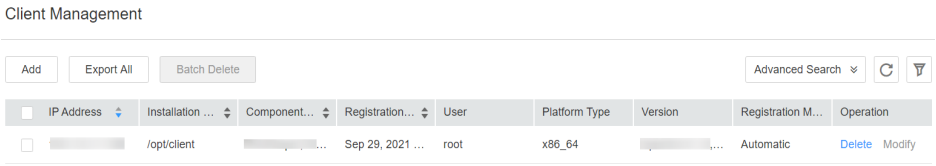
Paso 1 Inicie sesión en FusionInsight Manager.

Paso 2 Elija **Cluster**, haga clic en el nombre del clúster deseado y elija **Client Management** para ver información sobre los clientes instalados en el clúster.

Puede ver la dirección IP, la ruta de instalación, la lista de componentes, la hora de registro y el usuario de instalación del nodo en el que se encuentra el cliente.

Cuando el cliente se descarga e instala en el clúster de la última versión, la información del cliente se registra automáticamente.

Figura 7-15 Información del cliente



Agregar información de cliente.

Paso 3 Para agregar manualmente información sobre un cliente instalado, haga clic en **Add** y agregue manualmente la dirección IP, la ruta de instalación, la información del usuario, la plataforma y la información de registro del cliente según se le solicite.

Paso 4 Configure la información del cliente y haga clic en **OK**.

Modificar información de cliente.

Paso 5 Modificar la información sobre el cliente registrado manualmente.

En la página **Client Management**, seleccione el cliente de destino y haga clic en **Modify**. Después de modificar la información, haga clic en **OK**.

Eliminar información de cliente.

Paso 6 En la página **Client Management**, seleccione el cliente de destino y haga clic en **Delete**. En el cuadro de diálogo que se muestra, haga clic en **OK**.

Para eliminar varios clientes, seleccione todos ellos y haga clic en **Batch Delete**. En el cuadro de diálogo que se muestra, haga clic en **OK**.

Exportación de información de cliente.

Paso 7 En la página **Client Management**, haga clic en **Export All** para exportar información sobre todos los clientes registrados al PC local.

NOTA

En la página **Client Management** sólo se muestran los componentes que tienen clientes en la lista de componentes. Por lo tanto, algunos componentes que no tienen clientes y tienen componentes especiales no se muestran.

No se muestran los siguientes componentes:

LdapServer, KrbServer, DBService, Hue, MapReduce, y Flume

----Fin

7.2.1.8.2 Actualización de clientes por lotes

Escenario

El paquete cliente descargado desde FusionInsight Manager contiene la herramienta de actualización por lotes del cliente. Cuando es necesario actualizar varios clientes después de la actualización del clúster o la ampliación horizontal, puede utilizar esta herramienta para actualizar los clientes por lotes con unos pocos clics. Además, la herramienta proporciona la función ligera de actualizar por lotes el archivo **/etc/hosts** en los nodos donde se encuentran los clientes.

Procedimiento

Preparar para la actualización de cliente.

Paso 1 Inicie sesión en FusionInsight Manager.

Paso 2 Elija **Cluster**, haga clic en el nombre del clúster deseado, haga clic en **More** y seleccione **Download Client** para descargar el cliente completo en el directorio especificado en el servidor.

Para obtener más información, consulte **Descarga del cliente**.

Descomprima el paquete de cliente descargado y busque el directorio **batch_upgrade** por ejemplo, **/tmp/FusionInsight-Client/FusionInsight_Cluster_1_Services_ClientConfig/batch_upgrade**.

Paso 3 Elija **Cluster**, haga clic en el nombre del clúster deseado y elija **Client Management**. En la página **Client Management**, haga clic en **Export All** para exportar toda la información del cliente al equipo local.

Paso 4 Descomprima la información del cliente exportado y suba el archivo **client-info.cfg** al directorio **batch_upgrade**.

Paso 5 Complemente la contraseña en el archivo **client-info.cfg** haciendo referencia a **Información de referencia**.

Actualizar clientes por lotes.

Paso 6 Ejecute el comando **sh client_batch_upgrade.sh -u -f /tmp/FusionInsight-Client/FusionInsight_Cluster_1_Services_Client.tar -g /tmp/FusionInsight-Client/FusionInsight_Cluster_1_Services_ClientConfig/batch_upgrade/client-info.cfg** para realizar la actualización.

AVISO

Se recomienda eliminar el archivo **client-info.cfg** tan pronto como sea posible después de la actualización porque se ha configurado la contraseña.

Paso 7 Una vez completada la actualización, compruebe el resultado de la actualización ejecutando el comando **sh client_batch_upgrade.sh -c**.

Paso 8 Si el cliente está defectuoso, ejecute el comando **sh client_batch_upgrade.sh -s** para revertir el cliente.

NOTA

- La herramienta de actualización por lotes del cliente mueve el cliente original al directorio de copia de respaldo y, a continuación, utiliza el paquete cliente especificado por el parámetro **-f** para instalar el cliente. Por lo tanto, si el cliente original contiene contenido personalizado, guarde manualmente el contenido personalizado del directorio de copia de respaldo o mueva el contenido personalizado al directorio del cliente después de la actualización antes de ejecutar el comando **-c**. La ruta de copia de respaldo en el cliente es *{Original client path}*-**backup**.
- El comando **-u** es el requisito previo para los comandos **-c** y **-s**. Puede ejecutar el comando **-c** para confirmar la actualización o el comando **-s** para realizar una reversión solo después de ejecutar el comando **-u** para realizar una actualización.
- Puede ejecutar el comando **-u** varias veces para actualizar solo los clientes que no se pueden actualizar.
- La herramienta de actualización por lotes del cliente también es compatible con los clientes de versiones anteriores.
- Al actualizar un cliente instalado por un usuario no root, asegúrese de que el usuario tiene los permisos de lectura y escritura en el directorio donde se encuentra el cliente y el directorio principal en el nodo de destino. De lo contrario, la actualización fallará.
- El paquete de cliente especificado por el parámetro **-f** debe ser un paquete de cliente completo. Los paquetes de cliente de un solo componente o algunos componentes no se pueden usar como entrada.

----Fin

Información de referencia

Antes de actualizar los clientes por lotes, debe configurar manualmente la contraseña de usuario para iniciar sesión de forma remota en el nodo de cliente.

Ejecute el comando **vi client-info.cfg** para agregar una contraseña de usuario.

Ejemplo:

```
clientIp,clientPath,user,password
10.10.10.100,/home/omm/client /home/omm/client2,omm,Password
```

Los campos del archivo de configuración son los siguientes:

- **clientIp**: indica la dirección IP del nodo donde se encuentra el cliente.
- **clientPath**: indica la ruta de instalación del cliente. Las rutas múltiples están separados por espacios. Tenga en cuenta que la ruta no puede terminar con una barra diagonal (/).
- **user**: indica el nombre de usuario del nodo.
- **password**: indica la contraseña de usuario del nodo.

NOTA

Si la ejecución falla, vea el archivo **node.log** en el directorio **work_space/log_***XXX*.

7.2.1.8.3 Actualización del archivo hosts en lotes

Escenario

El paquete cliente descargado desde FusionInsight Manager contiene la herramienta de actualización por lotes del cliente. Esta herramienta proporciona la función de actualizar clientes por lotes y la función ligera de actualizar por lotes el archivo **/etc/hosts** en el nodo donde se encuentra el cliente.

Prerrequisitos

Usted ha hecho preparativos para la actualización. Para obtener más información, consulte "Preparación para la actualización del cliente." en **Actualización de clientes por lotes**.

Actualización del archivo hosts en lotes

Paso 1 Compruebe si el usuario configurado para el nodo donde se debe actualizar el archivo **/etc/hosts** es **root**.

- En caso afirmativo, vaya a **Paso 2**.
- Si no, cambie el usuario a **root** y vaya a **Paso 2**.

Paso 2 Ejecute el comando **sh client_batch_upgrade.sh -r -f /tmp/FusionInsight-Client/FusionInsight_Cluster_1_Services_Client.tar -g /tmp/FusionInsight-Client/FusionInsight_Cluster_1_Services_ClientConfig/batch_upgrade/client-info.cfg** para actualizar por lotes el archivo **/etc/hosts** en los nodos donde reside el cliente.

NOTA

- Cuando se actualiza por lotes el archivo **/etc/hosts**, el paquete de cliente ingresado puede ser un paquete de cliente completo o un paquete de cliente que contiene solo archivos de configuración (recomendado).
- El usuario configurado para el host donde se necesita actualizar el archivo **/etc/hosts** debe ser **root**. De lo contrario, la actualización falla.

----Fin

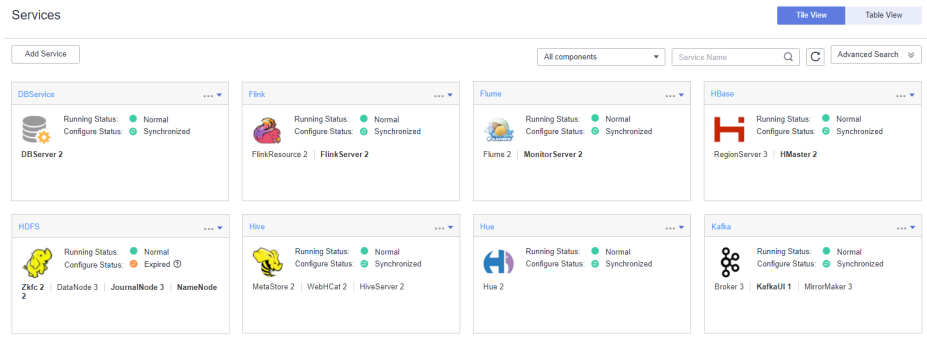
7.2.2 Gestión de un servicio

7.2.2.1 Descripción

Panel

Inicie sesión en FusionInsight Manager. Elija **Cluster**, haga clic en el nombre del clúster deseado y elija **Services**. Se muestra la página de gestión de servicios, incluidos el área funcional y la lista de servicios.

Figura 7-16 Página de gestión de servicios



Área funcional

En el área funcional de la página de gestión de servicios, puede seleccionar un tipo de vista y filtrar y buscar servicios por tipo de servicio. Puede utilizar la búsqueda avanzada para seleccionar los servicios necesarios según el estado de ejecución y el estado de configuración.

Lista de servicios

La lista de servicios de la página de gestión de servicios contiene todos los servicios instalados en el clúster. Si se selecciona la vista de mosaico, los servicios se mostrarán en estilo de panel. Si selecciona la vista de lista, los servicios se mostrarán en una tabla.

NOTA

En esta sección, el **Tile View** se utiliza de forma predeterminada.

La lista de servicios muestra el estado de ejecución, el estado de configuración, el tipo de rol y el número de instancias de cada servicio. En esta página, puede realizar algunas tareas de mantenimiento del servicio, como iniciar, detener y reiniciar servicios.

Tabla 7-4 Estado de ejecución del servicio

Estado	Descripción
Normal	Indica que el servicio se está ejecutando correctamente.
Faulty	Indica que el servicio no puede ejecutarse correctamente.
Partially Healthy	Indica que algunas funciones mejoradas del servicio son anormales.
Not started	Indica que el servicio está detenido.
Unknown	Indica que no se puede detectar el estado inicial del servicio.
Starting	Indica que se está iniciando el servicio.
Stopping	Indica que se está deteniendo el servicio.
Failed to start	Indica que no se puede iniciar el servicio.
Failed to stop	Indica que no se puede detener el servicio.

NOTA

- If the running status of a service is **Faulty**, an alarm is generated. Rectify the fault based on the alarm information.
- HBase, Hive, Spark, and Loader may be in the **Subhealthy** state.
  - If Yarn is installed but is abnormal, HBase is in the **Subhealthy** state. If the multi-instance function is enabled, all installed HBase service instances are in the **Subhealthy** state.
  - If HBase is installed but is abnormal, Hive, Spark, and Loader are in the **Subhealthy** state.
  - If any HBase instance is installed but is abnormal after the multi-instance function is enabled, Loader is in the **Subhealthy** state.
  - If an HBase instance is installed but is abnormal after the multi-instance function is enabled, the Hive and Spark instances that map to the HBase instance are in the **Subhealthy** state. That is, if HBase 2 is installed but is abnormal, Hive 2 and Spark2 are in the **Subhealthy** state.

Tabla 7-5 Estado de la configuración del servicio

Estado	Descripción
Synchronized	Indica que todos los parámetros de servicio han tenido efecto en el clúster.
Expired	Indica que la última configuración no está sincronizada y no tiene efecto después de modificar los parámetros de servicio. Es necesario sincronizar las configuraciones y reiniciar los servicios. Puede hacer clic en junto a **Configuration Status** para ver los elementos de configuración caducados.
Failed	Indica que se produce una excepción de comunicación o de lectura/escritura durante la sincronización de la configuración de parámetros. Utilice **Synchronize Configuration** para rectificar la falla.
Synchronizing	Indica que se está sincronizando la configuración del parámetro de servicio.
Unknown	Indica que no se puede detectar el estado inicial del servicio.

Puede hacer clic en un servicio de la lista de servicios para realizar operaciones sencillas de mantenimiento y gestión del servicio, como se describe en el documento **Tabla 7-6**.

Tabla 7-6 Mantenimiento básico y gestión

Elemento de menú en la interfaz de usuario	Descripción
Start Service	Iniciar un servicio especificado en el clúster.
Stop Service	Detener un servicio especificado en el clúster.

Elemento de menú en la interfaz de usuario	Descripción
Restart Service	Reiniciar un servicio especificado en el clúster. **NOTA** Si se reinicia un servicio, otros servicios que dependen de este servicio no estarán disponibles. Por lo tanto, seleccione **Restart upper-layer services**. Determine si se realiza esta operación basándose en la lista de servicios mostrada. Los servicios se reinician uno por uno debido a su dependencia. **Tabla 7-7** describe la duración del reinicio de un solo servicio.
Service Rolling Restart	Reiniciar un servicio especificado en el clúster sin interrumpir los servicios. Para obtener más información sobre la configuración de los parámetros, consulte **Tabla 7-3**.
Synchronize Configuration	● Habilitar nuevos parámetros de configuración para un servicio especificado en el clúster. ● Distribuir nuevos parámetros de configuración para los servicios cuyo **Configuration Status** sea **Expired**. **NOTA** Una vez sincronizados algunos servicios, reinicie los servicios para que surta efecto la configuración.

Tabla 7-7 Restart duration

Service	Restart Duration	Startup Duration	Remarks
ClickHouse	4 min	ClickHouseServer: 2 min ClickHouseBalancer: 2 min	-
HDFS	10min+x	NameNode: 4 min + x DataNode: 2 min JournalNode: 2 min Zkfc: 2 min	*x* indicates the NameNode metadata loading duration. It takes about 2 minutes to load 10,000,000 files. For example, *x* is 10 minutes for 50 million files. The startup duration fluctuates with reporting of DataNode data blocks.
Yarn	5 min + x	ResourceManager: 3 min + x NodeManager: 2 min	*x* indicates the time required for restoring ResourceManager reserved tasks. It takes about 1 minute to restore 10,000 reserved tasks.

Service	Restart Duration	Startup Duration	Remarks
MapReduce	2 min + x	JobHistoryServer: 2 min + x	*x* indicates the scanning duration of historical tasks. It takes about 2.5 minutes to scan 100,000 tasks.
ZooKeeper	2 min + x	quorumpeer: 2 min + x	*x* indicates the duration for loading znodes. It takes about 1 minute to load 1 million znodes.
Hive	3.5 min	HiveServer: 3 min MetaStore: 1 min 30s WebHcat: 1 min Hive service: 3 min	-
Spark2x	5 min	JobHistory2x: 5 min SparkResource2x: 5 min JDBCServer2x: 5 min	-
Flink	4 min	FlinkResource: 1 min FlinkServer: 3 min	-
Kafka	2 min + x	Broker: 1 min + x	*x* indicates the data restoration duration. It takes about 2 minutes to start 20,000 partitions for a single instance.
Storm	6 min	Nimbus: 3 min UI: 1 min Supervisor: 1 min Logviewer: 1 min	-
Flume	3 min	Flume: 2 min MonitorServer: 1 min	-

7.2.2.2 Otras operaciones de gestión de servicios

7.2.2.2.1 Página de detalles del servicio

Descripción

Inicie sesión en FusionInsight Manager y elija **Cluster** > *Name of the desired cluster* > **Services**. En la lista de servicios, haga clic en el nombre del servicio especificado para ir a la página de detalles del servicio, incluidas las páginas de pestañas **Dashboard**, **Instance**, **Instance Groups** y **Configurations** así como las áreas de función. Para algunos servicios, se puede mostrar la página de la herramienta de gestión personalizada. Para obtener más información sobre las herramientas de gestión admitidas, consulte **Tabla 7-8**.

Tabla 7-8 Herramientas de gestión personalizadas

Herramienta	Servicio	Descripción
Herramienta de configuración Flume	Flume	Configura los parámetros de recopilación para el servidor y el cliente de Flume.
Herramienta de gestión de clientes Flume	Flume	Visualiza la información de supervisión sobre el cliente de Flume.
Herramienta de monitoreo de topic de Kafka	Kafka	Monitorea y gestiona topics de Kafka.

La página **Dashboard** es la página predeterminada, que contiene la información básica, la lista de roles, la tabla de dependencias y el gráfico de supervisión, y más. Puede gestionar los servicios en la esquina superior derecha. Para obtener más información acerca de la gestión de servicios básicos, como inicio, detención, reinicio continuo y configuración de sincronización, consulte **Tabla 7-6**. Para obtener más información sobre otras operaciones de gestión de servicios, consulte **Tabla 7-9**.

Tabla 7-9 Operaciones de gestión de servicios

Ruta de navegación	Descripción
More > **Health Check**	Realiza una comprobación del estado del servicio actual. Los elementos de comprobación de estado incluyen el estado de cada objeto de comprobación, las alarmas relacionadas y los indicadores de supervisión definidos por el usuario. El resultado de la comprobación no es el mismo que los valores de **Running Status** mostrados en la GUI. Para exportar el resultado de la comprobación de estado, haga clic en **Export Report** en la esquina superior izquierda de la lista de comprobación. Si encuentras algún problema, haga clic en **View Help**.

Ruta de navegación	Descripción
More > **Download Client**	Descargue el cliente predeterminado que contiene solo servicios específicos y realice operaciones de gestión, ejecute servicios o realice un desarrollo secundario en el cliente. Para obtener más información, consulte **Descarga del cliente**.
More > **Change Service Name**	Cambia el nombre del servicio actual.
More > **Perform** *XX* **Switchover**	Para obtener más información, consulte **Realización de conmutación activa/en espera de una instancia de rol**.
More > **Enter/Exit Maintenance Mode**	Configura un servicio para entrar/salir del modo de mantenimiento.
Configurations > **Import/Export**	En el escenario en el que los servicios se migran a un nuevo clúster o se vuelven a implementar los mismos servicios, puede importar o exportar todos los datos de configuración de un servicio específico para copiar rápidamente los resultados de configuración.

Área de información básica

El área de información básica de la página de pestaña **Dashboard** contiene los datos básicos de estado del servicio, incluidos el estado de ejecución, los detalles de configuración, la versión y la información clave del servicio. Si el servicio admite las web UIs de código abierto, puede acceder a las web UIs de código abierto haciendo clic en los enlaces en el área de información básica.

NOTA

En la versión actual, usuario **admin** no tiene permiso para acceder a todas las funciones de servicio proporcionadas en la interfaz de usuario web de código abierto. Cree un administrador de servicio de componentes para acceder a la dirección WebUI.

Lista de roles

La lista de roles de la página de pestaña **Dashboard** contiene todos los roles del servicio. La lista de roles muestra el estado de ejecución y el número de instancias de cada rol.

Dependencia

La tabla de relaciones de dependencia de la página de pestaña **Dashboard** muestra los servicios de los que depende el servicio actual y otros servicios que dependen del servicio.

Registros históricos de alarmas y eventos

El área de historial de alarmas y eventos muestra las alarmas y eventos clave reportados por el servicio actual. Se muestran hasta 20 registros históricos.

Gráfico

El área del gráfico se muestra a la derecha de la pestaña **Dashboard** y contiene el informe del indicador clave de supervisión del servicio. Puede personalizar el informe de supervisión que se muestra en el área del gráfico, ver la descripción de las métricas de supervisión o exportar los datos de supervisión. Para un gráfico de contribución de recursos personalizado, puede ampliar el gráfico y cambiar entre el gráfico de tendencias y el gráfico de distribución.

NOTA

Algunos servicios del clúster proporcionan elementos de supervisión de recursos de nivel de servicio. Para obtener más información, consulte **Monitoreo de recursos**.

7.2.2.2.2 Realización de conmutación activa/en espera de una instancia de rol

Escenario

Algunos roles de servicio se despliegan en modo activo/en espera. Si la instancia activa necesita ser mantenida y no puede proporcionar servicios, o si se requiere otro mantenimiento, puede activar manualmente una conmutación activa/en espera.

Procedimiento

Paso 1 Inicie sesión en FusionInsight Manager.

Paso 2 Elija **Cluster** >*Name of the desired cluster* >**Services**.

Paso 3 Haga clic en el nombre del servicio especificado en la página de gestión de servicios.

Paso 4 En la página de detalles del servicio, expanda la lista desplegable **More** y seleccione **Perform** *Role Instance* **Switchover**.

Paso 5 En el cuadro de diálogo que se muestra, introduzca la contraseña del usuario de inicio de sesión actual y haga clic en **OK**.

Paso 6 En el cuadro de diálogo que se muestra, haga clic en **OK** para realizar la conmutación activa/en espera para la instancia de rol.

NOTA

- The Manager component package only supports the active/standby switchover of DBService role instances.
- The HD component package supports the active/standby switchover of the following service role instances: HDFS, YARN, Storm, HBase, and MapReduce.
- When an active/standby switchover is performed for a NameNode on HDFS, a NameService must be set.
- The Porter component package only supports the active/standby switchover of Loader role instances.
- This function cannot be used for other role instances.

----Fin

7.2.2.2.3 Monitoreo de recursos

Inicie sesión en FusionInsight Manager, seleccione **Cluster** > *Name of the desired cluster* > **Services**, y haga clic en **Resource**. Se muestra la página de monitoreo de recursos.

Algunos servicios del clúster proporcionan métricas de monitoreo de recursos de nivel de servicio. De forma predeterminada, se muestran los datos de monitoreo de las últimas 12

horas. Puede hacer clic en para personalizar un intervalo de tiempo. Las opciones de rango de tiempo son **12h**, **1d**, **1w** y **1m**. Puede hacer clic en para exportar la información del informe correspondiente. Si un elemento de monitoreo no tiene datos, el informe no se puede exportar. **Tabla 7-10** enumera los servicios y elementos de monitoreo que admiten el monitoreo de recursos.

Tabla 7-10 Monitoreo de recursos de servicio

Servicio	Métricas	Descripción
HDFS	Uso de recursos (por tenant)	● Recopila estadísticas sobre el uso de recursos de HDFS por tenant. ● Ve las métricas **Capacity** o **Number of File Objects**.
	Uso de recursos (por usuario)	● Recopila estadísticas sobre el uso de recursos HDFS por el usuario. ● Ve las métricas **Used Capacity** o **Number of File Objects**.
	Uso de recursos (por directorio)	● Recopila estadísticas sobre el uso de recursos HDFS por directorio. ● Ve las métricas **Used Capacity** o **Number of File Objects**. ● Puede hacer clic en para configurar el monitoreo del espacio. Alternativamente, puede especificar un directorio del sistema de archivos HDFS para el monitoreo.
	Uso de recursos (por réplica)	● Recopila estadísticas sobre el uso de recursos HDFS por recuento de réplicas. ● Ve las métricas **Used Capacity** o **File Count**.
	Uso de recursos (por tamaño de archivo)	● Recopila estadísticas sobre el uso de recursos HDFS por tamaño de archivo. ● Ve las métricas **Used Capacity** o **File Count**.
	Papelera de reciclaje (por usuario)	● Recopila estadísticas sobre el uso de la papelera de reciclaje HDFS por usuario. ● Ve las métricas **Recycle Bin Capacity** o **Number of File Objects**.
	Recuento de operaciones	● Recopila el número de operaciones en HDFS.
	Balanceo automático	● Recopila estadísticas sobre la velocidad de ejecución del balanceador automático HDFS y la capacidad total de la migración del balanceador actual.

Servicio	Métricas	Descripción
	Conexiones abiertas RPC de NameNode (por usuario)	● Muestra el número de conexiones de cada usuario en las solicitudes RPC de cliente conectadas a NameNodes.
	DataNodes lento	Muestra DataNode que transmite o procesa datos lentamente en el clúster.
	Discos lentos	Muestra el disco que procesa los datos lentamente en el DataNode del clúster.
HBase	Solicitudes de operación en tablas	Muestra el número de solicitudes de operación PUT, DELETE, GET, SCAN, INCREMENT y APPEND en todas las tablas de todos los RegionServers.
	Solicitudes de operación sobre RegionServers	Muestra el número de solicitudes de operación PUT, DELETE, GET, SCAN, INCREMENT y APPEND y el número de todas las solicitudes de operación de RegionServer.
	Solicitudes de operación de servicio	Muestra el número de solicitudes de operación PUT, DELETE, GET, SCAN, INCREMENT y APPEND en todas las regiones de RegionServers.
	HFiles en RegionServers	Muestra el número de HFiles en todos los RegionServers.
HetuEngine	Uso de recursos de Coordinator	Muestra el uso de recursos del Coordinator en la cola seleccionada.
	Ratio de uso de recursos del Coordinator	Muestra el uso de recursos del Coordinator en la cola seleccionada.
	Uso de recursos del Worker	Muestra el uso de recursos de Worker en la cola seleccionada.
	Ratio de uso de recursos del Worker	Muestra el uso de recursos de Worker en la cola seleccionada.
	Número de Coordinators y Workers	Muestra el número de Coordinators y Workers en la cola seleccionada.
Hive	Subprocesos de HiveServer2-Background-Pool (por IP)	Muestra el número de subprocesos de HiveServer2-Background-Pool de los usuarios principales. Estos subprovesos se miden y se muestran en un período de medición.
	Subprocesos de HiveServer2-Handler-Pool (por IP)	Muestra el número de HiveServer2-Handler-Pools de usuarios principales recopilados y mostrados en un período.

Servicio	Métricas	Descripción
	Número de MetaStore usado (por IP)	Recopila estadísticas y muestra el uso MetaStore de los principales usuarios en un período.
	Número de Job de Hive	Muestra el número de Jobs relacionados con el usuario recopilados por Hive en un período.
	Número de archivos a los que se ha accedido en la fase de Split	Muestra el número de archivos a los que accede el sistema de almacenamiento de archivos subyacente (HDFS de forma predeterminada) en la fase de Split en un período.
	Tiempo de operación básico de Hive	Recopila tiempo para crear un directorio (mkdirTime), crear un archivo (touchTime), escribir un archivo (writeFileTime), cambiar el nombre de un archivo (renameTime), mover un archivo (moveTime), eliminar un archivo (deleteFileTime) y eliminar un directorio (deleteCatalogTime) en un periodo de tiempo.
	Particiones de tabla	Muestra el número de particiones de todas las tablas Hive, que se muestra en el formato *database # table name*, *number of table partitions*.
	Recuento de Map de HQL	Recopila estadísticas sobre las sentencias HQL ejecutadas en un período y el número de sentencias Map invocadas durante la ejecución. La información mostrada incluye usuarios, sentencias HQL y el número de sentencias de Map.
	Estadísticas de acceso de HQL	Muestra el número de veces de acceso de HQL en un período.
Kafka	Distribución de uso de disco Kafka	Muestra las estadísticas de distribución de uso de disco del clúster de Kafka.
Spark2x	Estadísticas de acceso de HQL	Recopila estadísticas de acceso de HQL en un período, incluidos el nombre de usuario, la sentencia HQL y las veces de ejecución de la sentencia HQL.
Yarn	Recursos utilizados (por tarea)	● Muestra el número de núcleos de CPU y de memoria utilizados por una tarea. ● Ve las métricas **By memory** o **By CPU**.
	Uso de recursos (por tenant)	● Muestra el número de núcleos de CPU y de memoria utilizados por un tenant. ● Ve las métricas **By memory** o **By CPU**.

Servicio	Métricas	Descripción
	Ratio de uso de recursos (por tenant)	● Muestra la relación entre el número de núcleos de CPU y la memoria utilizada por un tenant. ● Ve las métricas **By memory** o **By CPU**.
	Ranking de la duración de la tarea	Muestra las tareas de Yarn ordenadas por consumo de tiempo.
	Conexiones abiertas RPC de ResourceManager (por usuario)	Muestra el número de conexiones RPC cliente a ResourceManager por usuario.
	Recuento de operaciones	Recopila estadísticas sobre el número y la proporción de operaciones correspondientes a cada tipo de operación de Yarn.
	Ranking de tareas en una cola por uso de recursos	● Muestra los recursos consumidos por las tareas que se ejecutan en una cola después de seleccionar la cola (tenant) en la GUI. ● Ve las métricas **By memory** o **By CPU**.
	Ranking de los usuarios en una cola por uso de recursos	● Muestra los recursos consumidos por los usuarios que ejecutan tareas en la cola después de seleccionar una cola (tenant) en la GUI. ● Ve las métricas **By memory** o **By CPU**.
ZooKeeper	Recursos usados (por Znode de segundo nivel)	● Muestra el estado del recurso de znode de nivel 2 de ZooKeeper. ● Ve las métricas **By Znode quantity** o **By capacity**.
	Número de conexiones (por dirección IP del cliente)	Muestra el estado del recurso de conexión de cliente de ZooKeeper.

7.2.2.2.4 Recopilación de información de pila

Escenario

Para cumplir con los requisitos de servicio reales, el administrador del clúster puede recopilar información de la pila sobre un rol o instancia especificado en FusionInsight Manager, guardar la información en un directorio local y descargar la información. La siguiente información puede ser recopilada:

1. Información jstack.
2. Información jmap -histo.
3. Información jmap -dump.
4. La información de Thr jstack y jmap-histo se puede recopilar continuamente para su comparación.

Procedimiento

Recopilación de información de pila

Paso 1 Inicie sesión en FusionInsight Manager.

Paso 2 Haga clic en **Cluster**, haga clic en el nombre del clúster deseado, haga clic en **Services** y haga clic en el servicio de destino.

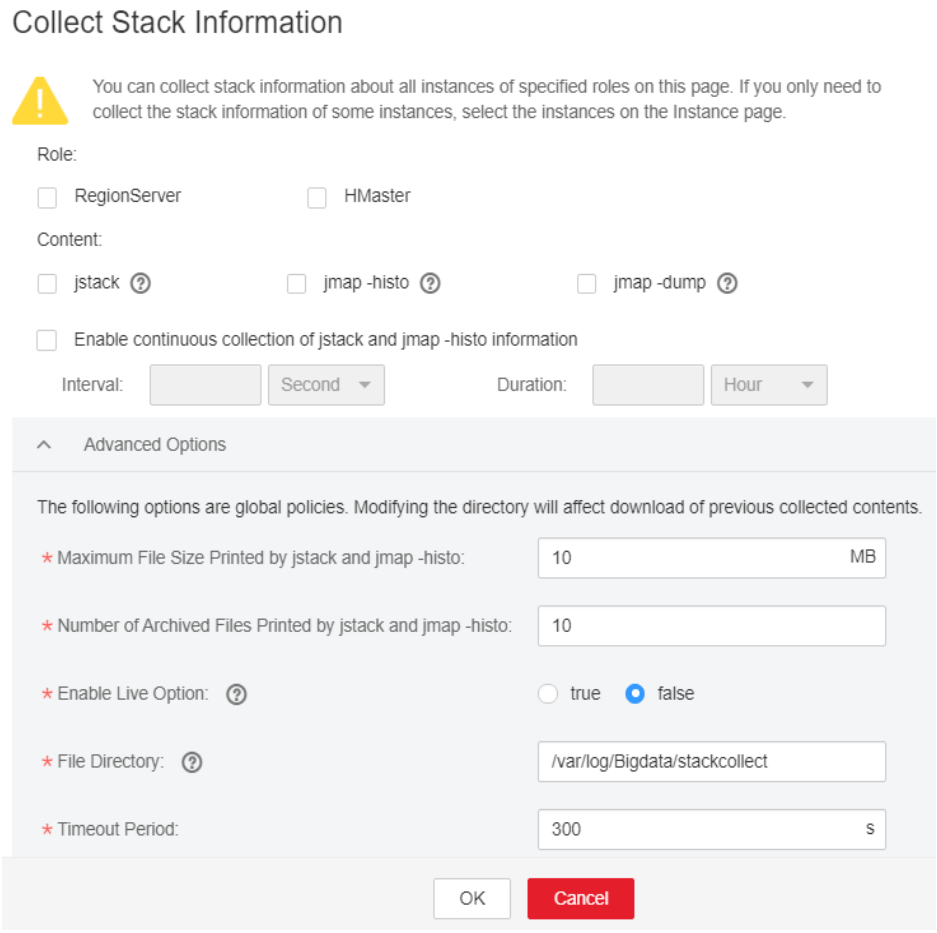
Paso 3 En la página que se muestra, elija **More** > **Collect Stack Information**.

NOTA

- Para recopilar información de pila de varias instancias, vaya a la lista de instancias, seleccione las instancias deseadas en la lista de instancias y elija **More** > **Collect Stack Information**.
- Para recopilar información de pila de una sola instancia, haga clic en la instancia deseada y elija **More** > **Collect Stack Information**.

Paso 4 En el cuadro de diálogo que se muestra, seleccione el rol y el contenido deseados, configure las opciones avanzadas (conserve la configuración predeterminada si no hay ningún requisito especial) y haga clic en **OK**.

Figura 7-17 Recopilación de información de pila



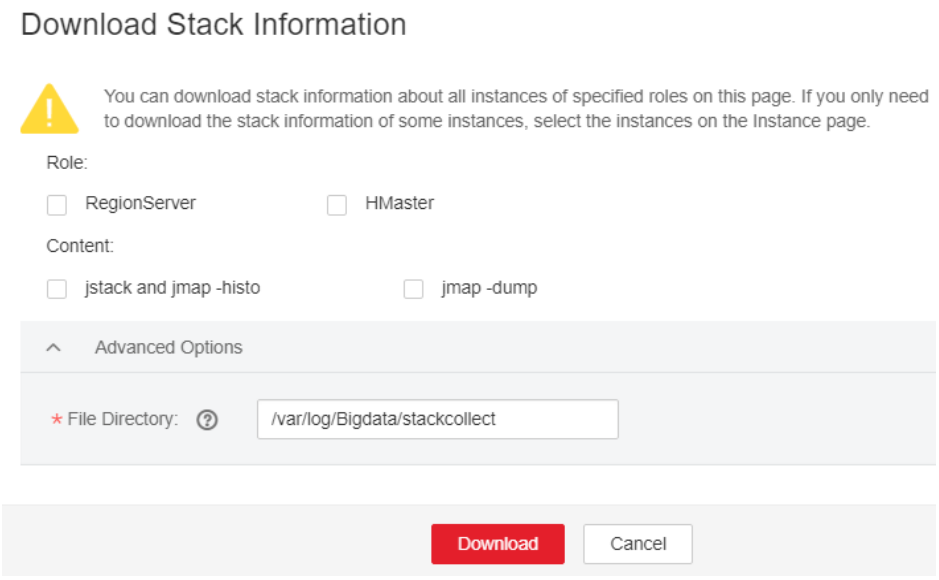
Paso 5 Una vez que la colección se haya completado correctamente, haga clic en **Download**.

Descarga de información de la pila

Paso 6 Haga clic en **Cluster**, haga clic en el nombre del clúster deseado, haga clic en **Services** y haga clic en el servicio de destino. Elija **More** > **Download Stack Information** en la esquina superior derecha.

Paso 7 Seleccione el rol y el contenido deseados y haga clic en **Download** para descargar la información de la pila en el PC local.

Figura 7-18 Descargar información de pila



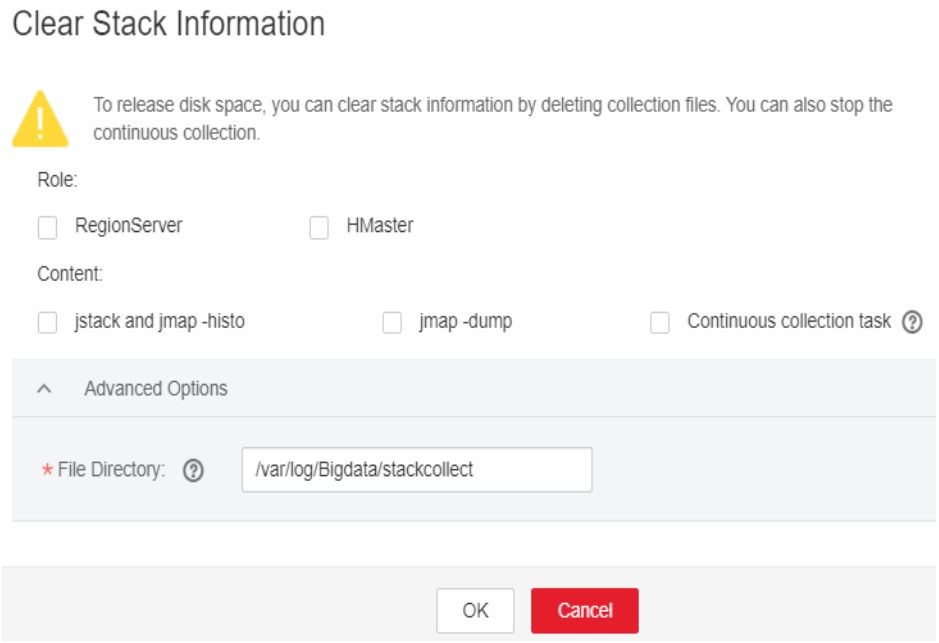
Borrar información de pila

Paso 8 Haga clic en **Cluster**, haga clic en el nombre del clúster deseado, haga clic en **Services** y haga clic en el servicio de destino.

Paso 9 Elija **More** > **Clear Stack Information** en la esquina superior derecha.

Paso 10 Seleccione el rol y el contenido deseados y configure **File Directory**. Haga clic en **OK**.

Figura 7-19 Borrar información de pila



----Fin

7.2.2.2.5 Cambio de autenticación de Ranger

Escenario

De forma predeterminada, el servicio Ranger está instalado y la autenticación Ranger está habilitada para un clúster recién instalado en modo de seguridad. Puede establecer políticas de acceso de seguridad detalladas para acceder a los recursos del componente a través del complemento de permiso del componente. Si no se requiere la autenticación de Ranger, el administrador del clúster puede deshabilitar manualmente la autenticación de Ranger en la página de servicio. Después de deshabilitar la autenticación de Ranger, el sistema continúa realizando el control de permisos basado en el modelo de rol del FusionInsight Manager al acceder a los recursos de los componentes.

En un clúster actualizado desde una versión anterior, la autenticación de Ranger no se utiliza de forma predeterminada cuando los usuarios acceden a los recursos de componentes. El administrador del clúster puede habilitar manualmente la autenticación de Ranger después de instalar el servicio Ranger.

NOTA

- En un clúster en modo de seguridad, los siguientes componentes admiten la autenticación de Ranger: HDFS, YARN, Kafka, Hive, HBase, Storm, Impala, y Spark2x.
- En un clúster en modo sin seguridad, Ranger admite el control de permisos en recursos de componentes basados en usuarios de sistema operativo. Los siguientes componentes son compatibles con la autenticación de Ranger: HBase, HDFS, Hive, Spark2x y YARN.
- Después de habilitar la autenticación de Ranger, toda la autenticación del componente será gestionada por Ranger. Los permisos establecidos por el complemento de autenticación original no serán válidos (Las reglas ACL de los componentes HDFS y YARN todavía tienen efecto). Tenga cuidado cuando realice esta acción. Se recomienda desplegar los permisos en Ranger por adelantado.
- Después de deshabilitar la autenticación de Ranger, toda la autenticación del componente será gestionada por el complemento de permiso del componente. El permiso establecido en Ranger no será válido. Tenga cuidado al realizar esta operación. Se recomienda desplegar los permisos en Manager por adelantado.

Habilitación de la autenticación de Ranger

Paso 1 Inicie sesión en FusionInsight Manager.

Paso 2 Elija **Cluster** > **Services**.

Paso 3 Haga clic en el nombre del servicio especificado en la página de gestión de servicios.

Paso 4 En la página de detalles del servicio, expanda la lista desplegable **More** y seleccione **Enable Ranger**.

Paso 5 En el cuadro de diálogo que se muestra, introduzca la contraseña del usuario de inicio de sesión actual y haga clic en **OK**.

Paso 6 En la lista de servicios, reinicie el servicio cuya configuración ha caducado.

----Fin

Desactivación de la autenticación de Ranger

Paso 1 Inicie sesión en FusionInsight Manager.

Paso 2 Elija **Cluster** > **Services**.

Paso 3 Haga clic en el nombre del servicio especificado en la página de gestión de servicios.

Paso 4 En la página de detalles del servicio, expanda la lista desplegable **More** y seleccione **Disable Ranger**.

Paso 5 Ingrese la contraseña del usuario de inicio de sesión actual y haga clic en **OK**. En el cuadro de diálogo que se muestra, haga clic en **OK**.

Paso 6 En la lista de servicios, reinicie el servicio cuya configuración ha caducado.

----Fin

7.2.2.3 Configuración del servicio

7.2.2.3.1 Modificación de parámetros de configuración del servicio

Escenario

Para cumplir con los requisitos de servicio reales, los administradores de clústeres pueden ver y modificar rápidamente las configuraciones de servicio predeterminadas en FusionInsight Manager. Configurar parámetros basados en la información proporcionada en la descripción de configuración.

NOTA

Los parámetros de DBService no se pueden modificar cuando solo existe una instancia de rol DBService en el clúster.

Impacto en el sistema

- Después de configurar las propiedades de un servicio, debe reiniciar el servicio si el estado del servicio es **Expired**. El servicio no está disponible durante el reinicio.
- Después de que los parámetros de configuración del servicio se modifiquen y luego surtan efecto después del reinicio, debe descargar e instalar el cliente de nuevo o descargar el archivo de configuración para actualizar el cliente. Por ejemplo, puede modificar los parámetros de configuración de los siguientes servicios: HBase, HDFS, Hive, Spark, YARN y MapReduce.

Procedimiento

Paso 1 Inicie sesión en FusionInsight Manager.

Paso 2 Elija **Cluster** >*Name of the desired cluster* >**Services**.

Paso 3 Haga clic en el nombre del servicio especificado en la página de gestión de servicios.

Paso 4 Haga clic en **Configuration**.

La página **Basic Configuration** se muestra de forma predeterminada. Para modificar más parámetros, haga clic en la pestaña **All Configurations**. El árbol de navegación muestra todos los parámetros de configuración del servicio. Los nodos de nivel 1 del árbol de navegación son nombres de servicio o nombres de rol. La categoría de parámetro se muestra después de expandir el nodo de nivel 1.

Como se muestra en la siguiente figura, el primer nodo **LdapServer** indica el nombre de servicio, y el segundo nodo **SlapdServer** indica el nombre de rol. El parámetro de configuración que se muestra tiene efecto para todas las instancias del rol y el servicio.

Figura 7-20 Árbol de navegación de parámetros de configuración

Paso 5 En el árbol de navegación, seleccione la categoría de parámetros especificada y cambie los valores de los parámetros a la derecha.

NOTA

Seleccione un valor de parámetro de puerto en el rango de valores de la derecha. Asegúrese de que todos los valores de parámetros del mismo servicio estén dentro del rango de valores y sean únicos. De lo contrario, no se puede iniciar el servicio.

Si no está seguro de la ubicación de un parámetro, puede escribir el nombre del parámetro en el cuadro de búsqueda en la esquina superior derecha. El sistema busca el parámetro en tiempo real y muestra el resultado.

Paso 6 Haga clic en **Save**. En el cuadro de diálogo de confirmación, haga clic en **OK**.

Espere hasta que aparezca el mensaje "Operation succeeded." Haga clic en **Finish**.

Se modifica la configuración.

NOTA

- Para actualizar la configuración de cola del servicio YARN sin reiniciar el servicio, elija **More** > **Refresh Queue** para actualizar la cola para que la configuración surta efecto.
- Durante la configuración del parámetro **flume.config.file**, puede cargar y descargar archivos. Después de cargar un archivo de configuración, el archivo antiguo se sobrescribirá. Si la configuración no se guarda y el servicio se reinicia, la configuración no surte efecto. Guarde la configuración a tiempo.
- Si necesita reiniciar el servicio para que la configuración surta efecto después de modificar los parámetros de configuración del servicio, elija **More** > **Restart Service** en la esquina superior derecha de la página del servicio.

----Fin

7.2.2.3.2 Modificación de parámetros de configuración personalizados de un servicio

Escenario

Todos los parámetros de código abierto se pueden configurar para todos los componentes del clúster de. Los parámetros utilizados en algunos escenarios de aplicación clave se pueden modificar en el FusionInsight Manager, y algunos parámetros de las características de código abierto no se pueden configurar para algunos clientes de componentes. Para modificar los parámetros de los componentes que Manager no admite directamente, los administradores de clústeres pueden agregar nuevos parámetros para los componentes mediante la función de personalización de la configuración en Manager. Los parámetros recién agregados se guardan en los archivos de configuración de componentes y entran en vigor después del reinicio.

Impacto en el sistema

- Después de configurar las propiedades de un servicio, debe reiniciar el servicio si el estado del servicio es **Expired**. El servicio no está disponible durante el reinicio.
- Después de que los parámetros de configuración del servicio se modifiquen y luego surtan efecto después del reinicio, debe descargar e instalar el cliente de nuevo o descargar el archivo de configuración para actualizar el cliente.

Prerrequisitos

Los administradores de clústeres han comprendido completamente el significado de los parámetros que se van a agregar, los archivos de configuración que se van a aplicar y el impacto en los componentes.

Procedimiento

Paso 1 Inicie sesión en FusionInsight Manager.

Paso 2 Elija **Cluster** >*Name of the desired cluster* >**Services**.

Paso 3 Haga clic en el nombre del servicio especificado en la página de gestión de servicios.

Paso 4 Haga clic en **Configuration** y haga clic en **All Configurations**.

Paso 5 En el árbol de navegación de la izquierda, localice un nodo de nivel 1 y seleccione **Customization**. El sistema muestra los parámetros personalizados del componente actual.

Los archivos de configuración que guardan los parámetros personalizados recién agregados se muestran en la columna **Parameter File**. Diferentes archivos de configuración pueden tener los mismos parámetros de código abierto. Después de que los parámetros en diferentes archivos se establecen en diferentes valores, la configuración tiene efecto depende de la secuencia de carga de los archivos de configuración por componentes. Puede personalizar los parámetros para los servicios y roles según sea necesario. No se admite la adición de parámetros personalizados para una instancia de rol única.

Paso 6 Busque la fila donde reside un parámetro especificado, introduzca el nombre del parámetro admitido por el componente en la columna **Name** e introduzca el valor del parámetro en la columna **Value**.

Puede hacer clic en + o - para agregar o eliminar un parámetro personalizado.

Paso 7 Haga clic en **Save**. En el cuadro de diálogo **Save Configuration** que se muestra, confirme la modificación y haga clic en **OK**. Después de que el sistema muestre "Operation succeeded", haga clic en **Finish**. La configuración se guardó con éxito.

Reinicie el servicio o la instancia caducada para que la configuración surta efecto.

----Fin

Ejemplo de tarea (Configuración de parámetros de Hive personalizados)

Hive depende de HDFS. De forma predeterminada, Hive accede al cliente HDFS. Los parámetros de configuración que han surtido efecto son controlados por HDFS. Por ejemplo, el parámetro HDFS **ipc.client.rpc.timeout** afecta al intervalo de tiempo de espera de RPC para que todos los clientes se conecten al servidor HDFS. Los administradores de clústeres pueden modificar el intervalo de tiempo de espera para que Hive se conecte a HDFS mediante la configuración de parámetros personalizados. Después de agregar este parámetro al archivo **core-site.xml** de Hive, este parámetro puede ser identificado por el servicio Hive y su configuración sobrescribe la configuración del parámetro en HDFS.

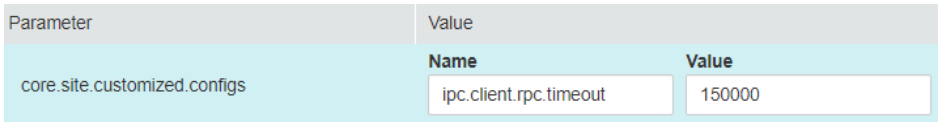
Paso 1 En el Administrador de FusionInsight, haga clic en **Cluster**, haga clic en el nombre del clúster deseado y haga clic en **Services**.

Paso 2 En la página mostrada, haga clic en **Configuration** y haga clic en **All Configurations**.

Paso 3 En el árbol de navegación de la izquierda, seleccione **Customization** para el servicio Hive. El sistema muestra los parámetros de servicio personalizados compatibles con Hive.

Paso 4 En **core-site.xml**, busque la fila que contiene el parámetro **core.site.customized.configs**, escriba **ipc.client.rpc.timeout** en la columna **Name** e introduzca un nuevo valor en la columna **Value**, por ejemplo, 150000. La unidad es ms.

Figura 7-21 Adición de parámetros personalizados



Paso 5 Haga clic en **Save**. En el cuadro de diálogo **Save Configuration** que se muestra, confirme la modificación y haga clic en **OK**. Espere hasta que aparezca el mensaje "Operation succeeded" y haga clic en **Finish**.

La configuración se guardó con éxito.

Después de guardar la configuración, reinicie el servicio o la instancia caducada para que la configuración surta efecto.

----Fin

7.2.3 Gestión de instancias

7.2.3.1 Descripción

Descripción

Inicie sesión en FusionInsight Manager, haga clic en **Cluster**, haga clic en el nombre del clúster deseado y elija **Service** > **KrbServer**. En la página mostrada, haga clic en **Instance**. La página de gestión de instancias mostrada contiene el área de función y la lista de instancias de rol.

Área funcional

Después de seleccionar las instancias que se van a operar en el área de función, puede mantener y gestionar las instancias de rol, como iniciar o detener las instancias. **Tabla 7-11** muestra las operaciones principales.

Tabla 7-11 Mantenimiento y gestión de instancias

Portal de UI	Descripción
Start Instance	Iniciar una instancia especificada en el clúster. Puede iniciar una instancia de rol en el estado **Not Started**, **Stop Failed** o **Startup Failed** para usar la instancia de rol.
More > Stop Instance	Detener una instancia especificada en el clúster. Puede detener una instancia de rol que ya no se utiliza o que es anormal.
More > Restart Instance	Reiniciar una instancia especificada en el clúster. Puede reiniciar una instancia de rol anormal para restaurarla.
More > Instance Rolling Restart	Reiniciar una instancia especificada en el clúster sin interrumpir los servicios. Para obtener más información sobre la configuración de los parámetros, consulte **Realización de un reinicio continuo de un clúster**.

Portal de UI	Descripción
More > Decommission/ Recommission	Vuelver a poner en servicio o desactivar una instancia específica en el clúster para cambiar el estado de disponibilidad del servicio. Para obtener más información, consulte **Desmantelar y volver a poner en servicio una instancia**. **NOTA** Solo el rol DataNode en HDFS, el rol NodeManager en Yarn, y el rol RegionServer en HBase soportan las funciones de reinicio y desmantelamiento.
Desired instance > **More** > **Synchronize Configuration**	Si el **Configuration Status** de una instancia de rol es de **Expired** la instancia de rol no se ha reiniciado después de modificar la configuración y la nueva configuración solo se guarda en FusionInsight Manager. En este caso, utilice esta función para entregar la nueva configuración a la instancia especificada. **NOTA** ● Después de sincronizar la configuración de la instancia de rol, debe reiniciar la instancia de rol cuya configuración ha caducado. La instancia de rol no está disponible durante el reinicio. ● Una vez completada la sincronización, reinicie la instancia para que la configuración surta efecto.
Desired instance > **Instance Configurations**	Para obtener más información, consulte **Gestión de configuraciones de instancia**.

Puede filtrar instancias según el rol al que pertenecen o su estado de ejecución en el área de función.

NOTA

Haga clic en **Advanced Search** para buscar instancias especificadas especificando otros criterios de filtro, como **Host Name**, **Management IP Address**, **Business IP Address** o **Instance Groups**.

Lista de instancias de rol

La lista de instancias de rol contiene las instancias de todos los roles del clúster. La lista muestra el estado de ejecución, el estado de configuración, los hosts y las direcciones IP relacionadas de cada instancia.

Tabla 7-12 Estado de ejecución de instancia

Estado	Descripción
Normal	Indica que la instancia se está ejecutando correctamente.
Faulty	Indica que la instancia no se puede ejecutar correctamente.
Decommissioned	Indica que la instancia está fuera de servicio.

Estado	Descripción
Not started	Indica que la instancia está detenida.
Unknown	Indica que no se puede detectar el estado inicial de la instancia.
Starting	Indica que se está iniciando la instancia.
Stopping	Indica que se está deteniendo la instancia.
Restoring	Indica que puede producirse una excepción en la instancia y que la instancia se está rectificando automáticamente.
Decommissioning	Indica que la instancia se está desmantelando.
Recommissioning	Indica que se está reiniciando la instancia.
Failed to start	Indica que no se puede iniciar el servicio.
Failed to stop	Indica que no se puede detener el servicio.

Detalles de la instancia

Puede hacer clic en un nombre de instancia para ir a la página de detalles de la instancia y ver la información básica, el archivo de configuración, los registros de instancia y los informes de métricas de monitoreo de la instancia.

7.2.3.2 Desmantelar y volver a poner en servicio una instancia

Escenario

Algunas instancias de rol proporcionan servicios para servicios externos en modo distribuido y paralelo. Los servicios almacenan de forma independiente información sobre si se puede utilizar cada instancia. Por lo tanto, debe usar FusionInsight Manager para volver a poner en marcha o desmantelar estas instancias para cambiar el estado de ejecución de la instancia.

En algunos casos no se admiten las funciones de reinicio y desmantelamiento.

NOTA

Las siguientes funciones admiten el retiro y la puesta en marcha: HDFS DataNode, YARN NodeManager, y HBase RegionServer.

- Si el número del DataNodes es menor o igual que el de las réplicas HDFS, no se puede realizar el desmantelamiento. Si el número de réplicas HDFS es tres y el número de DataNodes es inferior a cuatro en el sistema, no se puede realizar el desmantelamiento. En este caso, se informará de un error y obligará al FusionInsight Manager a salir del desmantelamiento 30 minutos después de que el FusionInsight Manager intente realizar el desmantelamiento.
- Durante la ejecución de tareas de MapReduce, se generan archivos con 10 réplicas. Por lo tanto, si el número de instancias de DataNode es inferior a 10, no se puede realizar el desmantelamiento.
- Si el número de racks de DataNode (el número de racks está determinado por el número de racks configurados para cada DataNode) es mayor que 1 antes de la retirada del servicio, y después de que algunos DataNodes sean retirados del servicio, el de los DataNodes restantes cambia a 1, la retirada del servicio fallará. Por lo tanto, antes de retirar las instancias de DataNode, debe evaluar el impacto de la retirada en el número de racks para ajustar el DataNodes que se va a retirar.
- Si se retiran varios DataNodes al mismo tiempo, y cada uno de ellos almacena un gran volumen de datos, es posible que el DataNodes no se retire debido al tiempo de espera. Para evitar este problema, se recomienda desmantelar un DataNode cada vez y realizar múltiples operaciones de desmantelar.

Procedimiento

Paso 1 Realice los siguientes pasos para realizar una comprobación de estado del DataNodes antes de retirar el servicio:

1. Inicie sesión en el nodo de instalación del cliente como usuario de cliente y cambie al directorio de instalación del cliente.
2. Para un clúster de seguridad, utilice el **hdfs** de usuario para la autenticación de permisos.

```
source bigdata_env                #Configure client environment variables.
kinit hdfs                        #Configure kinit authentication.
Password for hdfs@HADOOP.COM:     #Enter the login password of user hdfs.
```

3. Ejecute el comando **hdfs fsck / -list-corruptfileblocks** y compruebe el resultado devuelto.
   - Si aparece "has 0 CORRUPT files", vaya a **Paso 2**.
   - Si el resultado no contiene "has 0 CORRUPT files" y se devuelve el nombre del archivo dañado, vaya a **Paso 1.4**.
4. Ejecute el comando **hdfs dfs -rm** *Name of the damaged file* para eliminar el archivo dañado.

Paso 2 Inicie sesión en FusionInsight Manager.

Paso 3 Elija **Cluster** >*Name of the desired cluster* >**Services**.

Paso 4 Haga clic en el nombre del servicio especificado en la página de gestión de servicios. En la página mostrada, haga clic en la pestaña **Instance**.

Paso 5 Seleccione la instancia de rol especificada que se va a retirar del servicio.

Paso 6 Seleccione **Decommission** o **Recommission** en la lista desplegable **More**.

En el cuadro de diálogo que se muestra, introduzca la contraseña del usuario de inicio de sesión actual y haga clic en **OK**.

Seleccione **I confirm to decommission these instances and accept the consequence of service performance deterioration** y haga clic en **OK** para realizar la operación correspondiente.

NOTA

Durante la retirada de la instancia, si el servicio correspondiente a la instancia se reinicia en el clúster mediante otro navegador, FusionInsight Manager muestra un mensaje que indica que la retirada de la instancia se ha detenido, pero el estado operativo de la instancia se muestra como **Started**. En este caso, la instancia ha sido desmantelada en segundo plano. Para sincronizar el estado operativo, debe volver a desmantelar la instancia.

----Fin

7.2.3.3 Gestión de configuraciones de instancia

Escenario

Los parámetros de configuración de cada instancia de rol pueden modificarse. En el escenario en el que las instancias se migran a un nuevo clúster o el servicio se vuelve a desplegar, el administrador del clúster puede importar o exportar todos los datos de configuración de un servicio en FusionInsight Manager para copiar rápidamente los resultados de configuración.

FusionInsight Manager puede gestionar los parámetros de configuración de una única instancia de rol. La modificación de los parámetros de configuración y la importación o exportación de configuraciones de instancia no afectan a otras instancias.

Impacto en el sistema

Después de modificar la configuración de una instancia de rol, debe reiniciar la instancia si el estado de la instancia es **Expired**. La instancia de rol no está disponible durante el reinicio.

Modificación de la configuración de instancia

Paso 1 Inicie sesión en FusionInsight Manager.

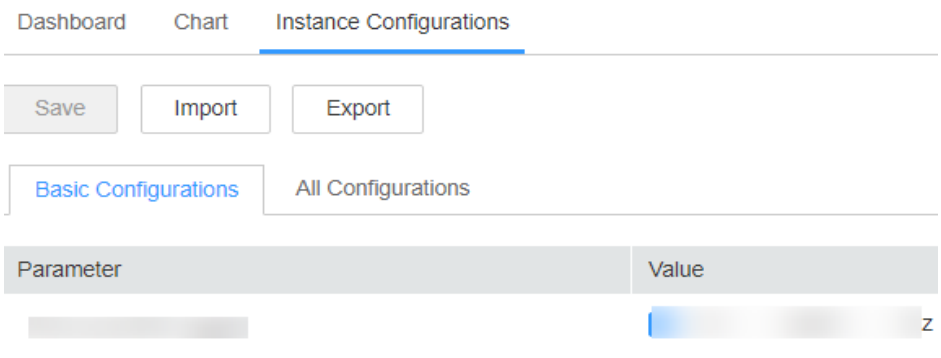
Paso 2 Elija **Cluster** >*Name of the desired cluster* >**Services**.

Paso 3 En la página que se muestra, haga clic en la pestaña **Instance**.

Paso 4 Haga clic en la instancia especificada y seleccione **Instance Configuration**.

De forma predeterminada, se muestra **Basic Configuration**. Para modificar más parámetros, haga clic en **All Configurations**. Todas las categorías de parámetros admitidas por la instancia se muestran en la página de pestaña **All Configurations**.

Figura 7-22 Configuraciones de instancias



Paso 5 En el árbol de navegación, seleccione la categoría de parámetros especificada y cambie los valores de los parámetros a la derecha.

Si no está seguro de la ubicación de un parámetro, puede escribir el nombre del parámetro en el cuadro de búsqueda en la esquina superior derecha. El sistema busca el parámetro en tiempo real y muestra el resultado.

Paso 6 Haga clic en **Save**. En el cuadro de diálogo de confirmación, haga clic en **OK**.

Espere hasta que aparezca el mensaje "Operation succeeded." Haga clic en **Finish**.

Se modifica la configuración.

NOTA

Una vez modificados los parámetros de configuración de una instancia de rol, debe reiniciar la instancia si el estado de la instancia es de **Expired**. Puede seleccionar la instancia caducada en la página **Instances** y elegir **More** > **Restart Instance**.

----Fin

Exportación/importación de la configuración de instancia

Paso 1 Inicie sesión en FusionInsight Manager.

Paso 2 Elija **Cluster** >*Name of the desired cluster* >**Services**.

Paso 3 Haga clic en el nombre del servicio especificado en la página de gestión de servicios. En la página mostrada, haga clic en la pestaña **Instance**.

Paso 4 Haga clic en la instancia especificada y seleccione **Instance Configurations**.

Paso 5 Haga clic en **Export** para exportar el archivo de parámetros de configuración al host local.

Paso 6 En la página **Instance Configurations**, haga clic en **Import**, seleccione el archivo de parámetros de configuración de la instancia e importe el archivo.

----Fin

7.2.3.4 Consulta del archivo de configuración de instancia

Escenario

FusionInsight Manager permite al personal de O&M ver los archivos de configuración de contenido, como las variables de entorno y las configuraciones de rol del nodo de instancia en la página de gestión. Si el personal de O&M necesita comprobar rápidamente si los elementos de configuración de la instancia están configurados incorrectamente o cuando es necesario ver algunos elementos de configuración ocultos, el personal de O&M puede ver directamente los archivos de configuración en FusionInsight Manager. En este caso, los usuarios analizan rápidamente los problemas de configuración.

Procedimiento

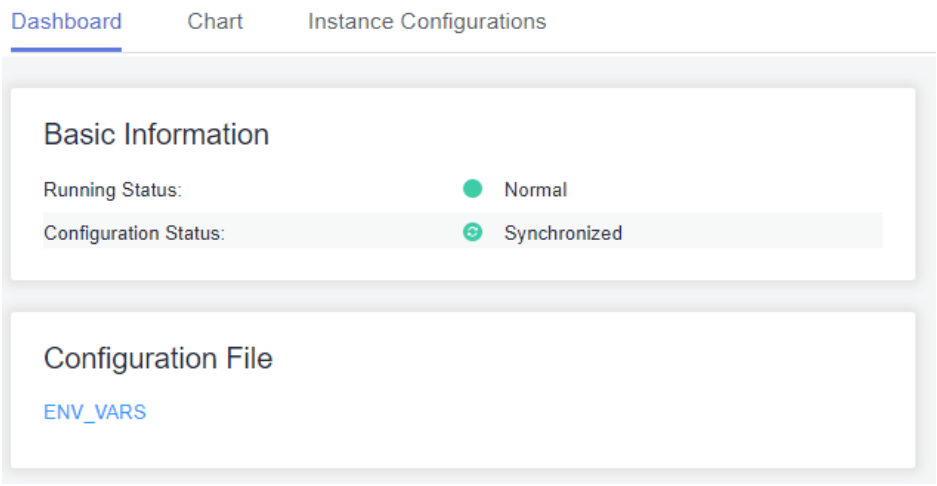
Paso 1 Inicie sesión en FusionInsight Manager.

Paso 2 Elija **Cluster** >*Name of the desired cluster* >**Service**.

Paso 3 Haga clic en el nombre del servicio especificado en la página de gestión de servicios. En la página mostrada, haga clic en la pestaña **Instance**.

Paso 4 Haga clic en el nombre de la instancia de destino. En el área **Configuration File** de la página **Instance Status**, se muestra la lista de archivos de configuración de la instancia.

Figura 7-23 Consulta del archivo de configuración de instancia



Paso 5 Haga clic en el nombre del archivo de configuración que se va a ver para ver los valores de los parámetros en el archivo de configuración.

Para obtener el archivo de configuración, puede descargar el archivo de configuración en el PC local.

NOTA

Si un nodo del clúster está defectuoso, no se puede ver el archivo de configuración. Rectifique el error antes de volver a ver el archivo de configuración.

----Fin

7.2.3.5 Grupo de instancias

7.2.3.5.1 Gestión de grupos de instancias

Escenario

Los grupos de instancias se pueden gestionar en FusionInsight Manager. Es decir, puede agrupar varias instancias en el mismo rol según un principio especificado, como los nodos con la misma configuración de hardware. La modificación de los parámetros de configuración de un grupo de instancias se aplica a todas las instancias del grupo.

En un clúster grande, los grupos de instancias se utilizan para mejorar la capacidad de gestionar instancias en lotes en el entorno heterogéneo. Después de agrupar las instancias, las instancias se pueden configurar repetidamente para reducir los elementos de configuración de instancias redundantes y mejorar el rendimiento del sistema.

Creación de un grupo de instancias

Paso 1 Inicie sesión en FusionInsight Manager.

Paso 2 Elija **Cluster** >*Name of the desired cluster* >**Services**.

Paso 3 Haga clic en el nombre del servicio especificado en la página de gestión de servicios.

Paso 4 En la página mostrada, haga clic en la pestaña **Instance Groups**.

Haga clic en y configure los parámetros según se le solicite.

Figura 7-24 Creación de un grupo de instancias

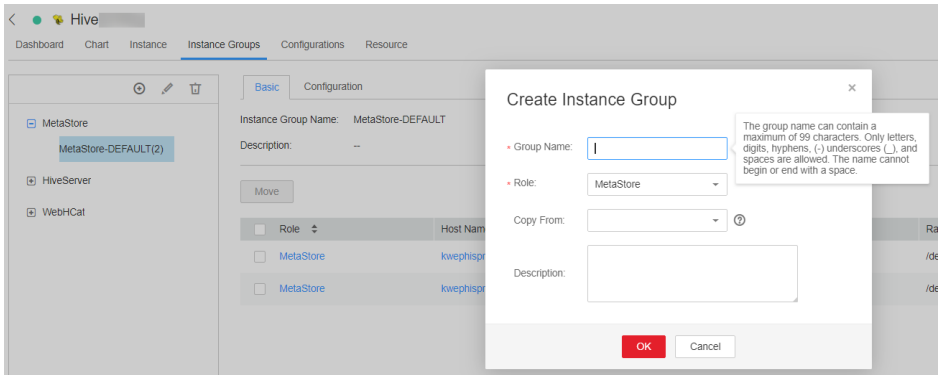


Tabla 7-13 Parámetros de configuración del grupo de instancias

Parámetro	Descripción
The group name	Indica el nombre del grupo de instancia. El valor solo puede contener letras, dígitos, guiones bajos (_), guiones (-) y espacios. Debe comenzar con una letra, un dígito, un guión bajo (_) o un guión (-) y no puede terminar con un espacio. Puede contener un máximo de 99 caracteres.
Role	Indica el rol al que pertenece un grupo de instancias.
Copy From	Indica que los valores de parámetros de un grupo de instancias especificado se copian en los parámetros de un nuevo grupo. Si el valor es nulo, se utilizan los valores predeterminados para los parámetros del nuevo grupo.
Description	Indica la descripción del grupo de instancias. Puede contener solo letras, dígitos, comas (,), puntos (.), guiones bajos (_), espacios y saltos de línea, y puede contener un máximo de 200 caracteres.

NOTA

- Cada instancia debe pertenecer a un solo grupo de instancias. Cuando se instala una instancia por primera vez, pertenece al grupo de instancias *Role name*-**DEFAULT** de forma predeterminada.
- Puede eliminar grupos de instancias innecesarios o no utilizados. Antes de eliminar un grupo de instancias, migre todas las instancias del grupo a otros grupos de instancias y, a continuación, elimine el grupo de instancias haciendo referencia a **Eliminación de un grupo de instancias**. No se puede eliminar el grupo de instancias predeterminado.

Paso 5 Haga clic en **OK**.

Se crea el grupo de instancias.

----Fin

Modificación de las propiedades de un grupo de instancias

Paso 1 Inicie sesión en FusionInsight Manager.

Paso 2 Elija **Cluster** >*Name of the desired cluster* >**Services**.

Paso 3 Haga clic en el nombre del servicio especificado en la página de gestión de servicios.

Paso 4 Haga clic en la pestaña **Instance Groups**. En la página de pestaña **Instance Groups**, busque la fila que contiene el grupo de instancias de destino.

Haga clic en y modifique los parámetros según se le solicite.

Paso 5 Haga clic en **OK** para guardar las modificaciones.

No se puede modificar el grupo de instancias predeterminado.

----Fin

Eliminación de un grupo de instancias

Paso 1 Inicie sesión en FusionInsight Manager.

Paso 2 Elija **Cluster** >*Name of the desired cluster* >**Services**.

Paso 3 Haga clic en el nombre del servicio especificado en la página de gestión de servicios.

Paso 4 Haga clic en la pestaña **Instance Groups**. En la página de pestaña **Instance Groups**, busque la fila que contiene el grupo de instancias de destino.

Paso 5 Haga clic en .

Paso 6 En el cuadro de diálogo que se muestra, haga clic en **OK**.

No se puede eliminar el grupo de instancias predeterminado.

----Fin

7.2.3.5.2 Consulta de información acerca de un grupo de instancias

Escenario

El administrador del clúster puede ver el grupo de instancias de un servicio especificado en el FusionInsight Manager.

Procedimiento

Paso 1 Inicie sesión en FusionInsight Manager.

Paso 2 Elija **Cluster** >*Name of the desired cluster* >**Services**.

Paso 3 Haga clic en el nombre del servicio especificado en la página de gestión de servicios.

Paso 4 En la página mostrada, haga clic en la pestaña **Instance Groups**.

Paso 5 En el árbol de navegación, seleccione un rol. En la página de pestaña **Basic**, vea todas las instancias del grupo de instancias.

NOTA

Para mover una instancia de un grupo de instancias a otro, realice las siguientes operaciones:

1. Seleccione la instancia que desea mover y haga clic en **Move**.
2. En el cuadro de diálogo que se muestra, seleccione un grupo de ejemplares al que se va a mover la instancia.

   Durante la migración, la configuración del nuevo grupo de instancias se hereda automáticamente. Si la configuración de la instancia se modifica antes de la migración, prevalecerá la configuración de la instancia.
3. Haga clic en **OK**.

   Reinicie el servicio o la instancia caducada para que la configuración surta efecto.

----Fin

7.2.3.5.3 Configuración de los parámetros del grupo de instancias

Escenario

En un clúster grande, los usuarios pueden configurar parámetros para varias instancias en lotes configurando los grupos de instancias relacionados en FusionInsight Manager, reduciendo los elementos de configuración de instancias redundantes y mejorando el rendimiento del sistema.

Procedimiento

Paso 1 Inicie sesión en FusionInsight Manager.

Paso 2 Elija **Cluster** >*Name of the desired cluster* >**Services**.

Paso 3 Haga clic en el nombre del servicio especificado en la página de gestión de servicios.

Paso 4 En la página mostrada, haga clic en la pestaña **Instance Groups**.

Paso 5 En el árbol de navegación, seleccione el nombre del grupo de instancias de un rol y cambie a la página de pestaña **Configuration**. Ajusta los parámetros que se van a modificar y haz clic en **Save**. La configuración tiene efecto para todas las instancias del grupo de instancias.

----Fin

7.3 Hosts

7.3.1 Página de gestión de host

7.3.1.1 Consulta de la lista de hosts

Descripción

Inicie sesión en el FusionInsight Manager, haga clic en **Hosts** y la lista de hosts se mostrará en la página de gestión de hosts. Puede ver la lista de hosts y la información básica de cada host.

Puede cambiar los tipos de vista y establecer criterios de búsqueda para filtrar y buscar hosts.

Vista del host

Puede hacer clic en **Role View** para ver los roles desplegados en cada host. Si el rol admite el modo activo/en espera, el nombre del rol se muestra en negrita.

Lista de hosts

La lista de hosts de la página de gestión de hosts contiene todos los hosts del clúster, y las operaciones O&M se pueden realizar en estos hosts.

En la página de gestión de hosts, puede filtrar hosts por tipo de nodo o clúster. Las reglas para filtrar los tipos de host son las siguientes:

- Un nodo de gestión es el nodo donde se implementa OMS. Además, los roles de control y los roles de datos también pueden implementarse en los nodos de gestión.
- Un nodo de control es el nodo donde se despliegan los roles de control. Además, los roles de datos también pueden desplegarse en nodos de control.
- Un nodo de datos es el nodo donde solo se implementan los roles de datos.

Si selecciona el **Host View**, se muestran la dirección IP, la planificación del rack, el nombre de zona de disponibilidad, el estado de ejecución, el nombre del clúster y el uso de recursos de hardware de cada host.

Tabla 7-14 Estado de ejecución del host

Estado	Descripción
Normal	Indica que el host está en el estado normal.
Faulty	Indica que el host es anormal.
Unknown	Indica que no se puede detectar el estado inicial del host.
Isolated	Indica que el host está aislado.
Suspended	Indica que el host está detenido.

7.3.1.2 Consulta del panel de control del host

Descripción

Inicie sesión en FusionInsight Manager, haga clic en **Hosts** y haga clic en un nombre de host en la lista de hosts. La página de detalles del host contiene el área de información básica, el área de estado del disco, el área de lista de funciones y el gráfico de monitoreo.

Área de información básica

El área de información básica contiene la información clave sobre el host, como la dirección IP de gestión, la dirección IP del servicio, el tipo de host, el rack, el firewall, el número de núcleos de CPU y el sistema operativo.

Área de estado del disco

El área de estado del disco contiene todas las particiones de disco configuradas para el clúster en el host y el uso de cada partición de disco.

Área de lista de instancias

El área de lista de instancias muestra todas las instancias de rol instaladas en el host y el estado de cada instancia de rol. Puede hacer clic en el archivo de registro junto al nombre de una instancia de rol para ver el contenido del archivo de registro de la instancia en línea.

Alarmas e historias de evento

El área de historial de alarmas y eventos muestra las alarmas y eventos clave reportados por el host actual. El sistema puede mostrar un máximo de 20 registros históricos.

Gráfico

El área del gráfico de monitoreo se muestra a la derecha de la página de detalles del host y contiene las métricas clave de monitoreo del host.

Puede elegir ▼ > **Customize** en la esquina superior derecha para personalizar los informes de monitoreo que se mostrarán en el área del gráfico. Seleccione un intervalo de tiempo y elija ▼ > **Export** para exportar datos detallados de métricas de monitoreo dentro del intervalo de tiempo especificado.

Puede hacer clic en  junto al título de un indicador de monitoreo para abrir la descripción del indicador de monitoreo.

Haga clic en la pestaña **Chart** del host para ver la información completa del gráfico de supervisión sobre el host.

Área de estado de la tarjeta GPU

Si el host está configurado con tarjetas GPU, el área de estado de la tarjeta GPU muestra el modelo, la ubicación y el estado de la tarjeta GPU instalada en el host.

7.3.1.3 Comprobación de procesos y recursos del host

Descripción

Inicie sesión en FusionInsight Manager, haga clic en **Hosts** y haga clic en el nombre de host especificado en la lista de hosts. En la página de detalles del host, haga clic en las pestañas **Process** y **Resource**.

Proceso de host

En la página de pestaña **Process**, se muestra la información sobre los procesos de rol de las instancias de servicio desplegadas en el host actual, incluido el estado del proceso, el PID y el tiempo de ejecución del proceso. Puede ver directamente los archivos de registro de cada proceso en línea.

Recurso de host

En la página de pestaña **Resource**, se muestra el uso detallado de recursos de las instancias de servicio desplegadas en el host actual, incluido el uso de CPU, memoria, disco y puerto.

7.3.2 Operaciones de mantenimiento del host

7.3.2.1 Inicio y detención de todas las instancias en un host

Escenario

Si un host es defectuoso, es posible que tenga que detener todos los roles en el host y realizar una comprobación de mantenimiento en el host. Una vez que se corrija el error del host, inicie todos los roles que se ejecuten en el host para recuperar los servicios del host. Puede iniciar o detener todas las instancias de un host en la página de gestión del host o en la página de detalles del host en FusionInsight Manager. A continuación se describe cómo realizar dichas operaciones en la página de gestión del host.

Procedimiento

Paso 1 Inicie sesión en FusionInsight Manager.

Paso 2 Haga clic en **Hosts**.

Paso 3 Seleccione el cuadro de verificación del host de destino.

Paso 4 Seleccione **Start All Instances** o **Stop All Instances** en la lista desplegable **More** para iniciar o detener todas las instancias de rol.

----Fin

7.3.2.2 Realización de una comprobación de estado del host

Escenario

Si el estado de ejecución de un host no es **Normal**, puede realizar comprobaciones de estado del host para comprobar si algunas funciones básicas son anormales. Durante la rutina O&M,

puede realizar comprobaciones de estado del host para asegurarse de que los parámetros de configuración y la supervisión de cada instancia de rol en el host son normales y pueden ejecutarse de forma estable durante mucho tiempo.

Procedimiento

Paso 1 Inicie sesión en FusionInsight Manager.

Paso 2 Haga clic en **Hosts**.

Paso 3 Seleccione el cuadro de verificación del host de destino.

Paso 4 Seleccione **Health Check** en la lista desplegable **More** para iniciar la comprobación de estado.

Para exportar el resultado de la comprobación de estado, haga clic en **Export Report** en la esquina superior izquierda. Si se detecta algún problema, haga clic en **Help**.

----Fin

7.3.2.3 Configuración de racks para hosts

Escenario

Todos los hosts de un clúster grande generalmente se despliegan en varios racks. Los hosts en diferentes racks se comunican entre sí a través de switches. El ancho de banda de red entre diferentes hosts en el mismo rack es mucho mayor que el de diferentes racks. En este caso, planifique la topología de red basándose en los siguientes requisitos:

- Para mejorar la velocidad de comunicación, se recomienda intercambiar datos entre hosts en el mismo rack.
- Para mejorar la capacidad de tolerancia a fallas, distribuya procesos o datos de servicios distribuidos en diferentes hosts de múltiples racks de la manera más dispersa posible.

Hadoop utiliza una estructura de directorios de archivos para representar hosts.

El HDFS no puede determinar automáticamente la topología de red de cada DataNode del clúster. Debe establecer el nombre del rack para identificar el rack donde se encuentra el host para que el NameNode pueda dibujar la topología de red de los DataNodes requeridos y realizar copias de respaldo de los datos de los DataNodes en diferentes racks. Del mismo modo, YARN necesita obtener información de rack y asignar tareas a diferentes NodeManagers según sea necesario.

Si cambia la topología de la red del clúster, debe reasignar racks para hosts en FusionInsight Manager para que los servicios relacionados se puedan ajustar automáticamente.

Impacto en el sistema

Si se cambia el nombre del rack host, la política de almacenamiento para las réplicas de HDFS, la asignación de tareas de YARN y la ubicación de almacenamiento de las particiones de Kafka se verán afectadas. Después de la modificación, debe reiniciar HDFS, YARN y Kafka para que la configuración surta efecto.

La configuración inadecuada del rack desequilibra las cargas (incluidas la CPU, la memoria, el disco y la red) entre los nodos del clúster, lo que reduce la confiabilidad y la estabilidad del

clúster. Por lo tanto, antes de asignar los bastidores, tenga en cuenta todos los aspectos y establezca correctamente racks.

Políticas de asignación de racks

NOTA

Rack físico: indica el rack real donde reside el host.

Rack lógico: indica el nombre del rack del host en FusionInsight Manager.

Política 1: Cada rack lógico tiene casi el mismo número de hosts.

Política 2: El nombre del rack lógico del host debe cumplir con el del rack físico al que pertenece el host.

Política 3: Si solo hay pocos hosts en un rack físico, combine este rack físico y otros racks físicos con pocos hosts en un rack lógico, que cumpla con la política 1. Los hosts de dos salas de equipos no se pueden colocar en un rack lógico. De lo contrario, pueden producirse problemas de rendimiento.

Política 4: Si hay muchos hosts en un rack físico, divida estos hosts en varios racks lógicos, lo que cumple con la política 1. Los hosts con grandes diferencias no deben colocarse en el mismo rack lógico. De lo contrario, se reducirá la confiabilidad del clúster.

Política 5: Se recomienda establecer **default** u otros valores para racks lógicos en la primera capa, y los valores en el mismo clúster deben ser coherentes.

Política 6: El número de hosts en cada rack no puede ser inferior a 3.

Política 7: Un clúster puede contener como máximo 50 racks lógicos. Si hay demasiados racks lógicos en un clúster, el mantenimiento es difícil.

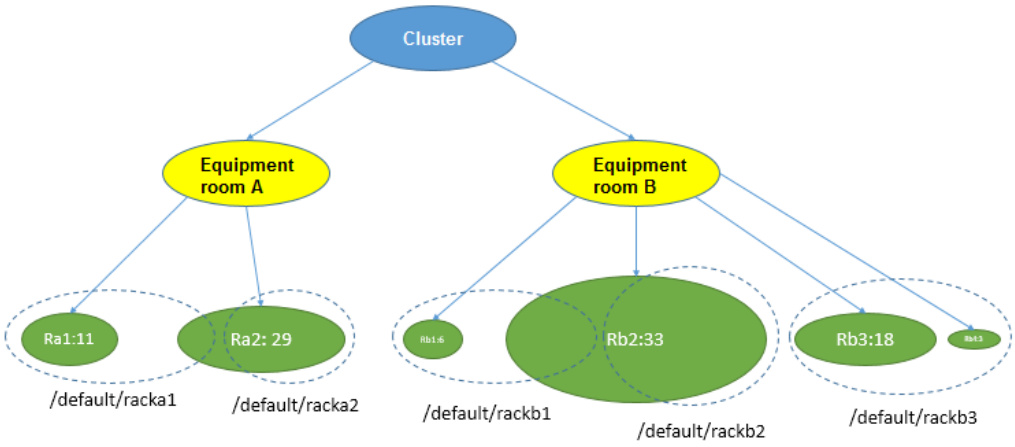
Prácticas recomendadas

Por ejemplo, en un clúster, 100 hosts están situados en dos salas de equipos A y B. A tiene 40 hosts y B tiene 60 hosts. En la sala A, hay 11 hosts en Ra1 de rack físico y 29 hosts en Ra2 de rack físico. En la sala B, hay seis hosts en el rack físico Rb1, 33 hosts en el rack físico Rb2, 18 hosts en el rack físico Rb3 y tres hosts en el rack físico Rb4.

De acuerdo con la política de asignación de rack, cada rack lógico contiene casi el mismo número (por ejemplo, 20) de hosts. Los detalles de la asignación son los siguientes:

- Rack lógico /default/racka1: 11 hosts en Ra1 de rack físico y nueve hosts en Ra2 de rack físico
- Rack lógico /default/racka2: los 20 hosts restantes (excepto los nueve hosts del rack lógico /default/racka1) en el rack físico Ra2
- Rack lógico /default/rackb1: seis hosts en rack físico Rb1 y 13 hosts en rack físico Rb2
- Rack lógico /default/rackb2: los 20 hosts restantes en el rack físico Rb2
- Rack lógico /default/rackb3:18 hosts en rack físico Rb3 y tres hosts en rack físico Rb4

Ejemplo de asignación de racks:



Procedimiento

Paso 1 Inicie sesión en FusionInsight Manager.

Paso 2 Haga clic en **Hosts**.

Paso 3 Seleccione el cuadro de verificación del host de destino.

Paso 4 Seleccione **Set Rack** en la lista desplegable **More**.

- Establezca los nombres de rack en jerarquía según la topología de red real. Separe racks de diferentes capas usando barras inclinadas (/).
- Las reglas de nomenclatura de rack son las siguientes:*/level1/level2/...* El número de niveles debe ser al menos 1, y el nombre no puede estar vacío. Un rack puede contener letras, dígitos y guiones bajos (_) y no puede superar los 200 caracteres.

  Por ejemplo, /default/rack0.
- Si los hosts del rack que se van a modificar contienen instancias de DataNode, asegúrese de que los niveles de nombre de rack de los hosts donde residen todas las instancias de DataNode son los mismos. De lo contrario, la configuración no se entrega.

Paso 5 Haga clic en **OK**.

----Fin

7.3.2.4 Aislamiento de un host

Escenario

Si un host es anormal o defectuoso y no puede proporcionar servicios o afecta al rendimiento del clúster, puede quitar el host del nodo disponible en el clúster temporalmente para que el cliente pueda tener acceso a otros nodos disponibles.

NOTA

Solo se pueden aislar nodos que no sean de gestión.

Impacto en el sistema

- Después de aislar un host, todas las instancias de rol del host se detendrán y no podrá iniciar, detener o configurar el host y todas las instancias del host.
- Para algunos servicios, después de aislar un host, algunas instancias en otros nodos no funcionan y el estado de configuración del servicio puede caducar.
- Después de aislar un host, no se pueden recopilar ni mostrar estadísticas sobre el estado de monitoreo y los datos indicadores del hardware y las instancias del host.
- Conservar el puerto SSH predeterminado (22) del nodo de destino. De lo contrario, la tarea descrita en esta sección fallará.

Procedimiento

Paso 1 Inicie sesión en FusionInsight Manager.

Paso 2 Haga clic en **Hosts**.

Paso 3 Seleccione la casilla de verificación del host que se va a aislar.

Paso 4 Seleccione **Isolate** en la lista desplegable **More**.

En el cuadro de diálogo que se muestra, introduzca la contraseña del usuario de inicio de sesión actual y haga clic en **OK**.

Paso 5 En el cuadro de diálogo de confirmación que se muestra, seleccione. "I confirm to isolate the selected hosts and accept possible consequences of service faults." Haga clic en **OK**.

Espere hasta que aparezca el mensaje "Operation succeeded" y haga clic en **Finish**.

El anfitrión se aísla con éxito y **Running Status** es de **Isolated**.

Paso 6 Inicie sesión en el host aislado como usuario **root** y ejecute el comando **pkill -9 -u omm** para detener los procesos de usuario **omm** en el nodo. A continuación, ejecute el comando **ps -ef | grep 'container' | grep '${BIGDATA_HOME}' | awk '{print $2}' | xargs -I '{}' kill -9 '{}'** para encontrar y detener el proceso del contenedor.

Paso 7 Cancele el estado de aislamiento del host antes de usar el host si ha rectificado la excepción o el error del host.

En la página **Hosts**, seleccione el host aislado y elija **More** > **Cancel Isolation**.

NOTA

Una vez cancelado el aislamiento, todas las instancias de rol en el host no se inician de forma predeterminada. Para iniciar instancias de rol en el host, seleccione el host de destino en la página Hosts y elija **More** > **Start All Instances**.

----Fin

7.3.2.5 Exportación de información de host

Escenario

Los administradores pueden exportar información sobre todos los hosts en FusionInsight Manager.

Procedimiento

Paso 1 Inicie sesión en FusionInsight Manager.

Paso 2 Haga clic en **Hosts**.

Paso 3 Especifique el estado de los hosts necesarios en el cuadro de lista desplegable en la esquina superior derecha o haga clic en **Advanced Search** para especificar hosts.

Paso 4 Haga clic en **Export All**, seleccione **TXT** o **CSV** para **Save As** y haga clic en **OK**.

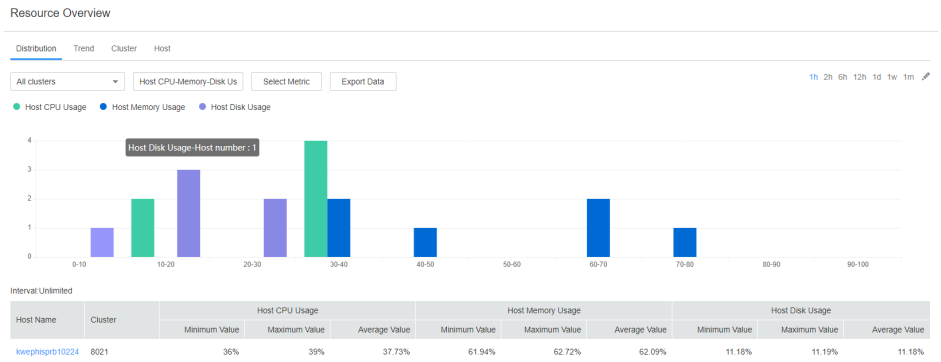
----Fin

7.3.3 Descripción de recursos

7.3.3.1 Distribución

Inicie sesión en el FusionInsight Manager y elija **Hosts** > **Resource Overview**. En la página **Resource Overview** que se muestra, haga clic en la pestaña **Distribution** para ver la distribución de recursos de cada clúster. De forma predeterminada, se muestran los datos de supervisión de la última hora (**1h**). Puede hacer clic en  para personalizar un intervalo de tiempo. Las opciones de rango de tiempo son **1h**, **2h**, **6h**, **12h**, **1d**, **1w** y **1m**.

Figura 7-25 Pestaña de distribución



- Puede hacer clic en **Select Metric** para personalizar la métrica que desea supervisar. **Tabla 7-15** describe todas las métricas que puede seleccionar. Después de seleccionar una métrica, se muestra la distribución del host en cada rango de la métrica.
- Cuando pasa el cursor sobre una columna de color, se muestra el número de hosts en el rango de métrica actual. Consulte **Figura 7-25**. Puede hacer clic en una columna de color para ver la lista de hosts en el rango de métricas.
  - Puede hacer clic en un nombre de host en la columna **Host Name** para acceder a la página de detalles del host.
  - Puede hacer clic en **View Trends** en la columna **Operation** de un host para ver los valores máximo, mínimo y promedio de la métrica actual en el clúster, así como el valor del host actual. En el clúster actual, si ha seleccionado **Host CPU-Memory-Disk Usage**, **View Trends** no está disponible.
- Puede hacer clic en **Export Data** para exportar los valores máximo, mínimo y promedio de la métrica actual de todos los nodos del clúster dentro del intervalo de tiempo especificado.

Tabla 7-15 Métricas

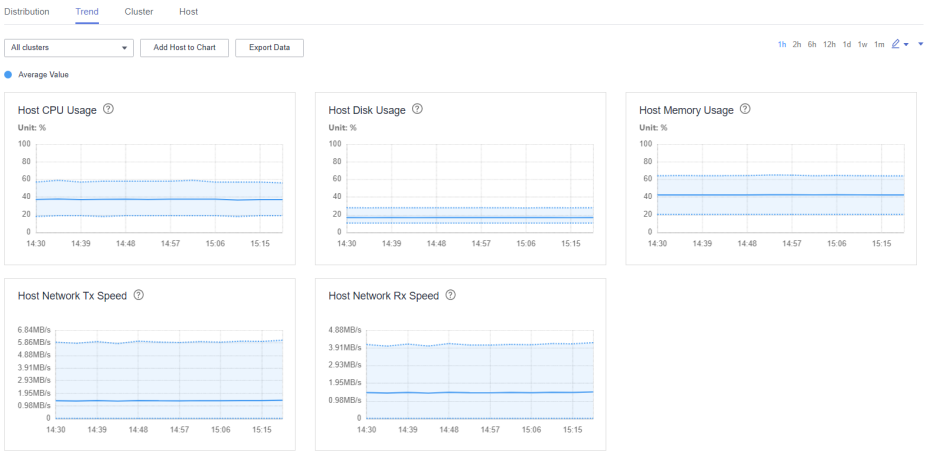
Categoría	Métrica
Proceso	● Número de procesos en ejecución ● Número total de procesos ● Número total de procesos de omm ● Proceso de suspensión ininterrumpida
Estado de red	● Colisiones de paquetes de red de host ● Número de estados de LAST_ACK ● Número de estados de CLOSING ● Número de estados de LISTENING ● Número de estados de CLOSED ● Número de estados de ESTABLISHED ● Número de estados de SYN_RECV ● Número de estados de TIME_WAITING ● Número de estados de FIN_WAIT2 ● Número de estados de FIN_WAIT1 ● Número de estados de CLOSE_WAIT ● Duración de resolución de nombre de DNS ● Uso del puerto efímero de TCP ● Errores de marco de paquetes de red de host
Lectura de red	● Paquetes de lectura de la red del host ● Paquetes perdidos de lectura de red de host ● Paquetes de error de lectura de red de host ● Velocidad de Rx de la red de host
Disco	● Velocidad de escritura en disco de host ● Disco utilizado en el host ● Disco libre en el host ● Velocidad de lectura del disco del host ● Uso del disco de host
Memoria	● Memoria libre ● Tamaño de memoria caché ● Tamaño total de memoria caché del kernel ● Tamaño de memoria compartida ● Uso de memoria de host ● Memoria utilizada

Categoría	Métrica
Escritura de red	● Paquetes de escritura en red de host ● Paquetes de error de escritura de red de host ● Velocidad de Tx de red de host ● Paquetes eliminados de escritura en red de host
CPU	● Uso de CPU de procesos cuyas prioridades han sido cambiadas ● Uso de CPU de procesos de espacio de usuario ● Uso de CPU de procesos de espacio del núcleo ● Uso de la CPU del host ● Tiempo total de CPU ● Tiempo de Idle de CPU
Estado de host	● Uso del handle de archivo de host ● Carga promedio del sistema operativo en 1 minuto ● Carga promedio del sistema operativo en 5 minutos ● Carga promedio del sistema operativo en 15 minutos ● Uso de PID de host

7.3.3.2 Tendencia

Inicie sesión en FusionInsight y elija **Hosts** > **Resource Overview**. En la página **Resource Overview** que se muestra, haga clic en la pestaña **Trend** para ver las tendencias de recursos de todos los clústeres o de un solo clúster. De forma predeterminada, se muestran los datos de supervisión de la última hora (**1h**). Puede hacer clic en para personalizar un intervalo de tiempo. Las opciones de rango de tiempo son **1h**, **2h**, **6h**, **12h**, **1d**, **1w** y **1m**. De forma predeterminada, el gráfico de tendencias de cada métrica muestra los valores máximo, mínimo y promedio de todo el clúster.

Figura 7-26 Pestaña de tendencia



- Puede hacer clic en **Add Host to Chart** para agregar líneas de tendencia de hasta 12 hosts a los gráficos de tendencias.
- Puede elegir ▼ > **Customize** para personalizar las métricas que se mostrarán en la página de pestaña. Para obtener más información sobre las métricas, consulte **Tabla 7-15** en **Distribución**.
- Puede hacer clic en **Export Data** para exportar los valores máximo, mínimo y promedio de todos los nodos del clúster para todas las métricas seleccionadas dentro del intervalo de tiempo especificado.

7.3.3.3 Clúster

Inicie sesión en el FusionInsight Manager y elija **Hosts** > **Resource Overview**. En la página **Resource Overview** que se muestra, haga clic en la pestaña **Cluster** para ver la supervisión de recursos de todos los clústeres.

De forma predeterminada, se muestran los datos de supervisión de la última hora (**1h**). Puede hacer clic en para personalizar un intervalo de tiempo. Las opciones de rango de tiempo son **1h**, **2h**, **6h**, **12h**, **1d**, **1w** y **1m**.

Figura 7-27 Pestaña de clúster

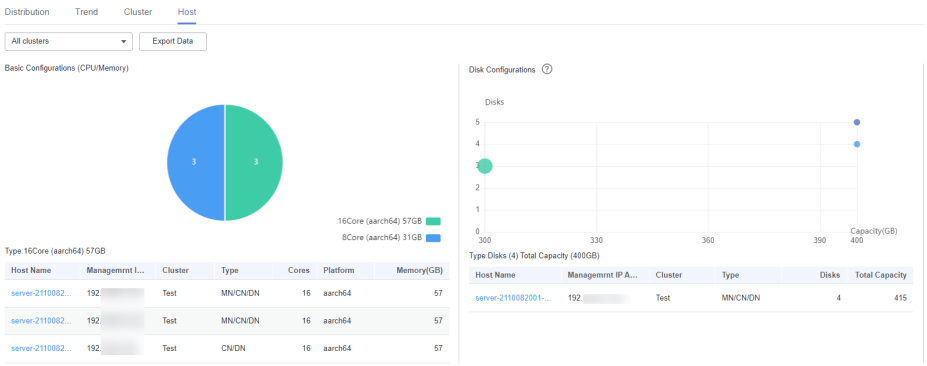
- Puede hacer clic en **Specify Cluster** para personalizar un clúster para mostrarlo.
- Puede elegir ▼ > **Customize** para personalizar las métricas que se mostrarán en la página de pestaña. Para obtener más información sobre las métricas, consulte **Tabla 7-15** en **Distribución**.
- Puede hacer clic en **Export Data** para exportar los valores de métrica de cada clúster dentro del intervalo de tiempo especificado.

7.3.3.4 Host

Inicie sesión en el FusionInsight Manager y elija **Hosts** > **Resource Overview**. En la página **Resource Overview** que se muestra, haga clic en la pestaña **Host** para ver la descripción general de los recursos del host, incluidas las configuraciones básicas (CPU/memoria) y las configuraciones de disco.

Puede hacer clic en **Export Data** para exportar la lista de configuración de todos los hosts del clúster, incluido el nombre del host, la dirección IP de gestión, el tipo de host, el número de núcleos, la arquitectura de la CPU, la capacidad de memoria y el tamaño del disco.

Figura 7-28 Pestaña de host



Configuraciones básicas (CPU/memoria)

Puede colocar el cursor sobre el gráfico circular para ver el número de hosts de cada configuración de hardware del clúster. La información se muestra en el formato de *Number of cores (CPU architecture) Memory size*.

Puede hacer clic en un segmento del gráfico circular para ver la lista de hosts.

Configuraciones de disco

El eje horizontal indica la capacidad total del disco (incluido el disco del sistema operativo) de un nodo, y el eje vertical indica el número de discos lógicos (incluido el disco del sistema operativo).

Puede colocar el cursor sobre un punto para ver información acerca de los discos de la configuración actual, incluida la cantidad de discos, la capacidad total y el número de hosts.

Puede hacer clic en un punto en el gráfico para ver la lista de hosts.

7.4 O&M

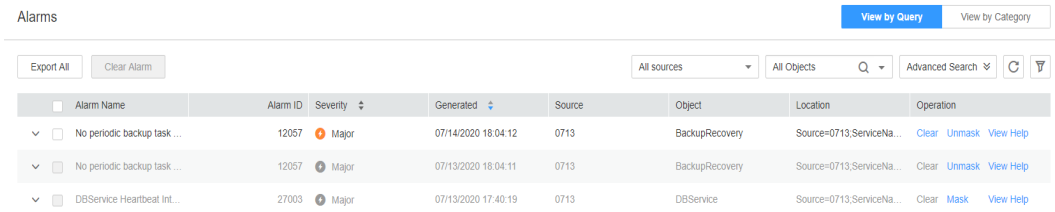
7.4.1 Alarmas

7.4.1.1 Descripción de alarmas y eventos

Alarmas

Inicie sesión en FusionInsight Manager y elija **O&M** > **Alarm** > **Alarms**. Puede ver la información sobre las alarmas reportadas por todos los clústeres en la página que se muestra en la **Figura 7-29**, incluidos el nombre de la alarma, el ID, la gravedad y el tiempo de generación. De forma predeterminada, las últimas 10 alarmas se muestran en cada página.

Figura 7-29 Alarmas



Puede hacer clic en ⌄ a la izquierda de una alarma para ver los parámetros detallados de la alarma. **Tabla 7-16** describe los parámetros.

Tabla 7-16 Parámetros de alarmas

Parámetro	Descripción
Alarm ID	ID de alarma
Alam Name	Nombre de la alarma
Severity	Severidad de alarma. Las opciones de valor son **Critical**, **Major**, **Minor** y **Suggestion**.
Generated	Hora en que se genera una alarma
Cleared	Hora en que se borra una alarma. Si la alarma no se borra, aparece **--**.
Source	Nombre del clúster
Object	Servicio, proceso o módulo que activa la alarma
Automaticall y Cleared	Si la alarma se puede borrar automáticamente después de rectificar la falla.
Alarm Status	Estado actual de la alarma. Las opciones de valor son **Auto**, **Manual** y **Uncleared**.
Alarm Cause	Indica la posible causa de una alarma.
Serial Number	Indica el número de alarmas generadas por el sistema.
Additional Information	Indica la información de error.
Location	Información detallada para localizar la alarma, que incluye lo siguiente: ● **Source**: clúster para el que se genera la alarma ● **ServiceName**: servicio para el que se genera la alarma ● **RoleName**: rol para el que se genera la alarma ● **HostName**: host para el que se genera la alarma

Gestión de alarmas.

- Haga clic en **Export All** para exportar todos los detalles de alarma.
- Si se han manejado varias alarmas, puede seleccionar una o más alarmas para borrarlas y hacer clic en **Clear Alarm** para borrar las alarmas por lotes. Se puede eliminar un máximo de 300 alarmas en cada lote.
- Puede hacer clic en para actualizar manualmente la página actual y hacer clic en para filtrar las columnas que se mostrarán.
- Puede filtrar las alarmas por objeto o clúster.
- Puede hacer clic en **Advanced Search** para buscar alarmas por ID de alarma, nombre, tipo, gravedad, hora de inicio o hora de finalización. Haga clic en **Search** para filtrar las alarmas que cumplan los criterios de búsqueda. Haga clic de nuevo en **Advanced Search** para ver el número de criterios de búsqueda que ha configurado.
- Puede hacer clic en **Clear**, **Mask** o **View Help** para realizar las operaciones correspondientes en una alarma.
- Si hay un gran número de alarmas, puede hacer clic en **View by Category** para ordenar las alarmas no claras por ID de alarma. Una vez clasificadas las alarmas, haga clic en el número de alarmas sin aclarar para ver los detalles de las alarmas.

Eventos

Inicie sesión en FusionInsight Manager y elija **O&M** > **Alarm** > **Events**. En la página **Events** que se muestra, puede ver información sobre todos los eventos del clúster, incluidos el nombre del evento, el ID, la gravedad, el tiempo de generación, el objeto y la ubicación. De forma predeterminada, los últimos 10 eventos se muestran en cada página.

Puede hacer clic en a la izquierda de un evento para ver los parámetros detallados del evento. **Tabla 7-17** describe los parámetros.

Tabla 7-17 Parámetros del evento

Parámetro	Descripción
Event ID	ID del evento
Event Name	Nombre del evento
Severity	Severidad del evento. Las opciones de valor son **Critical**, **Major**, **Minor** y **Suggestion**.
Generated	Hora en que se genera un evento
Object	Objeto para el que se puede generar el evento
Serial Number	Número del evento generado por el sistema
Location	Información detallada para localizar el evento, que incluye lo siguiente: ● **Source**: clúster para el que se genera el evento ● **ServiceName**: servicio para el que se genera el evento ● **RoleName**: rol para el que se genera el evento ● **HostName**: host para el que se genera el evento

Parámetro	Descripción
Additional Information	Indica la información de error.
Event Cause	Indica la posible causa de un evento.
Source	Nombre del clúster

Gestionar eventos.

- Haga clic en **Export All** para exportar todos los detalles del evento.
- Puede hacer clic en para actualizar manualmente la página actual y hacer clic en para filtrar las columnas que se mostrarán.
- Puede filtrar eventos por objeto o clúster.
- Puede hacer clic en **Advanced Search** para buscar eventos por ID de evento, nombre, gravedad, hora de inicio o hora de finalización.

7.4.1.2 Configuración del Umbral

Escenario

Puede configurar los umbrales de indicadores de supervisión para supervisar el estado de los indicadores en FusionInsight Manager. Si se producen datos anormales y se cumplen las condiciones preestablecidas, el sistema activa una alarma y muestra la información de alarma en la página de alarma.

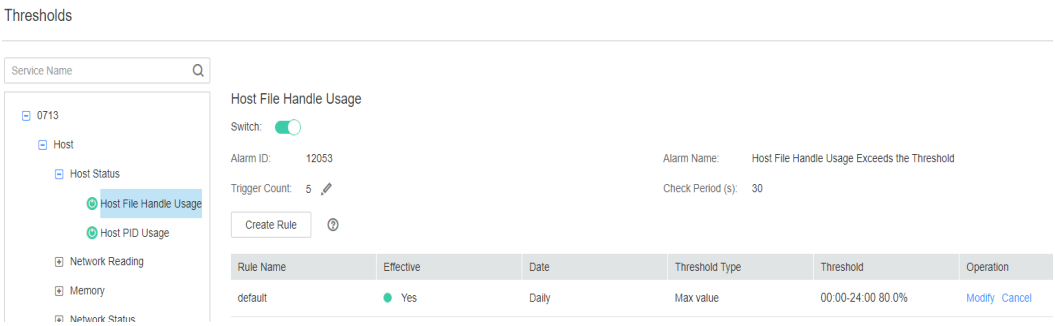
Procedimiento

Paso 1 Inicie sesión en FusionInsight Manager.

Paso 2 Elija **O&M** > **Alarm** > **Thresholds**.

Paso 3 Seleccione una métrica de supervisión para un host o servicio en el clúster.

Figura 7-30 Configuración del umbral para una métrica



Por ejemplo, después de seleccionar **Host Memory Usage**, se muestra la información acerca de este umbral de indicador.

- Si el interruptor de envío de alarma se muestra como  , se activa una alarma si se alcanza el umbral.
- **Alarm ID** y **Alarm Name**: información de alarma activada contra el umbral
- **Trigger Count**: FusionInsight Manager comprueba si el valor de una métrica de supervisión alcanza el umbral. Si el número de comprobaciones consecutivas alcanza el valor de **Trigger Count** se genera una alarma. **Trigger Count** es configurable.
- **Check Period (s)**: intervalo para que el sistema compruebe la métrica de monitorización.
- Las reglas de la lista de reglas se utilizan para activar alarmas.

Paso 4 Haga clic en **Create Rule** para agregar reglas utilizadas para los indicadores de supervisión.

Tabla 7-18 Parámetros de la regla del indicador de supervisión

Parámetro	Descripción	Valor de ejemplo
Rule Name	Nombre de una regla.	CPU_MAX
Severity	Gravedad de la alarma ● Critical ● Major ● Minor ● Warning	● Critical ● Major ● Minor ● Warning
Threshold Type	Puede utilizar el valor máximo o mínimo de un indicador como umbral de activación de alarma. Si **Threshold Type** se establece en **Max value**, el sistema genera una alarma cuando el valor del indicador especificado es mayor que el umbral. Si **Threshold Type** se establece en **Min value**, el sistema genera una alarma cuando el valor del indicador especificado es menor que el umbral.	● Max value ● Min value
Date	Este parámetro se utiliza para establecer la fecha en la que la regla entra en vigor.	● Daily ● Weekly ● Others
Add Date	Este parámetro solo está disponible cuando **Date** está establecido en **Others**. Puede establecer la fecha de entrada en vigor de la regla. Hay varias opciones disponibles.	09-30

Parámetro	Descripción	Valor de ejemplo
Thresholds	Este parámetro se utiliza para establecer el intervalo de tiempo cuando la regla entra en vigor.	Start and End Time: 00:00–08:30
	Umbral de la métrica de supervisión de reglas	Threshold: 10

NOTA

Puede hacer clic en  o para agregar o eliminar umbrales de tiempo.

Paso 5 Haga clic en **OK** para guardar las reglas.

Paso 6 Busque la fila que contiene una regla agregada y haga clic en **Apply** en la columna **Operation**. El valor de **Effective** para esta regla cambia a **Yes**.

Una nueva regla sólo se puede aplicar después de hacer clic en **Cancel** para una regla existente.

----Fin

Referencia de métrica de monitoreo

Las métricas de supervisión de alarmas de FusionInsight Manager se clasifican como métricas de información de nodo y métricas de servicio de clúster. **Tabla 7-19** describe las métricas para las que puede configurar umbrales en los nodos.

Tabla 7-19 Métricas de monitorización de nodos

Grupo métrico	Métrica	Descripción	Umbral predeterminado
CPU	Uso de la CPU del host	Este indicador refleja las capacidades de computación y control del clúster actual en un período de medición. Al observar el valor del indicador, puede comprender mejor el uso general de recursos del clúster.	90.0%
Disco	Uso de disco	Indica el uso del disco de un host.	90.0%

Grupo métrico	Métrica	Descripción	Umbral predeterminado
	Uso de Inode de disco	Indica el uso de inode de disco en un período de medición.	80.0%
Memoria	Uso de memoria de host	Indica el uso promedio de memoria en el momento actual.	90.0%
Estado de host	Uso del handle de archivo de host	Indica el uso de handles de archivo del host en un período de medición.	80.0%
	Uso de PID de host	Indica el uso de PID de un host.	90%
Estado de red	Uso del puerto efímero de TCP	Indica el uso de puertos TCP temporales del host en un período de medición.	80.0%
Lectura de red	Tasa de error de paquete de lectura	Indica la tasa de error de paquete de lectura de la interfaz de red en el host en un período de medición.	0.5%
	Tasa de paquetes perdidos de lectura	Indica la tasa de paquetes perdidos de lectura de la interfaz de red en el host en un período de medición.	0.5%
	Tasa de rendimiento de lectura	Indica el rendimiento de lectura promedio (en la capa MAC) de la interfaz de red en un período de medición.	80%

Grupo métrico	Métrica	Descripción	Umbral predeterminado
Escritura de red	Tasa de errores de paquetes de escritura	Indica la tasa de error de paquete de escritura de la interfaz de red en el host en un período de medición.	0.5%
	Tasa de paquetes perdidos de escritura	Indica la tasa de paquetes perdidos de escritura de la interfaz de red en el host en un período de medición.	0.5%
	Tasa de rendimiento de escritura	Indica el rendimiento promedio de escritura (en la capa MAC) de la interfaz de red en un período de medición.	80%
Proceso	Proceso de suspensión ininterrumpida	Número de procesos de estado D en el host en un período de medición	0
	Uso del proceso omm	Uso del proceso de omm en un período de medición	90

Tabla 7-20 Indicadores de servicio de clúster

Servicio	Nombre de grupo de indicador de monitoreo	Nombre de indicador	Descripción	Umbral predeterminado
DBService	Base de datos	Uso del número de conexiones de base de datos	Indica el uso del número de conexiones de base de datos.	90%
		Uso del espacio en disco del directorio de datos	Uso del espacio en disco del directorio de datos	80%

Servicio	Nombre de grupo de indicador de monitoreo	Nombre de indicador	Descripción	Umbral predeterminado
Flume	Agent	Calcular el uso de la memoria heap	Indica el uso de memoria heap de Flume.	95.0%
		Estadísticas de uso de memoria directa de Flume	Indica el uso de memoria directa de Flume.	80.0%
		Uso de memoria no heap de Flume	Indica el uso de memoria no heap de Flume.	80.0%
		Duración total de GC del proceso de Flume	Indica el tiempo total de GC de Flume.	12000 ms
HBase	GC	Tiempo de GC para generación antigua	Tiempo total de GC de RegionServer	5000 ms
		Tiempo de GC para generación antigua	Indica que el tiempo total de GC de HMaster.	5000 ms
	CPU & memoria	Estadísticas de uso de memoria directa de RegionServer	Indica el uso de memoria directa de theRegionServer Reg.	90%
		Estadísticas de uso de memoria heap de RegionServer	Indica el uso de memoria de heap de RegionServer.	90%
		Uso de memoria directa de HMaster	Indica el uso de memoria directa de HMaster.	90%
		Estadísticas de uso de memoria heap de HMaster.	Indica el uso de memoria heap de HMaster.	90%

Servicio	Nombre de grupo de indicador de monitoreo	Nombre de indicador	Descripción	Umbral predeterminado
	Servicio	Número de regiones en línea de un RegionServer	Número de regiones de un RegionServer	2000
		Región en recuento de transacciones por encima del umbral	Número de regiones que están en el estado RIT y alcanzan la duración umbral	1
	Replicación	Veces de error de sincronización de replicación (RegionServer)	Indica el número de veces que los datos de DR no se sincronizan.	1
		Número de archivos de registro que se van a sincronizar en el clúster activo	Número de archivos de registro que se sincronizarán en el clúster activo	128
		Número de HFiles que se van a sincronizar en el clúster activo	Número de HFiles que se van a sincronizar en el clúster activo	128
	Cola	Tamaño de la cola de Compaction	Tamaño de la cola de Compaction	100
HDFS	Archivo y bloque	Bloques perdidos	Indica el número de copias en bloque de las que carece el HDFS.	0
		Bloques bajo replicación	Número total de bloques que necesitan ser replicados por el NameNode	1000

Servicio	Nombre de grupo de indicador de monitoreo	Nombre de indicador	Descripción	Umbral predeterminado
	RPC	Tiempo promedio de procesamiento de RPC de NameNode activo	Indica el tiempo promedio de procesamiento de RPC.	100 ms
		Tiempo promedio de la cola RPC de NameNode activa	Indica el tiempo medio de cola de RPC.	200 ms
	Disco	Uso de disco HDFS	Indica el uso del disco HDFS.	80%
		Uso del disco DataNode	Indica el uso de disco de DataNodes en el HDFS.	80%
		Porcentaje de espacio reservado para réplicas de espacio no utilizado	Indica el porcentaje del espacio en disco reservado de todas las copias con respecto al espacio en disco total no utilizado de DataNodes.	90%
	Recurso	DataNodes defectuosos	Indica el número de DataNodes defectuosos.	3
		Estadísticas de uso de memoria no heap de NameNode	Indica el porcentaje de uso de memoria no heap de NameNode.	90%
		Estadísticas de uso de memoria directa de NameNode	Indica el porcentaje de memoria directa que utiliza NameNodes.	90%

Servicio	Nombre de grupo de indicador de monitoreo	Nombre de indicador	Descripción	Umbral predeterminado
		Estadísticas de uso de memoria heap de NameNode	Indica el porcentaje de uso de memoria no heap de NameNode.	95%
		Estadísticas de uso de memoria directa de DataNode	Indica el porcentaje de memoria directa que utiliza DataNodes.	90%
		Estadísticas de uso de memoria heap de DataNode	Uso de memoria heap de DataNode	95%
		Estadísticas de uso de memoria heap de DataNode	Indica el porcentaje de uso de memoria no heap de DataNode.	90%
	Recolección de basura	Tiempo de GC (NameNode)/ Tiempo de GC (DataNode)	Indica la duración de recolección de basura (GC) de NameNodes por minuto.	12000 ms
		Tiempo de GC	Indica la duración de GC de DataNodes por minuto.	12000 ms
Hive	HQL	Porcentaje de sentencias HQL ejecutadas con éxito por Hive	Indica el porcentaje de sentencias HQL que Hive ejecuta correctamente.	90.0%
	Fondo	Uso de subproceso de background	Uso de subprocesos de background	90%
	GC	Tiempo total de GC de MetaStore	Indica el tiempo total de GC de MetaStore.	12000 ms

Servicio	Nombre de grupo de indicador de monitoreo	Nombre de indicador	Descripción	Umbral predeterminado
		Tiempo total de GC en milisegundos	Indica el tiempo total de GC de HiveServer.	12000 ms
	Capacidad	Porcentaje de espacio HDFS utilizado por Hive con respecto al espacio disponible	Indica el porcentaje de espacio HDFS utilizado por Hive con respecto al espacio disponible.	85.0%
	CPU & memoria	Estadísticas de uso de memoria directa de MetaStore	Uso de memoria directa de MetaStore	95%
		Estadísticas de uso de memoria no heap de MetaStore	Uso de memoria no heap de MetaStore	95%
		Estadísticas de uso de memoria heap de MetaStore	Uso de memoria heap de MetaStore	95%
		Estadísticas de uso de memoria directa de HiveServer	Uso de memoria directa de HiveServer	95%
		Estadísticas de uso de memoria no heap de HiveServer	Uso de memoria no heap de HiveServer	95%
		Estadísticas de uso de memoria heap de HiveServer	Uso de memoria heap de HiveServer	95%

Servicio	Nombre de grupo de indicador de monitoreo	Nombre de indicador	Descripción	Umbral predeterminado
	Session	Porcentaje de Sessions conectadas al HiveServer con respecto al número máximo de Sessions permitidas por el HiveServer	Indica el porcentaje del número de sessions conectadas al HiveServer con respecto al número máximo de Sessions permitidas por el HiveServer.	90.0%
Kafka	Partición	Porcentaje de particiones que no están completamente sincronizadas	Indica el porcentaje de Partitions que no están completamente sincronizadas con el total de Partitions.	50%
	Otros	Porcentaje de Partition no disponible	Porcentaje de Partitions no disponibles de cada topic de Kafka	40%
		Uso de la conexión de usuario en Broker	Uso de conexiones de usuario en Broker	80%
	Disco	Uso del disco de Broker	Indica el uso del disco del disco donde se encuentra el directorio de datos del Broker.	80.0%
		Tasa de E/S de disco de un Broker	Uso de E/S del disco donde se encuentra el directorio de datos del Broker	80%

Servicio	Nombre de grupo de indicador de monitoreo	Nombre de indicador	Descripción	Umbral predeterminado
	Proceso	Duración de GC de Broker por minuto	Indica la duración de GC del proceso del Broker por minuto.	12000 ms
		Uso de memoria heap de Kafka	Indica el uso de memoria heap de Kafka.	95%
		Uso de memoria directa de Kafka	Indica el uso de memoria directa de Kafka.	95%
Loader	Memoria	Calcular uso de memoria heap	Indica el uso de memoria heap de Loader.	95%
		Uso de memoria directa de Loader	Indica el uso de memoria directa de Loader.	80.0%
		Uso de memoria no heap de Loader	Indica el uso de memoria no heap de Loader.	80%
	GC	Tiempo total de GC de Loader	Indica el tiempo total de GC de Loader.	12000 ms
MapReduce	Recolección de basura	Tiempo de GC	Indica el tiempo de GC.	12000 ms
	Recurso	Estadísticas de uso de memoria directa de JobHistoryServer	Indica el uso de memoria directa de JobHistoryServer.	90%
		Estadísticas de uso de memoria no heap de JobHistoryServer	Indica el uso de memoria no heap de JobHistoryServer.	90%

Servicio	Nombre de grupo de indicador de monitoreo	Nombre de indicador	Descripción	Umbral predeterminado
		Estadísticas de uso de memoria heap de JobHistoryServer	Indica el uso de memoria no heap de JobHistoryServer.	95%
Oozie	Memoria	Calcular uso de memoria heap	Indica el uso de memoria heap de Oozie.	95.0%
		Uso de memoria directa de Oozie	Indica el uso de memoria directa de Oozie.	80.0%
		Uso de memoria no heap de Oozie	Indica el uso de memoria no heap de Oozie.	80%
	GC	Duración total del GC de Oozie	Indica el tiempo total de GC de Oozie.	12000 ms
Spark2x	Memoria	Estadísticas de uso de memoria heap de JDBCServer2x	Uso de memoria heap de JDBCServer2x	95%
		Estadísticas de uso de memoria directa de JDBCServer2x	Uso de memoria directa de JDBCServer2x	95%
		Estadísticas de uso de memoria no heap de JDBCServer2x	Uso de memoria no heap de JDBCServer2x	95%
		Estadísticas de uso de memoria directa de JobHistory2x	Uso de memoria directa de JobHistory2x	95%
		Estadísticas de uso de memoria no heap de JobHistory2x	Uso de memoria no heap de JobHistory2x	95%

Servicio	Nombre de grupo de indicador de monitoreo	Nombre de indicador	Descripción	Umbral predeterminado
		Estadísticas de uso de memoria heap de JobHistory2x	Uso de memoria heap de JobHistory2x	95%
		Estadísticas de uso de memoria directa de IndexServer2x	Uso de memoria directa de IndexServer2x	95%
		Estadísticas de uso de memoria heap de IndexServer2x	Uso de memoria heap de IndexServer2x	95%
		Estadísticas de uso de memoria no heap de IndexServer2x	Uso de memoria no heap de IndexServer2x	95%
	Recuento de GC	Número de Full GC de JDBCServer2x	Número total de GC de JDBCServer2x	12
		Número de Full GC de JobHistory2x	Número total de GC de JobHistory2x	12
		Número de Full GC de IndexServer2x	Número total de GC de IndexServer2x	12
	Tiempo de GC	Tiempo total de GC en milisegundos	Tiempo total de GC de JDBCServer2x	12000 ms
		Tiempo total de GC en milisegundos	Tiempo total de GC de JobHistory2x	12000 ms
		Tiempo total de GC en milisegundos	Tiempo total de GC de IndexServer2x	12000 ms

Servicio	Nombre de grupo de indicador de monitoreo	Nombre de indicador	Descripción	Umbral predeterminado
Storm	Clúster	Número de supervisores disponibles	Indica el número de procesos de supervisor disponibles en el clúster en un período de medición.	1
		Uso de Slot	Indica el uso de slot en el clúster en un período de medición.	80.0%
	Nimbus	Calcular uso de memoria heap	Indica el uso de la memoria heap de Nimbus.	80%
Yarn	Recursos	Estadísticas de uso de memoria directa de NodeManager	Indica el porcentaje de memoria directa que utiliza NodeManagers.	90%
		Estadísticas de uso de memoria heap de NodeManager	Indica el porcentaje de uso de memoria heap de NodeManager.	95%
		Estadísticas de uso de memoria no heap de NodeManager	Indica el porcentaje de uso de memoria no heap de NodeManager.	90%
		Estadísticas de uso de memoria directa de ResourceManager	Indica el uso de memoria directa de Kafka.	90%
		Estadísticas de uso de memoria heap de ResourceManager	Indica el uso de memoria heap de ResourceManager.	95%

Servicio	Nombre de grupo de indicador de monitoreo	Nombre de indicador	Descripción	Umbral predeterminado
		Estadísticas de uso de memoria no heap de ResourceManager	Indica el uso de memoria no heap de ResourceManager.	90%
	Recolección de basura	Tiempo de GC	Indica la duración de GC de NodeManager por minuto.	12000 ms
		Tiempo de GC	Indica la duración de GC de ResourceManager por minuto.	12000 ms
	Otros	Aplicaciones fallidas de cola root	Número de tareas fallidas en la cola root	50
		Aplicaciones terminadas de la cola root	Número de tareas eliminadas en la cola root	50
	CPU & memoria	Memoria pendiente	Capacidad de memoria pendiente	83886080MB
	Aplicación	Solicitudes pendientes	Tareas pendientes	60
ZooKeeper	Conexión	Uso de conexiones de ZooKeeper	Indica el porcentaje de las conexiones utilizadas con respecto al total de conexiones de ZooKeeper.	80%
	CPU & memoria	Calcular uso de Directmemory	Indica el uso de memoria heap de ZooKeeper.	95%
		Calcular uso de memoria heap	Indica el uso de memoria directa de ZooKeeper.	80%

Servicio	Nombre de grupo de indicador de monitoreo	Nombre de indicador	Descripción	Umbral predeterminado
	GC	Duración de GC de ZooKeeper por minuto	Indica el tiempo de GC de ZooKeeper cada minuto.	12000 ms
meta	Operación de escritura de datos de OBS	Tasa de éxito para invocar a la API de escritura de OBS	Tasa de éxito para invocar a la API de lectura de datos de OBS	99.0%
	Operaciones de metadatos de OBS	Tiempo promedio para invocar a la API de metadatos de OBS	Tiempo promedio para invocar a la API de metadatos de OBS	500ms
		Tasa de éxito para invocar a la API de metadatos de OBS	Tasa de éxito para invocar a la API de metadatos de OBS	99.0%
	Operación de lectura de datos de OBS	Tasa de éxito para invocar a la API de lectura de datos de OBS	Tasa de éxito para invocar a la API de lectura de datos de OBS	99.0%
Ranger	GC	Duración de GC de UserSync	Duración de la recolección de basura (GC) de UserSync	12000 ms
		Duración de GC de RangerAdmin	Duración de GC de RangerAdmin	12000 ms
		Duración de GC de TagSync	Duración de GC de TagSync	12000 ms
	CPU & memoria	Uso de memoria no heap de UserSync	Uso de memoria no heap de UserSync	80.0%

Servicio	Nombre de grupo de indicador de monitoreo	Nombre de indicador	Descripción	Umbral predeterminado
		Uso de memoria directa de UserSync	Uso de memoria directa de UserSync	80.0%
		Uso de memoria heap de UserSync	Uso de memoria heap de UserSync	95.0%
		Uso de memoria no heap de RangerAdmin	Uso de memoria no heap de RangerAdmin	80.0%
		Uso de memoria heap de RangerAdmin	Uso de memoria heap de RangerAdmin	95.0%
		Uso de memoria directa de RangerAdmin	Uso de memoria directa de RangerAdmin	80.0%
		Uso de memoria directa de TagSync	Uso de memoria directa de TagSync	80.0%
		Uso de memoria no heap de TagSync	Uso de memoria no heap de TagSync	80.0%
		Uso de memoria heap de TagSync	Uso de memoria heap de TagSync	95.0%
ClickHouse	Cuota de clúster	Uso de la cuota de cantidad de servicio de Clickhouse en ZooKeeper	Cuota de los nodos de ZooKeeper utilizados por un servicio de ClickHouse	90%

Servicio	Nombre de grupo de indicador de monitoreo	Nombre de indicador	Descripción	Umbral predeterminado
		Uso de la cuota de capacidad del servicio Clickhouse de ZooKeeper	Cuota de capacidad del directorio de ZooKeeper utilizado por el servicio ClickHouse	90%

7.4.1.3 Configuración del estado de enmascaramiento de alarma

Escenario

Si no desea que FusionInsight Manager informe de las alarmas especificadas en los siguientes escenarios, puede enmascarar manualmente las alarmas.

- Algunas alarmas sin importancia y alarmas menores necesitan ser enmascaradas.
- Cuando un producto de terceros está integrado con FusionInsight, algunas alarmas del producto se duplican con las alarmas de FusionInsight y necesitan ser enmascaradas.
- Cuando el entorno de despliegue es especial, ciertas alarmas pueden ser reportadas falsamente y necesitan ser enmascaradas.

Después de enmascarar una alarma, las nuevas alarmas con el mismo ID que la alarma no se muestran en la página **Alarm** ni se cuentan. Todavía se muestran las alarmas notificadas.

Procedimiento

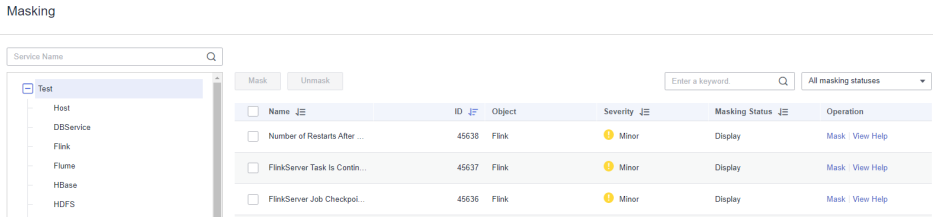
Paso 1 Inicie sesión en FusionInsight Manager.

Paso 2 Elija **O&M** > **Alarm** > **Masking Setting**.

Paso 3 En el área **Masking Setting**, seleccione el servicio o módulo especificado.

Paso 4 Seleccione una alarma de la lista de alarmas.

Figura 7-31 Enmascarar una alarma



Se muestra la información acerca de la alarma, incluidos el nombre de la alarma, ID, gravedad, estado de enmascaramiento y operaciones que se pueden realizar en la alarma.

- El estado de enmascaramiento incluye **Display** y **Masking**.
- Las operaciones incluyen **Masking** y **Help**.

NOTA

Puede filtrar las alarmas especificadas en función del estado de enmascaramiento y la gravedad de la alarma.

Paso 5 Establezca el estado de enmascaramiento de una alarma:

- Haga clic en **Masking**. En el cuadro de diálogo que se muestra, haga clic en **OK** para cambiar el estado de enmascaramiento de alarma a **Masking**.
- Haga clic en **Cancel Masking**. En el cuadro de diálogo que se muestra, haga clic en **OK** para cambiar el estado de enmascaramiento de la alarma a **Display**.

----Fin

7.4.2 Registro

7.4.2.1 Buscar registro en línea

Escenario

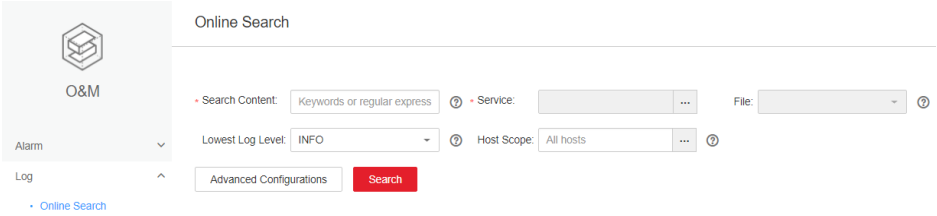
FusionInsight Manager le permite buscar registros en línea y ver el contenido del registro de los componentes para localizar fallas.

Procedimiento

Paso 1 Inicie sesión en FusionInsight Manager.

Paso 2 Elija **O&M** > **Log** > **Online Search**.

Figura 7-32 Búsquedas en línea



Paso 3 Configure los parámetros en **Tabla 7-21** para buscar los registros que necesita. Puede seleccionar una duración de búsqueda de registro predeterminada (incluidos **0.5h**, **1h**, **2h**, **6h**, **12h**, **1d**, **1w** y **1m**) o hacer clic en para personalizar **Start Data** y **End Data**.

Tabla 7-21 Parámetros de búsqueda de registro

Parámetro	Descripción
Search Content	Palabras clave o expresión regular a buscar

Parámetro	Descripción
Service	Servicio o módulo para el que desea consultar los registros
File	Archivos de registro que se buscarán cuando solo se seleccione un rol
Lowest Log Level	Nivel más bajo de registros a consultar. Después de seleccionar un nivel, se muestran los registros de este nivel y niveles superiores. Los niveles en orden ascendente son los siguientes: TRACE < DEBUG < INFO < WARN < ERROR < FATAL
Host Scope	● Puede hacer clic en ... para seleccionar hosts. ● Introduzca el nombre de host del nodo para el que desea consultar los registros o la dirección IP del plano de gestión. ● Utilice comas (,) para separar direcciones IP, por ejemplo, **192.168.10.10**,**192.168.10.11**. ● Utilice guiones (-) para indicar un segmento de dirección IP si las direcciones IP son consecutivas, por ejemplo, **192.168.10.[10-20]**. ● Utilice guiones (-) para indicar un segmento de dirección IP si las direcciones IP son consecutivas y use comas (,) para separar segmentos de dirección IP, por ejemplo, el **192.168.10.[10-20,30-40]**. **NOTA** – Si no se especifica este parámetro, todos los hosts se seleccionan de forma predeterminada. – Se puede introducir un máximo de 10 expresiones a la vez. – Se puede comparar un máximo de 2,000 hosts para todas las expresiones introducidas a la vez.
Advanced Configurations	● **Max Quantity**: número máximo de registros que se pueden mostrar a la vez. Si el número de registros consultados excede el valor de este parámetro, se omitirán los registros más antiguos. Si este parámetro no está definido, el número máximo de registros que se pueden mostrar a la vez no está limitado. ● **Timeout Duration**: duración del tiempo de espera de la consulta de registro. Este parámetro se utiliza para limitar el tiempo máximo de consulta de registro en cada nodo. Cuando el tiempo de espera de la consulta, la consulta se detiene y los registros que se han buscado todavía se muestran.

Paso 4 Haga clic en **Search**. Tabla 7-22 describe los campos en los resultados de búsqueda.

Tabla 7-22 Parámetros en los resultados de búsqueda

Parámetro	Descripción
Time	Hora en que se genera una línea de registro

Parámetro	Descripción
Source Cluster	Clúster para el que se genera el registro
Host Name	Nombre de host del nodo donde se encuentra el archivo de registro que registra la línea de registro
Location	Ruta del archivo de registro que registra la línea de registro Haga clic en la información de ubicación para ir a la página de navegación del registro en línea. De forma predeterminada, se muestran 100 líneas de registros antes y 100 líneas después de la línea de registro. Puede hacer clic en **Load More** en la parte superior o inferior de la página para ver más registros. Haga clic en **Download** para descargar el archivo de registro en el PC local.
Line No.	Número de línea de una línea de registro en el archivo de registro
Level	Nivel de la línea de registro
Log	Contenido del registro

NOTA

Puede hacer clic en **Stop** para detener la búsqueda por la fuerza. Puede ver los resultados de la búsqueda en la lista.

Paso 5 Haga clic en **Filter** para filtrar los registros que se mostrarán en la página. **Tabla 7-23** enumera los campos que puede utilizar para filtrar los registros. Después de configurar estos parámetros, haga clic en **Filter** para buscar registros que cumplan los criterios de búsqueda. Puede hacer clic en **Reset** para borrar la información que ha completado.

Tabla 7-23 Parámetros para filtrar registros

Parámetro	Descripción
Keywords	Palabras clave de los perdidos que se buscarán
Host Name	Nombre del host que se buscará
Location	Ruta del archivo de registro que se buscará
Started	Hora de inicio de los registros que se buscarán
Completed	Hora de finalización de los registros que se buscarán
Source Cluster	Clúster en el que se deben buscar registros

----Fin

7.4.2.2 Descarga de registro

Escenario

FusionInsight Manager le permite exportar por lotes los registros generados en todas las instancias de cada servicio.

Procedimiento

Paso 1 Inicie sesión en FusionInsight Manager.

Paso 2 Elija **O&M** >**Log** >**Download**.

Paso 3 Seleccione un rango de descarga de registro:

1. **Service**: Haga clic en y seleccione un servicio.
2. **Host**: Ingrese la dirección IP del host donde se despliega el servicio. También puede hacer clic en para seleccionar el host requerido.
3. Haga clic en  en la esquina superior derecha y configure **Start Time** y **End Time**.

Paso 4 Haga clic en **Download**.

El paquete de registro descargado contiene la información de topología de la hora de inicio y la hora de finalización, lo que le ayuda a encontrar rápidamente el registro que necesita.

El nombre del archivo de topología tiene el formato **topo_<***Topology structure change time***>.txt**. El archivo contiene la dirección IP del nodo, el nombre de host y las instancias de servicio que residen en el nodo. (Los nodos OMS se identifican mediante **Manager:Manager**.)

Ejemplo:

```
192.168.204.124|suse-124|
DBService:DBServer;KrbClient:KerberosClient;LdapClient:SlapdClient;LdapServer:Slap
dServer;Manager:Manager;meta:meta
```

----Fin

7.4.3 Realizar una comprobación de estado

7.4.3.1 Consulta de una tarea de comprobación de estado

Escenario

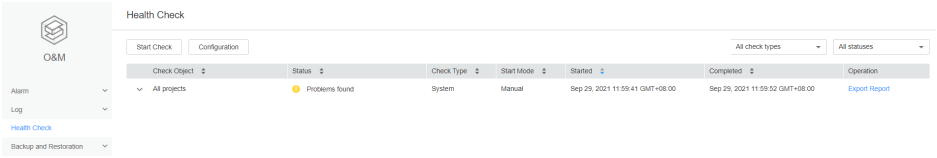
Los administradores pueden ver todas las tareas de comprobación de estado en el centro de gestión de comprobación de estado para comprobar si el clúster se ve afectado después de la modificación.

Procedimiento

Paso 1 Inicie sesión en FusionInsight Manager.

Paso 2 Elija **O&M** > **Health Check**.

Figura 7-33 Comprobación de estado



De forma predeterminada, se muestran todos los informes de comprobación de estado guardados. Los parámetros para un informe de comprobación de estado son los siguientes:

Tabla 7-24 Parámetros para un informe de comprobación de estado

Parámetro	Descripción
Check Object	Objeto a comprobar. Puede ampliar la lista para ver sus detalles.
Status	Compruebe el estado del resultado. Las opciones de valor son **No problems found**, **Problems found** y **Checking**.
Check Type	Entidad sobre la que se va a realizar la comprobación. Las opciones de valor son **System**, **Cluster**, **Host**, **Service** y **OMS**. Si selecciona **Cluster**, todos los elementos están marcados de forma predeterminada.
Start Mode	Si la comprobación de estado se realiza de forma automática o manual
Started	Hora de inicio de la comprobación
Completed	Hora de finalización de comprobación
Operation	Operaciones que puede realizar. Las opciones de valor son **Export Report** y **View Help**.

NOTA

- En la esquina superior derecha de la lista de comprobación, puede filtrar las comprobaciones de estado por tipo de comprobación o estado.
- Si **Check Type** es **Cluster**, **View Help** se muestra en la lista desplegable **Check Object**.
- Durante una comprobación de estado, el sistema determina si los objetos de comprobación están en buen estado basándose en sus datos históricos de métrica de monitoreo.

----Fin

7.4.3.2 Gestión de informes de comprobación de estado

Escenario

FusionInsight Manager le permite descargar y eliminar informes de comprobación de estado.

Procedimiento

Paso 1 Inicie sesión en FusionInsight Manager.

Paso 2 Elija **O&M** > **Health Check**.

Paso 3 Busque la fila que contiene el informe de comprobación de estado de destino y haga clic en **Export Report** en el **Operation** para descargar el informe.

----Fin

7.4.3.3 Modificación de configuración de comprobación de estado

Escenario

Los administradores pueden habilitar la comprobación automática del estado para reducir el tiempo de operación manual. De forma predeterminada, la comprobación de estado automática comprueba todo el clúster.

Procedimiento

Paso 1 Inicie sesión en FusionInsight Manager.

Paso 2 Elija **O&M** > **Health Check** > **Configuration**.

Periodic Health Check indica si se debe habilitar la comprobación de estado automática. Seleccione **Enable** para habilitar la comprobación automática de estado y seleccione **Disable** para deshabilitar la función.

Establezca el período de comprobación de estado en **Daily**, **Weekly** o **Monthly** según sea necesario.

Paso 3 Haga clic en **OK** para guardar las configuraciones.

----Fin

7.4.4 Configuración de copia de respaldo y restauración de copia de respaldo

7.4.4.1 Creación de una tarea de copia de respaldo

Escenario

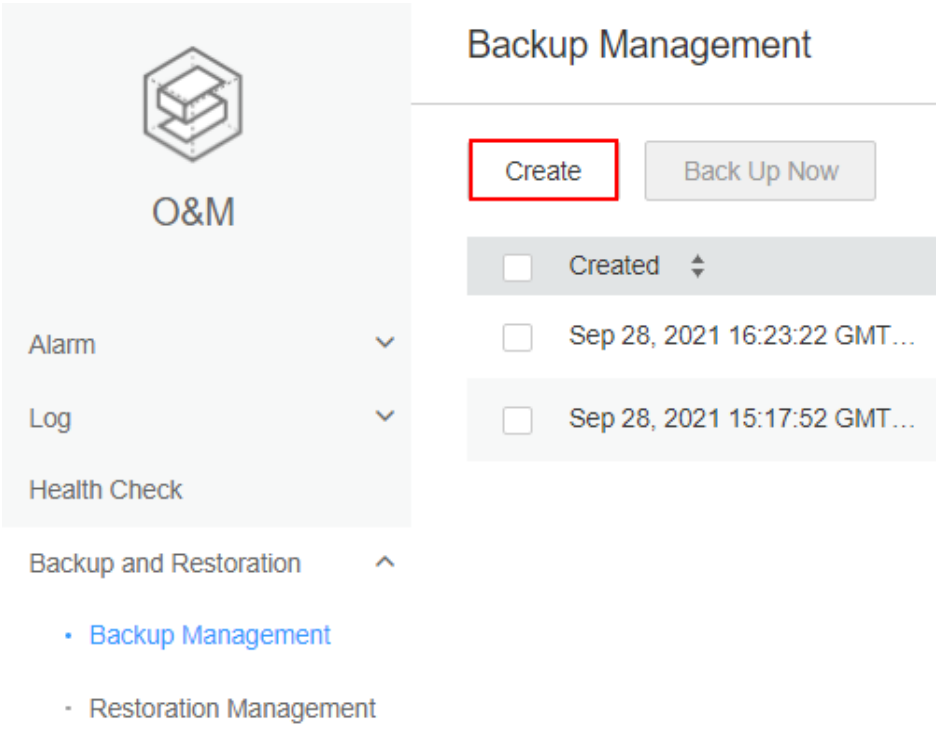
Puede crear tareas de copia de respaldo en FusionInsight Manager. La ejecución de tareas de copia de respaldo realiza copias de respaldo de los datos relacionados.

Procedimiento

Paso 1 Inicie sesión en FusionInsight Manager.

Paso 2 Elija **O&M** >**Backup and Restoration** >**Backup Management**. En la página que se muestra, haga clic en **Create**.

Figura 7-34 Creación de una tarea de copia de respaldo



Paso 3 Establezca **Backup Object** en **OMS** o en el clúster cuyos datos desea realizar una copia de respaldo.

Paso 4 Escriba un nombre de tarea en el cuadro de texto **Name**.

Paso 5 Establezca **Mode** en **Periodic** o **Manual** según sea necesario.

Tabla 7-25 Tipos de copia de respaldo

Tipo	Parámetro	Descripción
Periodic backup	Start Time	Indica la hora en que se inicia una tarea de copia de respaldo periódica por primera vez.
	Period	Intervalo de ejecución de tareas. Las opciones de valor son **Hours** y **Days**.
	Backup Policy	Se pueden seleccionar las siguientes políticas: ● Copia de respaldo completa la primera vez y copia de respaldo incremental posteriormente ● Copia de respaldo completa cada vez ● Copia de respaldo completa una vez cada n veces
Manual backup	N/A	Es necesario ejecutar manualmente la tarea para hacer una copia de respaldo de los datos.

Paso 6 Establezca los parámetros necesarios en el área **Configuration**.

- Se pueden realizar copias de respaldo de los metadatos y los datos de servicio.

- Para obtener más información sobre cómo realizar copias de respaldo de los datos de diferentes componentes, consulte **Copia de respaldo y gestión de recuperación**.

Paso 7 Haga clic en **OK** para guardar las configuraciones.

Paso 8 En la lista de tareas de copia de respaldo, puede ver la tarea de copia de respaldo creada.

Localice la fila que contiene la tarea de copia de respaldo de destino, elija **More** > **Back Up Now** en la columna **Operation** para ejecutar la tarea inmediatamente.

----Fin

7.4.4.2 Creación de una tarea de restauración de copia de respaldo

Escenario

Puede crear una tarea de restauración de copia de respaldo en FusionInsight Manager. Después de ejecutar la tarea de restauración, los datos de copia de respaldo especificados se restauran en el clúster.

Procedimiento

Paso 1 Inicie sesión en FusionInsight Manager.

Paso 2 Elija **O&M** >**Backup and Restoration** >**Restoration Management**. En la página que se muestra, haga clic en **Create**.

Paso 3 Configure **Task Name**.

Paso 4 Establezca **Recovery Object** en **OMS** o en el clúster cuyos datos desea restaurar.

Paso 5 Establezca los parámetros requeridos en el área **Recovery Configuration**.

- Los metadatos y los datos de servicio se pueden restaurar.
- Para obtener más información acerca de cómo restaurar datos de diferentes componentes, consulte **Copia de respaldo y gestión de recuperación**.

Paso 6 Haga clic en **OK** para guardar las configuraciones.

Paso 7 En la lista de tareas de restauración, puede ver las tareas de restauración creadas.

Busque la fila que contiene la tarea de restauración de destino, haga clic en **Start** en la columna **Operation** para ejecutar la tarea de restauración inmediatamente.

----Fin

7.4.4.3 Gestión de tareas de copia de respaldo y restauración de copias de respaldo

Escenario

También puede mantener y gestionar las tareas de restauración de copias de respaldo en el FusionInsight Manager.

Procedimiento

Paso 1 Inicie sesión en FusionInsight Manager.

Paso 2 Elija **O&M** > **Backup and Restoration** > **Backup Management** o **Restoration Management**.

Paso 3 En la columna **Operation** de la tarea especificada en la lista de tareas, seleccione la operación que se va a realizar.

Tabla 7-26 Operaciones de mantenimiento y gestión

Entrada de operación	Descripción
Config	Modifique los parámetros de la tarea de copia de respaldo.
Recover	Después de que algunos datos de servicio se hayan respaldado correctamente, puede utilizar esta función para restaurar los datos rápidamente.
More > **Back Up Now**	Realice esta operación para ejecutar la tarea de copia de respaldo inmediatamente.
More > **Stop**	Realice esta operación para detener una tarea en ejecución.
More > **Delete** or **Delete**	Esta operación se utiliza para eliminar tareas.
More > **Suspend**	Realice esta operación para deshabilitar la función de tarea de copia de respaldo automática.
More > **Resume**	Realice esta operación para habilitar la función de tarea de copia de respaldo automática.
More > **View History** or **View History**	Realice esta operación para cambiar a la página de registro de ejecución de tareas para ver los detalles de ejecución de tareas y la ruta de copia de respaldo.
View	Realice esta operación para comprobar la configuración de los parámetros de la tarea de restauración.
Start	Realice esta operación para ejecutar la tarea de restauración.

----Fin

7.5 Auditoría

7.5.1 Descripción

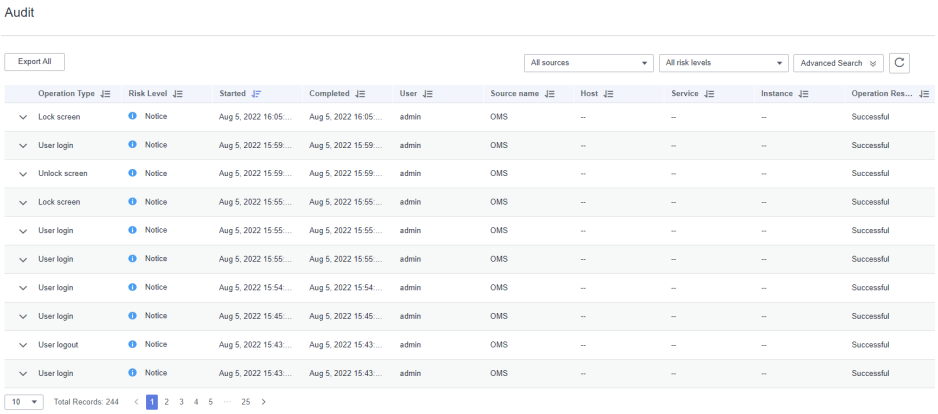
Escenario

La página **Audit** muestra las operaciones del usuario en Manager. En esta página, los administradores pueden ver las operaciones históricas de los usuarios en Manager. Para obtener más información sobre la auditoría, consulte **Registros de auditoría**.

Descripción

Inicie sesión en FusionInsight Manager y elija **Audit**. La página **Audit** muestra el tipo de operación, el nivel de riesgo, la hora de inicio, la hora de finalización, el usuario, el origen, el nombre de host, el servicio, la instancia y el resultado de la operación.

Figura 7-35 Lista de información de auditoría



- Puede seleccionar registros de auditoría en el nivel **Critical**, **Major**, **Minor** o **Notice** en la lista desplegable **All risk levels**.
- En **Advanced Search**, puede establecer criterios de filtro para consultar registros de auditoría.
  a. Puede consultar los registros de auditoría por gestión de usuarios, clúster, servicio y mantenimiento en la columna **Operation Type**.
  b. En la columna **Service**, puede seleccionar un servicio para consultar los registros de auditoría correspondientes.

     NOTA

     Puede seleccionar **--** para buscar registros de auditoría utilizando todos los demás criterios de búsqueda, excepto servicios.
  c. Puede consultar los registros de auditoría por resultado de la operación. Las opciones de valor son **All**, **Successful**, **Failed** y **Unknown**.
- Puede hacer clic en para actualizar manualmente la página actual o hacer clic en para filtrar las columnas que se muestran en la página.
- Haga clic en **Export All** para exportar toda la información de auditoría a la vez. La información de auditoría se puede exportar en formato **TXT** y **CSV**.

7.5.2 Configuración del volcado de registros de auditoría

Escenario

Los registros de auditoría del FusionInsight Manager se almacenan en la base de datos de forma predeterminada. Si los registros de auditoría se conservan durante mucho tiempo, el espacio en disco del directorio de datos puede ser insuficiente. Para almacenar registros de auditoría en otro servidor de archivado, los administradores pueden establecer los parámetros de volcado necesarios para volcar automáticamente estos registros. Esto facilita la gestión de los registros de auditoría.

Si no configura el volcado del registro de auditoría, el sistema guarda automáticamente los registros de auditoría en un archivo cuando el número de registros de auditoría alcanza 100,000 piezas. La ruta de guardado es de **${BIGDATA_DATA_HOME} /dbdata_om/dumpData/iam/operatelog** en el nodo de gestión activo. El formato de nombre de archivo es **OperateLog_store_***YY_MM_DD_HH_MM_SS***.csv**. El número máximo de archivos de registro de auditoría históricos es 50.

Procedimiento

Paso 1 Inicie sesión en FusionInsight Manager.

Paso 2 Elija **Audit** > **Configuration**.

Paso 3 Haga clic en el interruptor situado a la derecha de **Audit Log Dumping Flag**.

Audit Log Dump está deshabilitado de forma predeterminada. Si se muestra  , **Audit Log Dump** está activado.

Paso 4 Establezca los parámetros de volcado en función de la información proporcionada en el documento **Tabla 7-27**

Figura 7-36 Parámetros de volcado

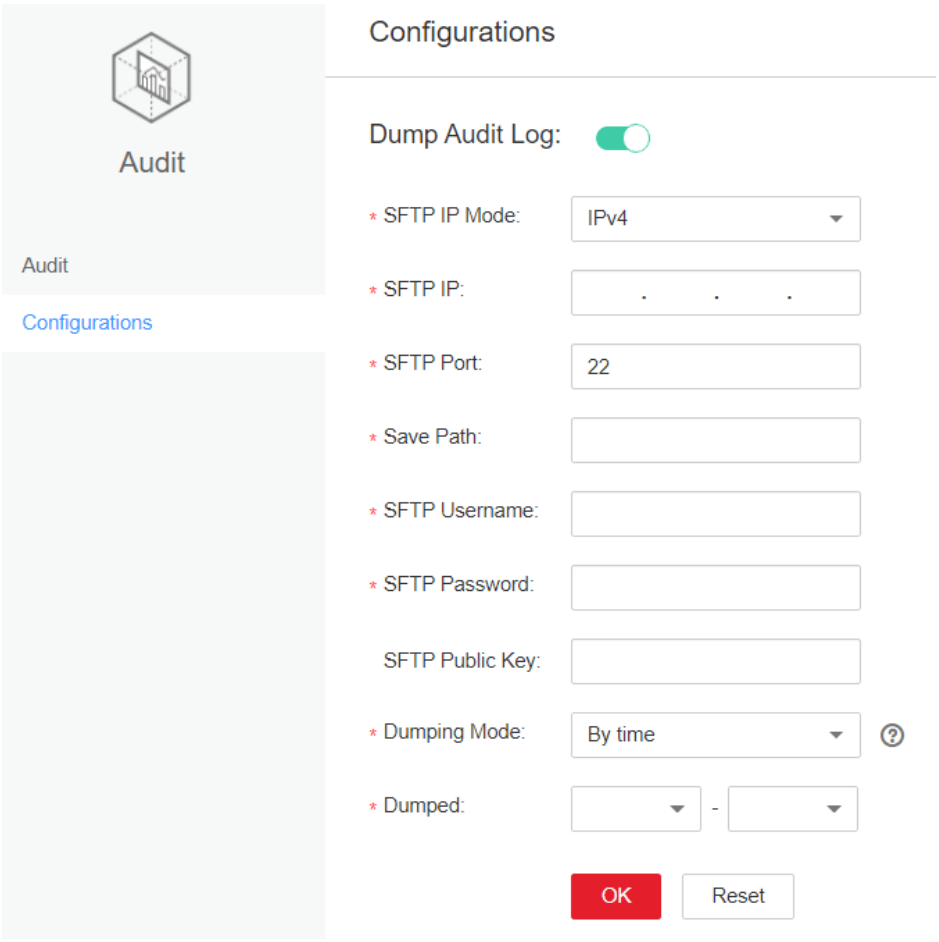


Tabla 7-27 Parámetros de volcado de registro de auditoría

Parámetro	Descripción	Valor
SFTP IP Mode	Modo de la dirección IP de destino. El valor puede ser **IPv4** o **IPv6**.	IPv4
SFTP IP	Servidor SFTP para almacenar registros de auditoría volcados. Se recomienda utilizar el servicio SFTP basado en SSH v2 para evitar riesgos de seguridad.	**192.168.10.51** (valor de ejemplo)
SFTP Port	Puerto de conexión del servidor SFTP para almacenar registros de auditoría volcados	**22** (valor de ejemplo)
Save Path	Ruta de acceso para almacenar registros de auditoría en el servidor SFTP	**/opt/omm/oms/auditLog** (valor de ejemplo)

Parámetro	Descripción	Valor
SFTP Username	Nombre de usuario para iniciar sesión en el servidor SFTP	**root** (valor de ejemplo)
SFTP Password	Contraseña para iniciar sesión en el servidor SFTP	*Password for logging into the SFTP server*
SFTP Public key	Especifica la clave pública del servidor SFTP. Este parámetro es opcional. Se recomienda establecer la clave pública del servidor SFTP. De lo contrario, pueden existir riesgos de seguridad.	-
Dumping Mode	Modo de volcado. Las opciones de valor son las siguientes: ● **By Quantity**: Si el número de piezas de registros alcanza el valor de este parámetro (**100000** por defecto), los registros se volcan. ● **By Time**: especifica la fecha en la que se vacian los registros. La frecuencia de volcado es una vez al año.	● By Quantity ● By Time
Dumping Date	Este parámetro solo está disponible cuando **Dumping Mode** está establecido en **By time**. Después de seleccionar una fecha de volcado, el sistema comienza a volcar en esta fecha. Los registros a ser volcados incluyen todos los registros de auditoría generados antes del 1 de enero de 00:00 del año en curso.	11-06

NOTA

Si la clave pública SFTP está vacía, el sistema muestra una advertencia de riesgo de seguridad. Evalúe el riesgo de seguridad y, a continuación, guarde la configuración.

Paso 5 Haga clic en **OK** para completar la configuración.

NOTA

Los campos clave en el archivo de volcado del registro de auditoría son los siguientes:

- **USERTYPE** indica el tipo de usuario. El valor **0** indica un usuario hombre-máquina, y el valor **1** indica un usuario máquina-máquina.
- **LOGLEVEL** indica el nivel de seguridad. El valor **0** indica Crítico, el valor **1** indica Mayor, el valor **2** indica Menor y el valor **3** indica Advertencia.
- **OPERATERESULT** indica el resultado de la operación. El valor **0** indica que la operación se ha realizado correctamente y el valor **1** indica que la operación ha fallado.

----Fin

7.6 Recursos para tenant

7.6.1 Multi-Tenancy

7.6.1.1 Descripción

Definición

Multi-tenancy se refiere a múltiples conjuntos de recursos (un conjunto de recursos es un tenant) en el clúster de big data de y es capaz de asignar y programar recursos. Los recursos incluyen recursos informáticos y recursos de almacenamiento.

Contexto

Los clústeres de datos de las empresas modernas se están volviendo cada vez más centralizados y basados en la nube. Los clústeres de big data de clase empresarial deben cumplir los siguientes requisitos:

- Llevar datos de diferentes tipos y formatos y ejecutar trabajos y aplicaciones de diferentes tipos (como análisis, consultas y procesamiento de secuencias).
- Aislar los datos de un usuario de los de otro usuario que tiene requisitos exigentes en materia de seguridad de datos, como un banco o un instituto gubernamental.

Los requisitos anteriores traen los siguientes desafíos a los clústeres de big data:

- Asignación y programación adecuadas de recursos para garantizar un funcionamiento estable de aplicaciones y trabajos.
- Control de acceso estricto para garantizar la seguridad de los datos y del servicio.

Multi-tenancy aísla los recursos de un clúster de big data en conjuntos de recursos. Los usuarios pueden arrendar los conjuntos de recursos deseados para ejecutar aplicaciones y trabajos y almacenar datos. En un clúster de big data, se pueden implementar varios conjuntos de recursos para satisfacer diversos requisitos de varios usuarios.

El clúster de big data de proporciona una solución de multitenant completa de big data de clase empresarial.

Características destacadas

- Configuración y aislamiento de recursos adecuados

  Los recursos de un tenant están aislados de los de otro tenant. El uso de recursos de un tenant no afecta a otros tenants. Este mecanismo garantiza que cada tenant pueda configurar los recursos en función de los requisitos de servicio, lo que mejora la utilización de los recursos.
- Medición y estadísticas del consumo de recursos

  Los tenants son solicitantes de recursos del sistema y consumidores. Los recursos del sistema se planifican y asignan en función de los tenants. El consumo de recursos por tenants puede ser medido y recolectado.
- Seguridad de datos garantizada y seguridad de acceso

En escenarios de multitenant, los datos de cada inquilino se almacenan por separado para garantizar la seguridad de los datos. El acceso a los recursos de tenants se controla para garantizar la seguridad del acceso.

7.6.1.2 Principios técnicos

7.6.1.2.1 Gestión de multitenant

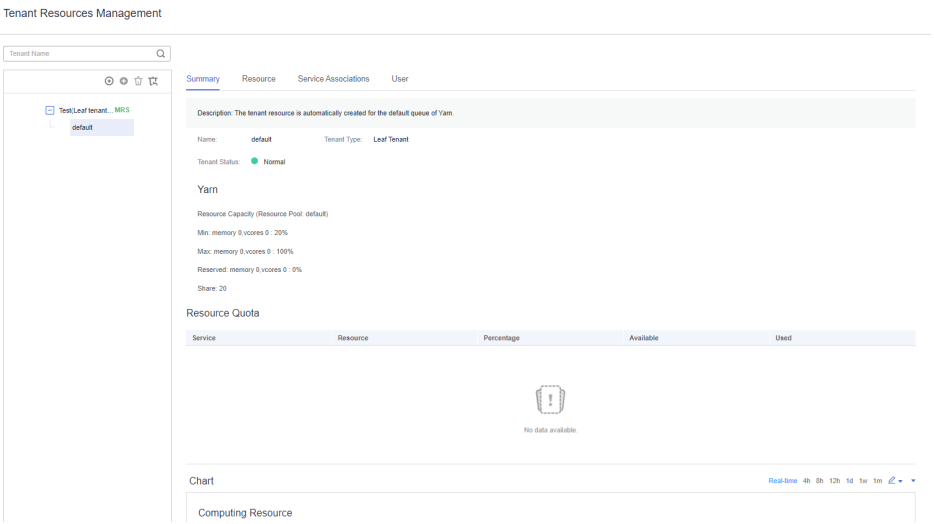
Gestión de multitenant unificado

Inicie sesión en FusionInsight Manager y elija **Tenant Resources** > **Tenant Resources Management**. En la página que se muestra, puede encontrar que FusionInsight Manager es una plataforma unificada de gestión de múltiples tenants que integra varias funciones, como la gestión del ciclo de vida del tenant, la configuración de recursos del tenant, la asociación de servicios del tenant y las estadísticas de uso de recursos del tenant, ofreciendo un modelo maduro de gestión de múltiples tenants y lograr una gestión centralizada de tenant y servicio.

Interfaz gráfica de usuario

FusionInsight Manager proporciona la interfaz gráfica de gestión de múltiples tenants y gestiona y opera varios niveles de tenants utilizando la estructura de árbol. Además, FusionInsight Manager integra la información básica y la cuota de recursos del tenant actual en una interfaz para facilitar O&M y la gestión, como se muestra en **Figura 7-37**.

Figura 7-37 Página de gestión de tenant del FusionInsight Manager



Gestión jerárquica de tenant

FusionInsight Manager admite un modelo jerárquico de gestión de tenant en el que puede agregar subtenants a un tenant existente para reconfigurar recursos. Los subtenants de los tenants de nivel 1 son tenants de nivel 2. Y así sucesivamente. FusionInsight Manager proporciona a las empresas un modelo de gestión de múltiples tenants probado en el campo, lo que permite la gestión centralizada de tenants y servicios.

Gestión de permisos simplificado

FusionInsight Manager oculta los detalles internos de la gestión de permisos de los usuarios comunes y simplifica las operaciones de gestión de permisos para los administradores, mejorando la usabilidad y la experiencia del usuario de la gestión de permisos de tenant.

- FusionInsight Manager emplea el control de acceso basado en roles (RBAC) para configurar diferentes permisos para los usuarios en función de escenarios de servicio durante la gestión de múltiples tenants.
- El administrador de tenants tiene permisos de gestión de tenant, que incluyen ver recursos y servicios del tenant actual, agregar o eliminar subtenants del inquilino actual y gestionar permisos de recursos de subtenants. FusionInsight Manager admite la configuración del administrador para un único tenant para que la gestión sobre este tenant se pueda delegar a un usuario que no sea el administrador del sistema.
- Los roles de un tenant tienen todos los permisos sobre los recursos informáticos y los recursos de almacenamiento del tenant. Cuando se crea un tenant, el sistema crea automáticamente roles para este tenant. Puede agregar un usuario y vincularlo a los roles de tenant para que el usuario pueda usar los recursos del tenant.

Gestión clara de recurso

- **Configuración de recursos de autoservicio**

  En FusionInsight Manager, puede configurar los recursos informáticos y los recursos de almacenamiento durante la creación de un tenant y agregar, modificar o eliminar los recursos del tenant.

  Los permisos de los roles asociados a un tenant se actualizan automáticamente cuando se modifican los recursos informáticos o de almacenamiento del tenant.

- **Estadísticas de uso de recurso**

  Las estadísticas de uso de recursos son fundamentales para que los administradores determinen las actividades O&M en función del estado de las aplicaciones y servicios de clústeres, lo que mejora la eficiencia de O&M del clúster. FusionInsight Manager muestra las estadísticas de recursos de tenants en **Resource Quota** incluidos los vCores, la memoria y los recursos de almacenamiento de HDFS.

  NOTA

  - **Resource Quota** calcula dinámicamente el uso de recursos de tenants.

Service	Resource	Percentage	Available	Used
HDFS	Space	0.00%	20.00 GB	0 MB
Yarn	Memory	0.00%	8.00 GB	0 MB
Yarn	CPU	0.00%	4 vCores	0 vCores

    Los recursos disponibles del programador Superior se calculan de la siguiente manera:

    - Superior

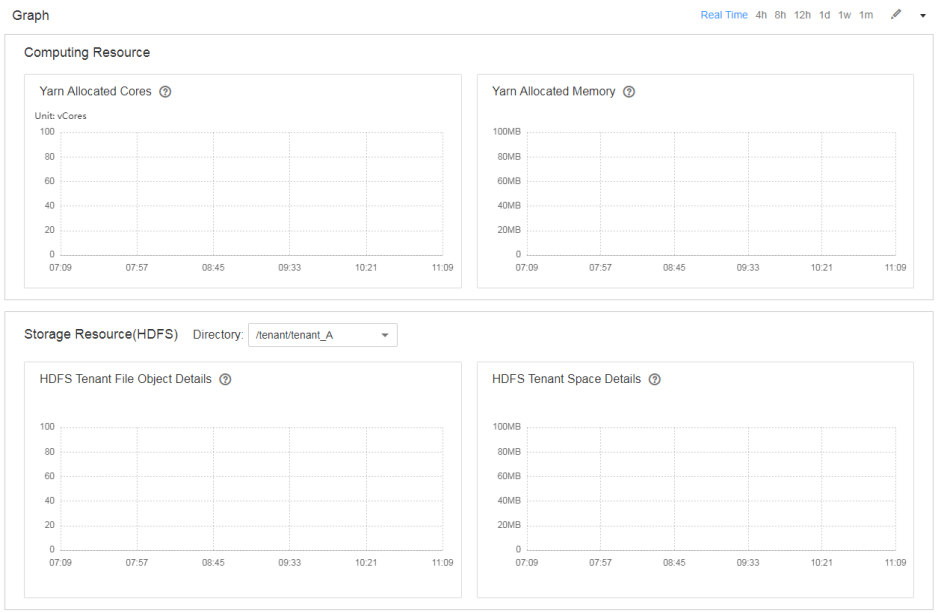
      Los recursos de Yarn disponibles (memoria y CPU) se asignan en proporción en función de la ponderación de la cola.

  - Cuando el administrador del tenant está vinculado a un rol de tenant, el administrador del tenant tiene los permisos para gestionar al tenant y usar todos los recursos del tenant.

- **Monitoreo de recurso gráfico**

  El monitoreo gráfico de recursos admite la visualización gráfica de las métricas de monitoreo enumeradas en **Tabla 7-28**, como se muestra en **Figura 7-38**.

Figura 7-38 Monitoreo preciso



De forma predeterminada, se muestran los datos de supervisión en tiempo real. Puede hacer clic en para personalizar un intervalo de tiempo. Los intervalos de tiempo predeterminados incluyen 4 horas, 8 horas, 12 horas, 1 día, 1 semana y 1 mes. Haga clic en y seleccione **Export** para exportar la información de la métrica de supervisión.

Tabla 7-28 Métricas de monitoreo

Servicio	Elemento métrico	Descripción
HDFS	Detalles de espacio de tenant de HDFS ● Espacio asignado ● Espacio utilizado	HDFS puede supervisar un directorio de almacenamiento especificado. El directorio de almacenamiento es el mismo que el directorio agregado por el tenant actual de **Resource**.
	Detalles de objeto de archivo de tenant de HDFS ● Número de objetos de archivo usados	
Yarn	Núcleos asignados de Yarn ● Número máximo de núcleos de CPU en un AM ● Núcleos asignados ● Número de núcleos de CPU usados en un AM	Se muestra la información de monitoreo del tenant actual. Si no se configura ningún elemento secundario para un tenant, esta información no se muestra. Los datos de monitoreo se obtienen de **Scheduler** > **Application Queues** > **Queue:** *Tenant name* en la web UI nativa de Yarn.

Servicio	Elemento métrico	Descripción
	Memoria asignada de Yarn ● Memoria máxima asignada de AM ● Memoria asignada ● Memoria usada de AM	

7.6.1.2.2 Modelo de multitenant

Modelo relacionado

En la siguiente figura se muestra un modelo multitenant.

Figura 7-39 Modelo de multitenant

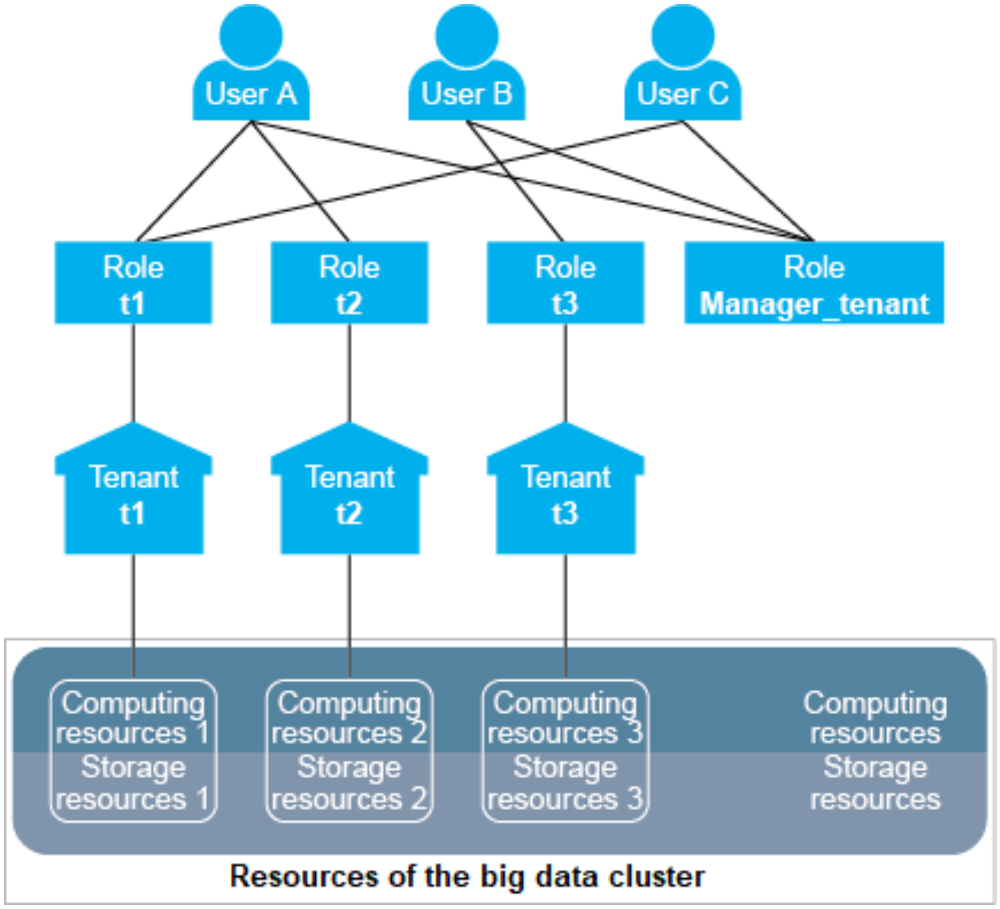


Tabla 7-29 describe los conceptos involucrados en **Figura 7-39**.

Tabla 7-29 Conceptos en el modelo

Concepto	Descripción
Usuario	Una persona física que tiene un nombre de usuario y contraseña y utiliza el clúster de big data. Hay tres usuarios diferentes en **Figura 7-39**: el usuario A, el usuario B y el usuario C.
Rol	Un rol es un portador de uno o más permisos. Los permisos se asignan a objetos específicos, por ejemplo, permisos de acceso para el directorio **/tenant** en HDFS. **Figura 7-39** muestra cuatro roles: **t1**, **t2**, **t3** y **Manager_tenant**. ● Los roles **t1**, **t2** y **t3** se generan automáticamente cuando se crean los tenants. Los nombres de los roles son los mismos que los nombres del tenant. Es decir, los roles **t1**, **t2** y **t3** se asignan a los tenants **t1**, **t2** y **t3**. Los nombres de roles y los nombres de tenant deben usarse en pareja. ● El rol **Manager_tenant** está predeterminado en el clúster y no se puede usar por separado.
Tenant	Un tenant es un conjunto de recursos en un clúster de big data. Los tenants múltiples se denominan multi-tenancy. Los conjuntos de recursos divididos adicionalmente bajo un tenant se denominan sub-tenants. **Figura 7-39** muestra tres tenants: **t1**, **t2** y **t3**.
Recurso	● Los recursos informáticos incluyen CPU y memoria. Los recursos informáticos de un tenant se asignan a partir del total de recursos informáticos en el clúster. Un tenant no puede ocupar los recursos informáticos de otro tenant. En **Figura 7-39**, se asignan recursos informáticos 1, 2 y 3 a los tenants **t1**, **t2** y **t3** respectivamente a partir de los recursos informáticos del clúster. ● Los recursos de almacenamiento incluyen discos y sistemas de almacenamiento de terceros. Los recursos de almacenamiento de un tenant se asignan a partir del total de recursos de almacenamiento en el clúster. Un tenant no puede ocupar los recursos de almacenamiento de otro tenant. En el caso de **Figura 7-39**, los recursos de almacenamiento 1, 2 y 3 se asignan a los inquilinos **t1**, **t2** y **t3** respectivamente a partir de los recursos de almacenamiento del clúster.

If a user wants to use a tenant's resources or add or delete a sub-tenant of a tenant, the user needs to be bound to both the tenant role and role **Manager_tenant**. **Tabla 7-30 Tabla 7-30** lista los roles enlazados a cada usuario en **Figura 7-39**.

Tabla 7-30 Roles enlazados a cada usuario

Usuario	Rol	Permiso
Usuario A	● Rol **t1** ● Rol **t2** ● Rol **Manager_tenant**	● Utiliza los recursos de los tenants **t1** y **t2**. ● Agrega o elimina subtenants de tenants **t1** y **t2**.
Usuario B	● Rol **t3** ● Rol **Manager_tenant**	● Utiliza los recursos del tenant **t3**. ● Agrega o elimina subtenants de tenant **t3**.
Usuario C	● Rol **t1** ● Rol **Manager_tenant**	● Utiliza los recursos de tenant **t1**. ● Agrega o elimina subtenants de tenant **t1**.

Un usuario puede estar enlazado a varios roles, y un rol también puede estar enlazado a varios usuarios. Los usuarios se asocian con tenants después de estar vinculados a los roles de tenant. Por lo tanto, los tenants y los usuarios forman una relación de muchos a muchos. Un usuario puede usar los recursos de varios tenants, y varios usuarios pueden usar los recursos del mismo tenant. Por ejemplo, en **Figura 7-39**, el usuario A usa los recursos de tenants **t1** y **t2**, y los usuarios A y C usan los recursos de tenant **t1**.

NOTA

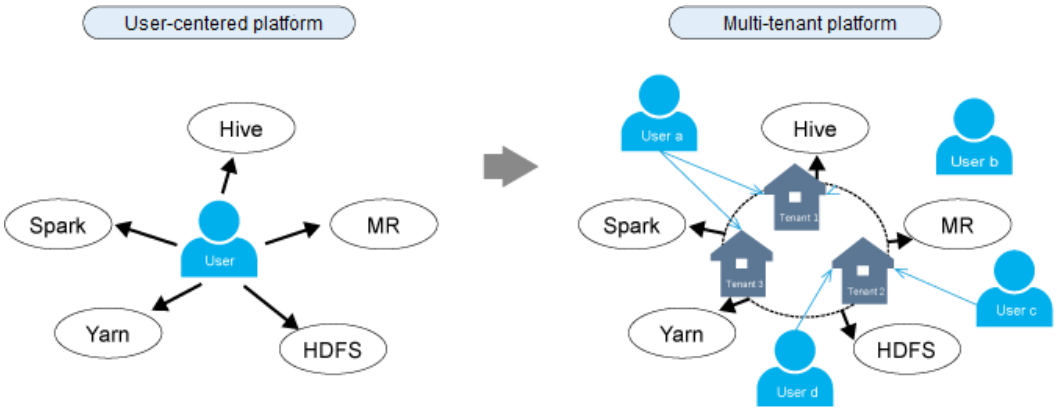
Los conceptos de un tenant principal, subtenant, tenant de nivel 1 e tenant de nivel 2 están diseñados para los escenarios de servicio multitenant. Preste atención a las diferencias de estos conceptos y los conceptos de un recurso de tenant de hoja y un recurso de tenant no hoja en FusionInsight Manager.

- Tenant de nivel 1: determinado en base al nivel del tenant. Por ejemplo, el primer tenant creado es un tenant de nivel 1 y su subtenant es un tenant de nivel 2.
- Tenant principal y subtenant: indica la relación jerárquica entre los tenants.
- Recurso de tenant no hoja: indica el tipo de tenant seleccionado durante la creación del tenant. Este tipo de tenant se puede utilizar para crear subtenants.
- Recurso de tenant de hoja: indica el tipo de tenant seleccionado durante la creación del tenant. Este tipo de tenant no se puede utilizar para crear subtenants.

Plataforma multitenant

Tenant es un concepto central de la plataforma de big data de FusionInsight. Desempeña un papel importante en la transformación de las plataformas de big data de centradas en el usuario a multiusuario para mantenerse al día con los entornos de aplicaciones multiusuario de las empresas. **Figura 7-40** muestra la transformación de las plataformas de big data.

Figura 7-40 Transformación de la plataforma de centrado en el usuario a multitenant



En una plataforma de big data centrada en el usuario, los usuarios pueden acceder y usar directamente todos los recursos y servicios.

- Sin embargo, las aplicaciones de usuario pueden utilizar solo recursos de clúster parciales, lo que resulta en una baja utilización de recursos.
- Los datos de diferentes usuarios pueden almacenarse juntos, disminuyendo la seguridad de los datos.

En una plataforma de big data de multitenant, los usuarios utilizan los recursos y servicios requeridos accediendo a los tenants.

- Los recursos se asignan y programan en función de los requisitos de la aplicación y se utilizan en función de tenants, lo que aumenta la utilización de los recursos.
- Los usuarios pueden acceder a los recursos de tenants solo después de estar asociados con roles de tenant, lo que mejora la seguridad de acceso.
- Los datos de tenants están aislados, lo que garantiza la seguridad de los datos.

7.6.1.2.3 Descripción de recursos

Los recursos de clúster de se clasifican en recursos informáticos y recursos de almacenamiento. La arquitectura multi-tenant implementa el aislamiento de recursos.

- **Computación de recursos**

  Los recursos informáticos incluyen CPU y memoria. Un tenant no puede ocupar los recursos informáticos de otro tenant.
- **Recursos de almacenamiento**

  Los recursos de almacenamiento incluyen discos y sistemas de almacenamiento de terceros. Un tenant no puede acceder a los datos de otro tenant.

Recursos de cómputo

Los recursos de computación se dividen en recursos de servicio estáticos y recursos dinámicos.

- **Recursos de servicio estático**

  Los recursos de servicio estático son recursos informáticos asignados a cada servicio y no se comparten entre servicios. Los recursos informáticos totales de cada servicio son fijos. Estos servicios incluyen Flume, HBase, HDFS e Yarn.

- **Recursos dinámicos**

  Los recursos dinámicos son recursos informáticos programados dinámicamente en una cola de trabajos por el servicio de gestión de recursos distribuidos Yarn. Yarn programa de forma dinámica los recursos para las colas de trabajos de MapReduce, Spark2x, Flink y Hive.

  NOTA

  Los recursos asignados a Yarn en un clúster de big data son recursos de servicio estáticos, pero Yarn puede asignarlos dinámicamente a colas de trabajos.

Recursos de almacenamiento

Los recursos de almacenamiento son recursos de almacenamiento de datos que el servicio de almacenamiento de archivos distribuido HDFS puede asignar. El directorio es la unidad básica de asignación de recursos de almacenamiento de HDFS. Tenants pueden obtener recursos de almacenamiento de los directorios especificados en el sistema de archivos de HDFS.

7.6.1.2.4 Recursos dinámicos

Descripción

Yarn proporciona gestión de recursos distribuidos para un clúster de big data. Se puede configurar el volumen total de recursos asignados a Yarn. A continuación, Yarn asigna y programa los recursos informáticos para las colas de trabajos. Yarn asigna y programa los recursos informáticos de las colas de trabajos de MapReduce, Spark, Flink y Hive.

Las colas de Yarn son unidades fundamentales de los recursos informáticos de programación.

Los recursos obtenidos por los tenants que usan colas de Yarn son recursos dinámicos. Los usuarios pueden crear y modificar dinámicamente las cuotas de cola y ver el estado y las estadísticas de las colas.

Grupos de recursos

Hoy en día, los sistemas de IT empresariales a menudo se enfrentan a entornos de clústeres complejos y diversos requisitos de capa superior. Por ejemplo:

- Clúster heterogéneo: La velocidad informática, la capacidad de almacenamiento y el rendimiento de la red de cada nodo del clúster son diferentes. Todas las tareas de las aplicaciones complejas deben asignarse correctamente a cada nodo informático del clúster en función de los requisitos de servicio.
- Aislamiento informático: Los datos deben compartirse entre varios departamentos, pero los recursos informáticos deben distribuirse en diferentes nodos informáticos.

Estos requieren que los nodos de cómputo sean particionados adicionalmente.

Los grupos de recursos se utilizan para especificar la configuración de los recursos dinámicos. Las colas de Yarn están asociadas con grupos de recursos para la asignación y programación de recursos.

Un tenant solo puede tener un grupo de recursos predeterminado. Los usuarios pueden estar vinculados al rol de un tenant para usar los recursos en el grupo de recursos del tenant. Para utilizar recursos en varios grupos de recursos, un usuario puede estar enlazado a roles de varios tenant.

Mecanismo de programación

Los recursos dinámicos de Yarn admiten la programación basada en etiquetas. Esta política crea etiquetas para nodos de proceso (Yarn NodeManagers) y agrega los nodos de proceso con la misma etiqueta al mismo grupo de recursos. A continuación, Yarn asocia dinámicamente las colas con grupos de recursos en función de los requisitos de recursos de las colas.

Por ejemplo, un clúster tiene más de 40 nodos que están etiquetados por **Normal**, **HighCPU**, **HighMEM** o **HighIO** en función de sus configuraciones de hardware y red y agregados en cuatro grupos de recursos, respectivamente. **Tabla 7-31** describe el rendimiento de cada nodo en el grupo de recursos.

Tabla 7-31 Rendimiento de cada nodo en un grupo de recursos

Etiqueta	Cantidad de nodos	Configuración de hardware y red	Agregado a	Asociado con
Normal	10	General	Grupo de recursos A	Cola común
HighCPU	10	CPU de alto rendimiento	Grupo de recursos B	Cola de computación intensiva
HighMEM	10	Memoria de gran capacidad	Grupo de recursos C	Cola con uso intensivo de memoria
HighIO	10	Red de alto rendimiento	Grupo de recursos D	Cola intensiva de E/S

Una cola puede utilizar solo los nodos de proceso en su grupo de recursos asociado.

- Una cola común está asociada con el grupo de recursos A y utiliza nodos **Normal** con configuraciones generales de hardware y red.
- Una cola informática intensiva está asociada con el grupo de recursos B y utiliza nodos **HighCPU** con CPU de alto rendimiento.
- Una cola que consume mucha memoria está asociada con el grupo de recursos C y utiliza nodos **HighMEM** con gran memoria.
- Una cola de E/S intensiva está asociada con el grupo de recursos C y utiliza nodos **HighIO** con red de alto rendimiento.

Las colas de Yarn se asocian con grupos de recursos especificados para utilizar de manera eficiente los recursos en grupos de recursos y maximizar el rendimiento de los nodos.

FusionInsight Manager admite un máximo de 50 grupos de recursos. El sistema tiene un grupo de recursos predeterminado.

Programadores

By default, the Superior scheduler is enabled for the cluster.

- El programador Superior es una versión mejorada y lleva el nombre del Lake Superior, lo que indica que el programador puede gestionar una gran cantidad de datos.

Para cumplir con los requisitos de la empresa y hacer frente a los desafíos de programación que enfrenta la comunidad Yarn, el programador Superior hace las siguientes mejoras:

- Política mejorada de uso compartido de recursos

  El programador Superior admite la jerarquía de colas. Integra las funciones de programadores de código abierto y comparte recursos basados en políticas configurables. En términos de instancias, los administradores pueden usar el programador Superior para configurar un valor absoluto o una política de porcentaje para los recursos de cola. La política de uso compartido de recursos del programador Superior mejora la programación basada en etiquetas de Yarn como una característica de grupo de recursos. Los nodos del clúster de Yarn se pueden agrupar en función de la capacidad o el tipo de servicio para garantizar que las colas puedan utilizar los recursos de manera más eficiente.

- Política de reserva de recursos basada en tenant

  Algunos tenants pueden ejecutar tareas críticas en algún momento, y sus necesidades de recursos deben abordarse preferentemente. El programador Superior construye un mecanismo para soportar la política de reserva de recursos. Los recursos reservados se pueden asignar a las tareas críticas que se ejecutan en las colas de tenant especificadas de manera oportuna para garantizar la correcta ejecución de la tarea.

- Compartición justa entre tenants y usuarios de grupo de recurso

  El programador Superior permite configurar recursos compartidos para los usuarios en una cola. Cada tenant puede tener usuarios con diferentes ponderaciones. Los usuarios muy ponderados pueden requerir más recursos compartidos.

- Rendimiento de programación garantizado en un gran clúster

  El programador Superior recibe los latidos de cada NodeManager y guarda la información de recursos en la memoria, lo que permite al programador controlar el uso de recursos del clúster globalmente. El programador Superior utiliza el modelo de programación push, lo que hace que la programación sea más precisa y eficiente y mejora notablemente la utilización de los recursos del clúster. Además, el programador Superior ofrece un excelente rendimiento cuando el intervalo entre los latidos NodeManager es largo y evita las tormentas de latidos en grupos grandes.

- Política de prioridad

  Si no se puede cumplir el requisito mínimo de recursos de un servicio después de que el servicio obtenga todos los recursos disponibles, se produce una preferencia. La función de preferencia está deshabilitada por defecto.

7.6.1.2.5 Recursos de almacenamiento

Descripción

Como servicio de almacenamiento de archivos distribuido en un clúster de big data, HDFS almacena todos los datos de usuario de las aplicaciones de capa superior en el clúster de big data, incluidos los datos escritos en tablas HBase o tablas Hive.

Un directorio es la unidad básica de asignación de recursos de almacenamiento HDFS. HDFS soporta la estructura de archivos jerárquica convencional. Los usuarios o las aplicaciones pueden crear directorios y crear, eliminar, mover o cambiar el nombre de archivos en directorios. Tenants pueden obtener recursos de almacenamiento de información de directorios especificados en el sistema de archivos HDFS.

Mecanismo de programación

Los directorios HDFS se pueden almacenar en nodos con etiquetas especificadas o discos de tipos de hardware especificados. Por ejemplo:

- Cuando las tareas de consulta en tiempo real y de análisis de datos se ejecutan en el mismo clúster, las tareas de consulta en tiempo real solo deben desplegar en ciertos nodos, y los datos de la tarea también deben almacenarse en estos nodos.
- De acuerdo con los requisitos de servicio reales, los datos clave deben almacenarse en nodos altamente confiables.

Los administradores pueden configurar de forma flexible las políticas de almacenamiento de datos HDFS según los requisitos de servicio reales y las características de datos para almacenar datos en nodos específicos.

Para tenants, los recursos de almacenamiento se refieren a los recursos HDFS que usan. Los datos de directorios especificados se pueden almacenar en las rutas de almacenamiento especificadas por el tenant, implementando así la programación de recursos de almacenamiento y asegurando el aislamiento de datos entre los tenants.

Los usuarios pueden agregar o eliminar directorios de almacenamiento HDFS de tenants y establecer la cuota de cantidad de archivos y la cuota de capacidad de almacenamiento de los directorios para gestionar los recursos de almacenamiento.

7.6.1.3 Uso de Multi-Tenancy

7.6.1.3.1 Descripción

Los tenants se utilizan en escenarios de control de recursos y aislamiento de servicios. Los administradores deben determinar los escenarios de servicio de los recursos del clúster y, a continuación, planificar los tenants.

NOTA

- Yarn en un nuevo clúster utiliza el programador Superior de forma predeterminada. Para obtener más información, consulte **Uso del Superior Scheduler**.

Multitenant implica tres tipos de operaciones: crear un tenant, gestión de tenants, y gestión de recursos. **Tabla 7-32** describe estas operaciones.

Tabla 7-32 Operaciones multitenant

Operación	Acción	Descripción
Creación de un tenant	● Agregar un tenant. ● Agregar un subtenant. ● Crear un usuario y vincular el usuario al rol de un tenant.	Durante la creación de un tenant, puede configurar sus recursos informáticos, recursos de almacenamiento y servicios asociados en función de los requisitos de servicio. Además, puede agregar usuarios al tenant y vincular los roles necesarios a estos usuarios. Un usuario para crear un tenant de nivel 1 debe estar vinculado al rol **Manager_administrator** o **System_administrator**. Un usuario para crear un subtenant debe estar vinculado al rol del tenant principal al menos.
Gestión de tenants	● Gestionar el directorio del tenant. ● Restaure los datos del tenant. ● Borra las colas no asociadas de un tenant. ● Eliminar un tenant.	Puede editar tenants a medida que cambian los servicios. Un usuario para gestionar o eliminar un tenant de nivel 1 o restaurar datos de tenant debe estar enlazado al rol **Manager_administrator** o **System_administrator**. Un usuario para gestionar o eliminar un subtenant debe estar vinculado al rol del tenant principal al menos.
Gestión de recursos	● Crear un grupo de recurso. ● Modificar un grupo de recursos. ● Eliminar un grupo de recursos. ● Configurar una cola. ● Configurar la política de capacidad de cola de un grupo de recursos. ● Borrar configuraciones de una cola.	Puede volver a configurar los recursos para los tenants a medida que cambien los servicios. Un usuario para gestionar recursos debe estar enlazado al rol **Manager_administrator** o **System_administrator**.

7.6.1.3.2 Descripción del proceso

Los administradores deben determinar los escenarios de servicio de los recursos del clúster y, a continuación, planificar los tenants. Después de eso, los administradores agregan tenants y configuran recursos dinámicos, recursos de almacenamiento y servicios asociados para los tenants en FusionInsight Manager.

Descripción del proceso muestra el proceso para crear un tenant.

Figura 7-41 Creación de un tenant

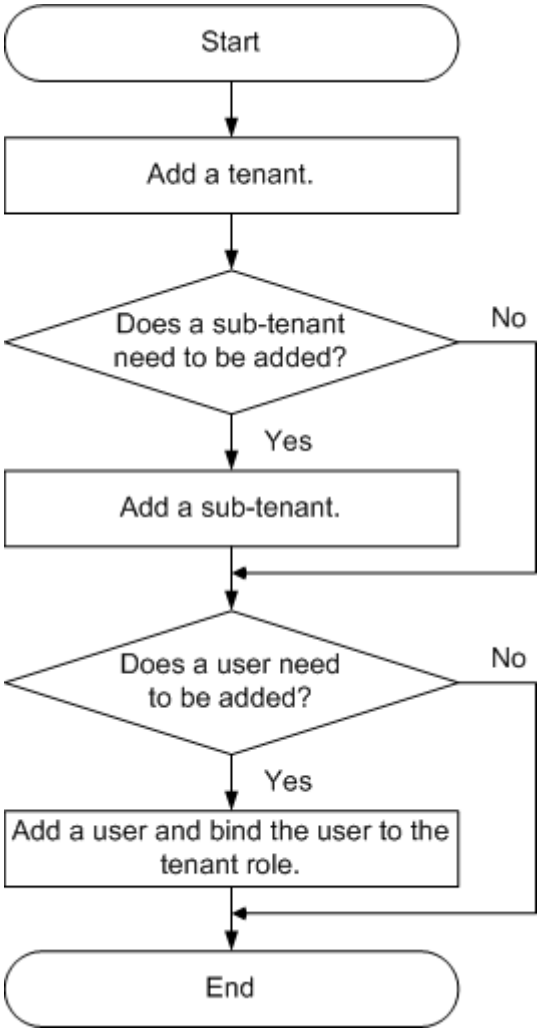


Tabla 7-33 describe las operaciones para crear un tenant.

Tabla 7-33 Operaciones para crear un tenant

Operación	Descripción
Agregar un tenant.	Puede configurar los recursos informáticos, los recursos de almacenamiento y los servicios asociados del tenant.
Agregar un subtenant.	Puede configurar los recursos informáticos, los recursos de almacenamiento y los servicios asociados del subtenant.
Agregar un usuario y vincular el usuario al rol de tenant.	Si un usuario desea utilizar los recursos de tenant **tenant1** o agregar o eliminar subtenants para **tenant1**, el usuario debe estar enlazado a los roles **Manager_tenant** y **tenant1**_*Cluster ID*.

7.6.2 Uso del Superior Scheduler

7.6.2.1 Creación de tenants

7.6.2.1.1 Adición de un tenant

Escenario

Puede crear tenants en FusionInsight Manager en función del consumo de recursos y la planificación de aislamiento y los requisitos de los servicios.

Prerrequisitos

- Se ha planificado un nombre de tenant en función de los requisitos de servicio. El nombre no puede ser el mismo que el de un rol, directorio HDFS o cola de Yarn que existe en el clúster actual.
- Los recursos que se asignarán al tenant actual se han previsto para garantizar que la suma de los recursos de subtenants en cada nivel no exceda de los recursos del tenant actual.

Procedimiento

Paso 1 Inicie sesión en el FusionInsight Manager y elija **Tenant Resources**.

Paso 2 Haga clic en . En la página que se muestra, configure los atributos de tenant de acuerdo con **Tabla 7-34**.

Tabla 7-34 Parámetros del tenant

Parámetro	Descripción
Cluster	Indica el clúster para el que desea crear un tenant.
Name	• Indica el nombre del tenant actual. El valor consta de 3 a 50 caracteres, incluidos dígitos, letras y guiones bajos (_). • Planifique un nombre de tenant en función de los requisitos de servicio. El nombre no puede ser el mismo que el de un rol, directorio HDFS o cola de Yarn que existe en el clúster actual.
Tenant Resource Type	Especifica si el tenant es un tenant de hoja. • Cuando se selecciona **Leaf Tenant Resource**, el tenant actual es un tenant de hoja y no se puede agregar ningún subtenant. • Cuando se selecciona **Non-leaf Tenant Resource**, el tenant actual no es un tenant de hoja y se pueden agregar subtenants al tenant actual.

Parámetro	Descripción
Computing Resource	Especifica los recursos de cálculo dinámicos para el tenant actual. ● Cuando se selecciona **Yarn**, el sistema crea automáticamente una cola en Yarn y la cola recibe el mismo nombre que el nombre del tenant. – Un tenant de hoja puede enviar trabajos directamente a la cola. – Un tenant que no sea de hoja no puede enviar trabajos directamente a la cola. Sin embargo, Yarn agrega una cola adicional (oculta) llamada **default** para que el tenant no hoja registre la capacidad de recursos restante del tenant. Los trabajos reales no se ejecutan en esta cola. ● Si **Yarn** no está seleccionado, el sistema no crea automáticamente una cola.
Configuration Mode	Indica el modo de configuración de los parámetros de recursos informáticos. ● Si selecciona **Basic**, solo tendrá que configurar **Default Resource Pool Capacity (%)**. ● Si selecciona **Advanced**, puede configurar manualmente la ponderación de asignación de recursos y los recursos mínimos, máximos y reservados del tenant.
Default Resource Pool Capacity (%)	Indica el porcentaje de recursos informáticos utilizados por el tenant actual en el grupo de recursos predeterminado. El valor oscila entre **0** y **100%**.
Weight	Indica la ponderación de asignación de recursos. El valor varía de **0** a **100**.
Minimum Resource	Indica los recursos garantizados para el tenant (se admite la preferencia). El valor puede ser un porcentaje o un valor absoluto de los recursos del tenant principal. Cuando un tenant tiene una carga de trabajo ligera, los recursos del tenant se asignan automáticamente a otros tenants. Cuando los recursos disponibles del tenant son menores que el valor de **Minimum Resource**, el tenant puede adelantarse a los recursos que se han prestado a otros tenants.
Maximum Resource	Indica el máximo de recursos que puede utilizar el tenant. El tenant no puede obtener más recursos que el valor configurado. El valor puede ser un porcentaje o un valor absoluto de los recursos del tenant principal.
Reserved Resource	Indica los recursos reservados para el tenant. Los recursos reservados no pueden ser utilizados por otros tenants aunque no se esté ejecutando ningún trabajo en los recursos actuales del tenant. El valor puede ser un porcentaje o un valor absoluto de los recursos del tenant principal.

Parámetro	Descripción
Storage Resource	Especifica los recursos de almacenamiento para el tenant actual. ● Cuando se selecciona **HDFS**, el sistema asigna automáticamente los recursos de almacenamiento. ● Cuando **HDFS** no está seleccionado, el sistema no asigna automáticamente los recursos de almacenamiento.
Quota	Indica la cuota de archivos y directorios.
Space Quota	Indica la cuota para el espacio de almacenamiento HDFS utilizado por el tenant actual. ● Si la unidad está establecida en **MB**, el valor varía entre **1** y **8796093022208**. Si la unidad está establecida en **GB**, el valor varía entre **1** y **8589934592**. ● Este parámetro indica el espacio de almacenamiento HDFS máximo que puede utilizar el tenant, pero no el espacio real utilizado. ● Si su valor es mayor que el tamaño del disco físico HDFS, el espacio máximo disponible es el espacio completo del disco físico HDFS.
Storage Path	Indica un directorio HDFS para los datos de recursos del tenant. ● El sistema crea automáticamente una carpeta con el nombre del tenant en el directorio **/tenant** de forma predeterminada. Por ejemplo, el directorio de almacenamiento HDFS predeterminado para el **ta1** del tenant es **/tenant/ta1**. ● Cuando se crea un tenant por primera vez, el sistema crea el directorio **/tenant** en el directorio raíz HDFS. La ruta de almacenamiento es personalizable.
Service	Especifica si se asocian recursos de otros servicios. Para obtener más información, consulte **Paso 4**.
Description	Indica la descripción del tenant actual.

NOTA

Los roles, los recursos informáticos y los recursos de almacenamiento se crean automáticamente cuando se crean los tenants.

- El nuevo rol tiene permisos sobre los recursos informáticos y de almacenamiento. Este rol y sus permisos son controlados automáticamente por el sistema y no se pueden gestionar manualmente eligiendo **System** > **Permission** > **Role**. El nombre del rol tiene el formato de *Tenant name_Cluster ID*. El ID del primer clúster no se muestra de forma predeterminada.
- Cuando utilice este tenant, cree un usuario del sistema y vincule al usuario al rol del tenant. Para obtener más información, consulte **Adición de un usuario y vinculación del usuario a un rol de tenant**.
- Durante la creación del tenant, el sistema crea automáticamente una cola de Yarn con el nombre del tenant. Si el nombre de la cola ya existe, la nueva cola se denomina **Tenant name-***N*. *N* indica un número natural a partir de **1**. Cuando existe un mismo nombre, el valor *N* aumenta automáticamente para diferenciar la cola de los demás. Por ejemplo, **saletenant**, **saletenant-1** y **saletenant-2**.

Paso 3 Compruebe si el tenant actual necesita estar asociado con recursos de otros servicios.

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 5**.

Paso 4 Haga clic en **Associate Service** para configurar otros recursos de servicio utilizados por el tenant actual y haga clic en **OK**.

- Establezca **Service** en **HBase** y **Association Type** en **Exclusive** o **Shared**.

  NOTA

  - **Exclusive** indica que los recursos de servicio son utilizados exclusivamente por el tenant y no pueden asociarse con otros tenants.
  - **Shared** indica que los recursos de servicio se pueden compartir con otros tenants.

NOTA

- Solo HBase puede asociarse con un nuevo tenant. Sin embargo, HDFS, HBase y Yarn pueden asociarse con tenants existentes.
- Para asociar un tenant existente a los recursos de servicio, haga clic en el tenant de destino en la lista de tenant, cambie a la página **Service Associations** y haga clic en **Associate Service** para configurar los recursos que se asociarán al tenant.
- Para desasociar un tenant existente de los recursos de servicio, haga clic en el tenant de destino en la lista de tenant, cambie a la página **Service Associations** y haga clic en **Delete** en la columna **Operation**. En el cuadro de diálogo que se muestra, seleccione **I have read the information and understand the impact** y haga clic en **OK**.

Paso 5 Haga clic en **OK**. Espere hasta que el sistema muestre un mensaje que indique que el tenant se ha creado correctamente.

----Fin

7.6.2.1.2 Adición de un subtenant

Escenario

Puede crear subtenants en FusionInsight Manager y asignar recursos del tenant actual a los subtenants en función del consumo de recursos y la planificación de aislamiento y los requisitos de los servicios.

Prerrequisitos

- Se ha agregado un tenant principal que no es de hoja.
- Se ha planificado un nombre de subtenant basado en los requisitos de servicio. El nombre no puede ser el mismo que el de un rol, directorio HDFS o cola de Yarn que existe en el clúster actual.
- Los recursos que se asignarán al tenant actual se han previsto para garantizar que la suma de los recursos de subtenants en cada nivel no exceda de los recursos del tenant actual.

Procedimiento

Paso 1 Inicie sesión en el FusionInsight Manager y elija **Tenant Resources**.

Paso 2 En la lista de tenants de la izquierda, seleccione un tenant padre y haga clic en . En la página para agregar un subtenant, establezca atributos para el subtenant según **Tabla 7-35**.

Tabla 7-35 Parámetros de subtenant

Parámetro	Descripción
Cluster	Indica el clúster al que pertenece el tenant principal.
Parent Tenant Resource	Indica el nombre del inquilino principal.
Name	● Indica el nombre del tenant actual. El valor consta de 3 a 50 caracteres, incluidos dígitos, letras y guiones bajos (_). ● Planifique un nombre de subtenant basado en los requisitos de servicio. El nombre no puede ser el mismo que el de un rol, directorio HDFS o cola de Yarn que existe en el clúster actual.
Tenant Resource Type	Especifica si el tenant es un tenant de hoja. ● Cuando se selecciona **Leaf Tenant Resource**, el tenant actual es un tenant de hoja y no se puede agregar ningún subtenant. ● Cuando se selecciona **Non-leaf Tenant Resource**, el tenant actual no es un tenant de hoja y se pueden agregar subtenants al tenant actual. Sin embargo, la profundidad del tenant no puede exceder de 5 niveles.

Parámetro	Descripción
Computing Resource	Especifica los recursos de cálculo dinámicos para el tenant actual. ● Cuando se selecciona **Yarn**, el sistema crea automáticamente una cola en Yarn y la cola recibe el mismo nombre que el nombre del subtenant. – Un tenant de hoja puede enviar trabajos directamente a la cola. – Un tenant que no sea de hoja no puede enviar trabajos directamente a la cola. Sin embargo, Yarn agrega una cola adicional (oculta) llamada **default** para que el tenant no hoja registre la capacidad de recursos restante del tenant. Los trabajos reales no se ejecutan en esta cola. ● Si **Yarn** no está seleccionado, el sistema no crea automáticamente una cola.
Configuration Mode	Indica el modo de configuración de los parámetros de recursos informáticos. ● Si selecciona **Basic**, solo tendrá que configurar **Default Resource Pool Capacity (%)**. ● Si selecciona **Advanced**, puede configurar manualmente la ponderación de asignación de recursos y los recursos mínimos, máximos y reservados del tenant.
Default Resource Pool Capacity (%)	Indica el porcentaje de recursos informáticos utilizados por el tenant actual. El valor base es el total de recursos del tenant principal.
Weight	Indica la ponderación de asignación de recursos. El valor varía de **0** a **100**.
Minimum Resource	Indica los recursos garantizados para el tenant (se admite la preferencia). El valor puede ser un porcentaje o un valor absoluto de los recursos del tenant principal. Cuando un tenant tiene una carga de trabajo ligera, los recursos del tenant se asignan automáticamente a otros tenants. Cuando los recursos disponibles del tenant son menores que el valor de **Minimum Resource**, el tenant puede adelantarse a los recursos que se han prestado a otros tenants.
Maximum Resource	Indica el máximo de recursos que puede utilizar el tenant. El tenant no puede obtener más recursos que el valor configurado. El valor puede ser un porcentaje o un valor absoluto de los recursos del tenant principal.
Reserved Resource	Indica los recursos reservados para el tenant. Los recursos reservados no pueden ser utilizados por otros tenants aunque no se esté ejecutando ningún trabajo en los recursos actuales del tenant. El valor puede ser un porcentaje o un valor absoluto de los recursos del tenant principal.

Parámetro	Descripción
Storage Resource	Especifica los recursos de almacenamiento para el tenant actual. ● Cuando se selecciona **HDFS**, el sistema crea automáticamente una carpeta con el nombre del subtenant en el directorio de tenant principal de HDFS. ● Cuando **HDFS** no está seleccionado, el sistema no asigna automáticamente los recursos de almacenamiento.
Quota	Indica la cuota de archivos y directorios.
Space Quota	Indica la cuota para el espacio de almacenamiento HDFS utilizado por el tenant actual. ● Si la unidad está establecida en **MB**, el valor varía entre **1** y **8796093022208**. Si la unidad está establecida en **GB**, el valor varía entre **1** y **8589934592**. ● Este parámetro indica el espacio de almacenamiento HDFS máximo que puede utilizar el tenant, pero no el espacio real utilizado. ● Si su valor es mayor que el tamaño del disco físico HDFS, el espacio máximo disponible es el espacio completo del disco físico HDFS. ● Si esta cuota es mayor que la cuota del tenant principal, el espacio de almacenamiento real no excede la cuota del tenant principal.
Storage Path	Indica el directorio de almacenamiento de HDFS para el tenant. ● El sistema crea automáticamente una carpeta con el nombre del subtenant en el directorio del tenant principal de forma predeterminada. Por ejemplo, si el subtenant es **ta1s** y el directorio principal es **/tenant/ta1**, la ruta de almacenamiento para el subtenant es entonces **/tenant/ta1/ta1s**. ● La ruta de almacenamiento se puede personalizar en el directorio principal.
Service	Especifica si se asocian recursos de otros servicios. Para obtener más información, consulte **Paso 4**.
Description	Indica la descripción del tenant actual.

NOTA

Los roles, los recursos informáticos y los recursos de almacenamiento se crean automáticamente cuando se crean los tenants.

- El nuevo rol tiene permisos sobre los recursos informáticos y de almacenamiento. Este rol y sus permisos son controlados automáticamente por el sistema y no se pueden gestionar manualmente eligiendo **System** > **Permission** > **Role**. El nombre del rol tiene el formato de *Tenant name_Cluster ID*. El ID del primer clúster no se muestra de forma predeterminada.
- Cuando utilice este tenant, cree un usuario del sistema y vincule al usuario al rol del tenant. Para obtener más información, consulte **Adición de un usuario y vinculación del usuario a un rol de tenant**.
- El subtenant puede asignar además los recursos de su tenant principal. La suma de los porcentajes de recursos de subtenants directos bajo un tenant principal en cada nivel no puede exceder 100%. La suma de los porcentajes de recursos de computación de todos los tenants de nivel 1 no puede exceder el 100%.

Paso 3 Compruebe si el tenant actual necesita estar asociado con recursos de otros servicios.

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 5**.

Paso 4 Haga clic en **Associate Service** para configurar otros recursos de servicio utilizados por el tenant actual.

1. Establezca **Services** a **HBase**.
2. Establezca **Association Type** de la siguiente manera:
   - **Exclusive** indica que los recursos de servicio son utilizados exclusivamente por el tenant y no pueden asociarse con otros tenants.
   - **Shared** indica que los recursos de servicio se pueden compartir con otros tenants.

NOTA

- Solo HBase puede asociarse con un nuevo tenant. Sin embargo, HDFS, HBase y Yarn pueden asociarse con tenants existentes.
- Para asociar un tenant existente a los recursos de servicio, haga clic en el tenant de destino en la lista de tenant, cambie a la página **Service Associations** y haga clic en **Associate Service** para configurar los recursos que se asociarán al tenant.
- Para desasociar un tenant existente de los recursos de servicio, haga clic en el tenant de destino en la lista de tenant, cambie a la página **Service Associations** y haga clic en **Delete** en la columna **Operation**. En el cuadro de diálogo que se muestra, seleccione **I have read the information and understand the impact** y haga clic en **OK**.

3. Haga clic en **OK**.

Paso 5 Haga clic en **OK**. Espere hasta que el sistema muestre un mensaje que indique que el tenant se ha creado correctamente.

----Fin

7.6.2.1.3 Adición de un usuario y vinculación del usuario a un rol de tenant

Escenario

Un tenant recién creado no puede iniciar sesión directamente en el clúster para acceder a los recursos. Debe agregar un usuario para el tenant en FusionInsight Manager y vincularlo al rol del tenant para asignar permisos de operación al usuario.

Prerrequisitos

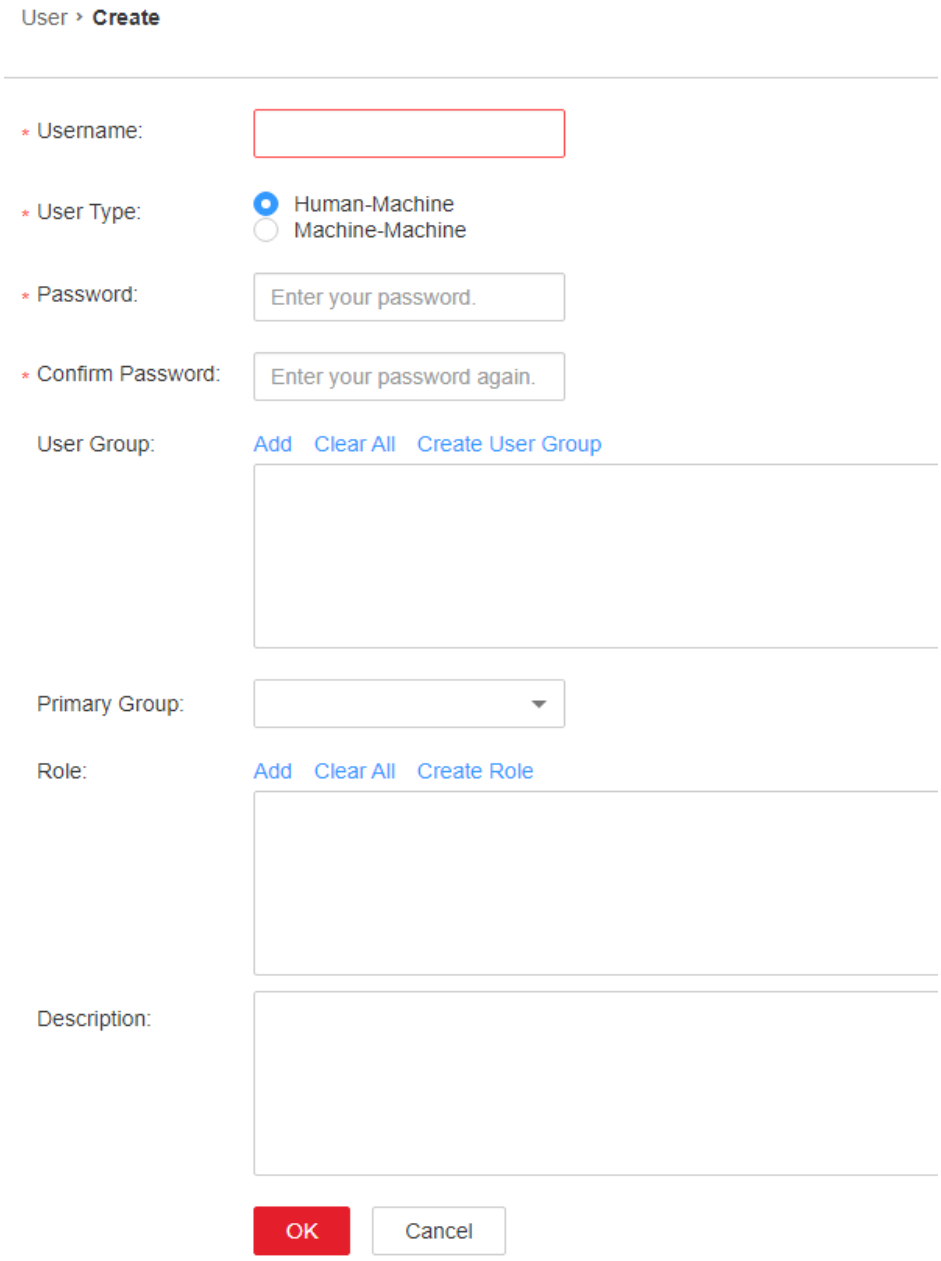
Ha aclarado los requisitos de servicio y ha creado un tenant.

Procedimiento

Paso 1 Inicie sesión en FusionInsight Manager y elija **System** > **Permission** > **User**.

Paso 2 Si desea agregar un usuario al sistema, haga clic en **Create**.

Figura 7-42 Adición de un usuario



Si desea enlazar roles de inquilino a un usuario existente en el sistema, busque la fila del usuario y haga clic en **Modify** en la columna **Operation**.

Establezca los atributos de usuario según **Tabla 7-36**.

Tabla 7-36 Parámetros del usuario

Parámetro	Descripción
Username	Indica el nombre de usuario actual. El valor contiene de 3 a 32 caracteres, incluidos dígitos, letras, guiones bajos (_), guiones (-) y espacios. ● El nombre de usuario no puede ser el mismo que el nombre de usuario del sistema operativo de cualquier nodo del clúster. De lo contrario, no se puede utilizar el usuario. ● No se permite un nombre de usuario que difiera solo en mayúsculas y minúsculas de un nombre de usuario existente. Por ejemplo, si **User1** se ha creado, no puede crear **user1**. Ingrese el nombre de usuario correcto cuando utilice **User1**.
User Type	Las opciones son **Human-Machine** y **Machine-Machine**. ● Usuario de **Human-Machine**: utilizado para FusionInsight Manager O&M y las operaciones del cliente de componentes. Si selecciona esta opción, establezca **Password** y **Confirm Password** en consecuencia. ● Usuario de **Machine-Machine**: utilizado para el desarrollo de aplicaciones. Si selecciona esta opción, la contraseña se genera aleatoriamente.
Password	Este parámetro es obligatorio si **User Type** tiene el valor de **Human-Machine**. La contraseña debe contener de 8 a 64 caracteres de al menos cuatro tipos de los siguientes: letras mayúsculas, minúsculas, dígitos, caracteres especiales y espacios. La contraseña no puede ser el nombre de usuario o el nombre de usuario escrito al revés.
Confirm Password	Vuelva a ingresar la contraseña.
User Group	En el área **User Group**, haga clic en **Add** y seleccione grupos de usuarios para agregar el usuario a los grupos. ● Si se han agregado roles a los grupos de usuarios, se pueden conceder al usuario los permisos de los roles. ● Por ejemplo, agregue el usuario al grupo de usuarios de Hive para asignar permisos de Hive al usuario.
Primary Group	Seleccione un grupo como grupo principal para que el usuario cree directorios y archivos. La lista desplegable contiene todos los grupos seleccionados en **User Group**.

Parámetro	Descripción
Role	Haga clic en **Add** para vincular un rol de tenant al usuario. **NOTA** ● Si un usuario desea utilizar los recursos del tenant **tenant1** y agregar o eliminar subtenants para **tenant1**, debe estar enlazado a los roles **Manager_tenant** y **tenant1**_*Cluster ID*. ● Si el tenant se ha asociado con el servicio HBase y la autenticación de Ranger está habilitada para el clúster, debe configurar los permisos de ejecución de HBase en la página Ranger.
Description	Indica la descripción del usuario actual.

Paso 3 Haga clic en **OK**.

----Fin

7.6.2.2 Gestión de tenants

7.6.2.2.1 Gestión de directorios de tenant

Escenario

Puede gestionar los directorios de almacenamiento de HDFS que utilizan los tenants especificados en función de los requisitos de servicio del FusionInsight Manager, como agregar directorios de tenant, cambiar las cuotas para directorios y archivos y para espacio de almacenamiento, y eliminar directorios.

Prerrequisitos

Se ha agregado un tenant con recursos de almacenamiento de HDFS.

Ver un directorio de tenant

Paso 1 Inicie sesión en el FusionInsight Manager y elija **Tenant Resources**.

Paso 2 En la lista de tenant de la izquierda, haga clic en el tenant de destino.

Paso 3 Haga clic en la pestaña **Resource**.

Paso 4 Vea la tabla **HDFS Storage**.

- La columna **File Number Threshold** proporciona la cuota para los archivos y directorios del directorio del tenant.
- La columna **Space Quota** proporciona el tamaño del espacio de almacenamiento del directorio del tenant.

----Fin

Adición de un directorio de tenant

Paso 1 En FusionInsight Manager, seleccione **Tenant Resources**.

Paso 2 En la lista de tenant de la izquierda, haga clic en el tenant de destino.

Paso 3 Haga clic en la pestaña **Resource**.

Paso 4 En el área **HDFS Storage**, haga clic en **Create Directory**.

- **Parent Directory**: indica el directorio de almacenamiento utilizado por el tenant principal del inquilino actual.

  NOTA

  Este parámetro no se muestra si el tenant actual no es un subtenant.

- Establezca **Path** en una ruta de directorio del tenant.

  NOTA

  Si el tenant actual no es un subtenant, la nueva ruta se crea en el directorio raíz de HDFS.

- Establezca **Quota** en la cuota de archivos y directorios.
- **File Number Threshold (%)** sólo es válido cuando **Quota** está establecido. Si la relación entre el número de archivos usados y el valor de **Quota** excede el valor de este parámetro, se genera una alarma. Si no se especifica este parámetro, no se notifica ninguna alarma en este escenario.

  NOTA

  El número de archivos usados se recopila cada hora. Por lo tanto, la alarma que indica que la relación de archivos usados excede el umbral se retrasa.

- Establezca **Space Quota** en el tamaño del espacio de almacenamiento del directorio del tenant.
- Si la relación entre el espacio de almacenamiento usado y el valor de **Space Quota** excede el valor **Storage Space Threshold (%)**, se genera una alarma. Si no se especifica este parámetro, no se notifica ninguna alarma en este escenario.

  NOTA

  El espacio de almacenamiento utilizado se recoge cada hora. Por lo tanto, la alarma que indica que la relación de espacio de almacenamiento usado excede el umbral se retrasa.

Paso 5 Haga clic en **OK**.

----Fin

Modificación de un directorio de tenant

Paso 1 En FusionInsight Manager, seleccione **Tenant Resources**.

Paso 2 En la lista de tenant de la izquierda, haga clic en el tenant de destino.

Paso 3 Haga clic en la pestaña **Resource**.

Paso 4 En la tabla **HDFS Storage**, haga clic en **Modify** en la columna **Operation** del directorio de tenant especificado.

- Establezca **Quota** en la cuota de archivos y directorios.
- **File Number Threshold (%)** sólo es válido cuando **Quota** está establecido. Si la relación entre el número de archivos usados y el valor de **Quota** excede el valor de este parámetro, se genera una alarma. Si no se especifica este parámetro, no se notifica ninguna alarma en este escenario.

- Establezca **Space Quota** en el tamaño del espacio de almacenamiento del directorio del tenant.
- Si la relación entre el espacio de almacenamiento usado y el valor de **Space Quota** excede el valor **Storage Space Threshold (%)**, se genera una alarma. Si no se especifica este parámetro, no se notifica ninguna alarma en este escenario.

Paso 5 Haga clic en **OK**.

----Fin

Eliminación de un directorio de tenant

Paso 1 En FusionInsight Manager, seleccione **Tenant Resources**.

Paso 2 En la lista de tenant de la izquierda, haga clic en el tenant de destino.

Paso 3 Haga clic en la pestaña **Resource**.

Paso 4 En la tabla **HDFS Storage**, haga clic en **Delete** en la columna **Operation** del directorio de tenant especificado.

NOTA

No se puede eliminar el directorio del tenant creado por el sistema durante la creación del tenant.

Paso 5 Haga clic en **OK**.

----Fin

7.6.2.2.2 Restauración de datos de tenant

Escenario

Los datos del tenant se almacenan en el FusionInsight Manager y en los componentes del clúster. Cuando los componentes se recuperan de fallas o se reinstalan, algunos datos de configuración de todos los tenants pueden volverse anormales. En este caso, debe restaurar manualmente los datos de configuración en el FusionInsight Manager.

Procedimiento

Paso 1 Inicie sesión en el FusionInsight Manager y elija **Tenant Resources**.

Paso 2 En la lista de tenant de la izquierda, haga clic en el tenant de destino.

Paso 3 Compruebe el estado de los datos del tenant.

1. En la página **Summary**, verifique **Tenant Status**. Un icono verde indica que el tenant está disponible y gris indica que el tenant no está disponible.
2. Haga clic en **Resource** y compruebe los iconos a la izquierda de **Yarn** y **HDFS Storage**. Un icono verde indica que el recurso está disponible y el gris indica que el recurso no está disponible.
3. Haga clic en **Service Associations** y compruebe la columna **Status** de los servicios asociados. **Normal** indica que el componente puede proporcionar servicios para el tenant asociado. **Not Available** indica que el componente no puede proporcionar servicios al tenant.

4. Si alguno de los elementos de comprobación anteriores es anormal, vaya a **Paso 4** para restaurar los datos del tenant.

Paso 4 Haga clic en . En el cuadro de diálogo que se muestra, introduzca la contraseña del usuario de inicio de sesión actual y haga clic en **OK**.

Paso 5 En la ventana **Restore Tenant Resource Data**, seleccione uno o más componentes para restaurar los datos y haga clic en **OK**. El sistema restaura automáticamente los datos del tenant.

----Fin

7.6.2.2.3 Eliminación de un tenant

Escenario

Puede eliminar tenants que ya no se utilizan en FusionInsight Manager según los requisitos de servicio para liberar recursos ocupados por los tenants.

Prerrequisitos

- Se ha agregado un tenant.
- El tenant no tiene sub-tenants. Si el tenant tiene sub-tenants, elimínelos; de lo contrario, no se puede eliminar el tenant.
- El rol del tenant no está asociado con ningún usuario o grupo de usuarios.

Procedimiento

Paso 1 Inicie sesión en el FusionInsight Manager y elija **Tenant Resources**.

Paso 2 En la lista de tenant de la izquierda, haga clic en el tenant de destino y haga clic en .

NOTA

- Si desea conservar los datos del tenant, seleccione **Reserve the data of this tenant resource**. De lo contrario, se eliminará el espacio de almacenamiento del tenant.

Paso 3 Haga clic en **OK**.

Se tarda unos minutos en guardar la configuración. Después de eliminar el tenant, el rol y el espacio de almacenamiento del tenant también se eliminan.

NOTA

Después de eliminar el tenant, la cola del tenant todavía existe en Yarn. La cola del tenant no se muestra en la página de gestión de roles en Yarn.

----Fin

7.6.2.3 Gestión de recursos

7.6.2.3.1 Adición de un grupo de recursos

Escenario

En un clúster, puede agrupar lógicamente NodeManagers de Yarn en grupos de recursos de Yarn. Cada NodeManager pertenece a un solo grupo de recursos. Puede crear un grupo de recursos personalizado en FusionInsight Manager y agregar los hosts que no se han agregado a ningún grupo de recursos personalizado a este grupo de recursos para que las colas especificadas puedan usar los recursos informáticos proporcionados por estos hosts.

El sistema contiene un grupo de recursos **default** de forma predeterminada. Todas las NodeManagers que no se agregan a grupos de recursos personalizados pertenecen a este grupo de recursos.

Procedimiento

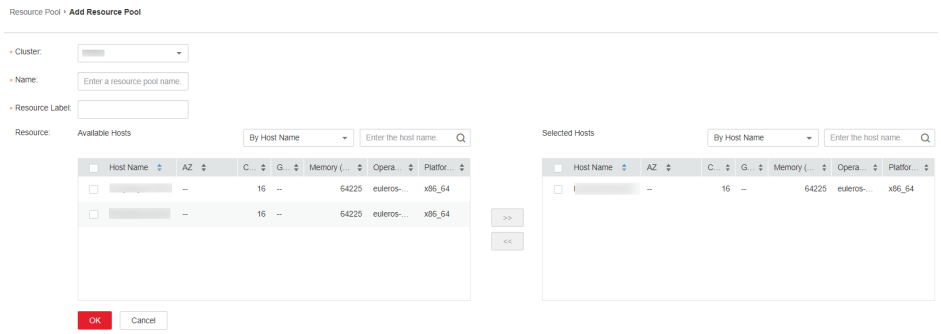
Paso 1 Inicie sesión en FusionInsight Manager.

Paso 2 Elija **Tenant Resources** > **Resource Pool**.

Paso 3 Haga clic en **Add Resource Pool**.

Paso 4 Establezca los atributos del grupo de recursos.

Figura 7-43 Adición de recursos



- **Cluster**: Seleccione el clúster al que se va a agregar el grupo de recursos.
- **Name**: Introduzca el nombre del grupo de recursos. El nombre contiene de 1 a 50 caracteres, incluidos dígitos, letras y guiones bajos (_), y no puede comenzar con un guion bajo (_).
- **Resource Label**: Introduzca la etiqueta de recursos del grupo de recursos. El valor puede contener de 1 a 50 caracteres, incluidos dígitos, letras, guiones bajos (_), y guiones (-), y debe comenzar con un dígito o letra.
- **Resource**: En el área **Available Hosts**, seleccione los hosts especificados y haga clic en >> para agregar los hosts al área **Selected Hosts**. Solo se pueden seleccionar los hosts del clúster. La lista de hosts del grupo de recursos se puede dejar en blanco.

  NOTA

  Puede filtrar hosts por nombre de host, número de núcleos de CPU, memoria, sistema de operación o tipo de plataforma según los requisitos del servicio.

Paso 5 Haga clic en **OK**.

Después de crear el grupo de recursos, puede ver su nombre, miembros y modo en la lista del grupo de recursos. Los hosts que se agregan al grupo de recursos personalizado ya no son miembros del grupo de recursos **default**.

----Fin

7.6.2.3.2 Modificación de un grupo de recursos

Escenario

Cuando es necesario ajustar los hosts de un grupo de recursos en función de los requisitos de servicio, puede modificar los miembros del grupo de recursos en FusionInsight Manager.

Procedimiento

Paso 1 Inicie sesión en FusionInsight Manager.

Paso 2 Elija **Tenant Resources** > **Resource Pool**.

Paso 3 Busque la fila que contiene el grupo de recursos especificado y haga clic en **Edit** en la columna **Operation**.

Paso 4 En el área **Resource**, modifique hosts.

- Agregar hosts: Seleccione los hosts deseados en **Available Hosts** y haga clic en >> para agregarlos al grupo de recursos.
- Eliminar hosts: Seleccione los hosts deseados de **Selected Hosts** y haga clic en << para quitarlos del grupo de recursos. La lista de hosts del grupo de recursos se puede dejar en blanco.

Paso 5 Haga clic en **OK**.

----Fin

7.6.2.3.3 Eliminación de un grupo de recursos

Escenario

Si ya no se utiliza un grupo de recursos en función de los requisitos de servicio, puede eliminarlo en FusionInsight Manager.

Prerrequisitos

- Cualquier cola del clúster no utiliza el grupo de recursos que se eliminará como el grupo de recursos predeterminado. Antes de eliminar el fondo de recursos, cancele el grupo de recursos predeterminado. Para obtener más información, consulte **Configuración de una cola**.
- Las políticas de distribución de recursos de todas las colas se han borrado del grupo de recursos que se van a eliminar. Para obtener más información, consulte **Borrar configuraciones de cola**.

Procedimiento

Paso 1 Inicie sesión en FusionInsight Manager.

Paso 2 Elija **Tenant Resources** > **Resource Pool**.

Paso 3 Busque la fila que contiene el grupo de recursos especificado y haga clic en **Delete** en la columna **Operation**.

Paso 4 En el cuadro de diálogo que se muestra, haga clic en **OK**.

----Fin

7.6.2.3.4 Configuración de una cola

Escenario

Puede modificar las configuraciones de cola de un tenant especificado en FusionInsight Manager.

Prerrequisitos

Se ha agregado un tenant que utiliza el Superior scheduler.

Procedimiento

Paso 1 En FusionInsight Manager, seleccione **Tenant Resources**.

Paso 2 Elija **Dynamic Resource Plan**.

Paso 3 Haga clic en la pestaña **Queue Configurations**.

Paso 4 Establezca **Cluster** en el nombre del clúster de destino. En el área **All tenants resources**, busque la fila que contiene el recurso de tenant de destino y haga clic en **Modify** en la columna **Operation**.

NOTA

- También puede acceder a la página **Modify Queue Configuration** de la siguiente manera: En la lista de tenant de la página **Tenant Resources Management**, haga clic en el tenant de destino, haga clic en la pestaña **Resource** y haga clic en junto a **Queue Configurations (*Queue name*)**.
- Una cola puede estar enlazada a un solo grupo de recursos no predeterminado.
- Para parámetros como **Max Allocated vCores**, **Max Allocated Memory(MB)**, **Max Running Apps**, **Max Running Apps per User** y **Max Pending Apps**, si el valor de un sub-tenant es de **-1**, el valor del tenant principal se puede establecer a un límite específico. Si el valor del tenant principal es un límite específico, el valor del subtenant se puede establecer en **-1**.
- **Max Allocated vCores** y **Max Allocated Memory(MB)** deben cambiarse a valores distintos de **-1**.

Tabla 7-37 Parámetros de configuración de cola

Parámetro	Descripción
Max Master Shares(%)	Indica el porcentaje máximo de recursos ocupados por todas las ApplicationMasters de la cola actual.

Parámetro	Descripción
Max Allocated vCores	Indica el número máximo de núcleos que se pueden asignar a un solo contenedor Yarn en la cola actual. El valor predeterminado es **-1**, lo que indica que el número de núcleos no está limitado dentro del rango de valores.
Max Allocated Memory(MB)	Indica la memoria máxima que se puede asignar a un solo contenedor Yarn en la cola actual. El valor predeterminado es **-1**, lo que indica que la memoria no está limitada dentro del rango de valores.
Max Running Apps	Indica el número máximo de tareas que se pueden ejecutar al mismo tiempo en la cola actual. El valor predeterminado es **-1**, lo que indica que el número no está limitado dentro del rango de valores. (el significado es el mismo si el valor está vacío). El valor **0** indica que las tareas no se pueden ejecutar. El valor oscila entre **-1** y **2147483647**.
Max Running Apps per User	Indica el número máximo de tareas que puede ejecutar cada usuario en la cola actual al mismo tiempo. El valor predeterminado es **-1**, lo que indica que el número no está limitado dentro del rango de valores. (el significado es el mismo si el valor está vacío). El valor **0** indica que las tareas no se pueden ejecutar. El valor oscila entre **-1** y **2147483647**.
Max Pending Apps	Indica el número máximo de tareas que se pueden suspender al mismo tiempo en la cola actual. El valor predeterminado es **-1**, lo que indica que el número no está limitado dentro del rango de valores. (el significado es el mismo si el valor está vacío). El valor **0** indica que las tareas no se pueden suspender. El valor oscila entre **-1** y **2147483647**.
Resource Allocation Rule	Indica la regla para asignar recursos a diferentes tareas de un usuario. La regla puede ser **FIFO** o **FAIR**. Si un usuario envía varias tareas en la cola actual y la regla es **FIFO**, las tareas se ejecutan una por una en orden secuencial; si la regla es **FAIR**, los recursos se asignan uniformemente a todas las tareas.
Default Resource Label	Indica que las tareas se ejecutan en un nodo con una etiqueta de recurso especificada.
Active	● **ACTIVE**: indica que la cola actual puede recibir y ejecutar tareas. ● **INACTIVE**: indica que la cola actual puede recibir pero no puede ejecutar tareas. Las tareas enviadas a la cola se suspenden.
Open	● **OPEN**: indica que la cola actual está abierta. ● **CLOSED**: indica que la cola actual está cerrada. Las tareas enviadas a la cola se rechazan.

Parámetro	Descripción
Migrate Queue Upon Fault	Si Cross-AZ HA está habilitado para un clúster y una AZ es defectuosa, establezca **Migrate Queue Upon Fault** en **TRUE** para migrar las colas en ejecución del tenant a otras AZ.

Paso 5 Haga clic en **OK**.

----Fin

7.6.2.3.5 Configuración de la política de capacidad de cola de un grupo de recursos

Escenario

Después de agregar un grupo de recursos, puede configurar la política de capacidad de los recursos disponibles para las colas de Yarn para que los trabajos de las colas se puedan ejecutar correctamente en el grupo de recursos.

Esta sección describe cómo configurar la política de cola en FusionInsight Manager. Las colas de tenant equipadas con el programador Superior pueden usar recursos en diferentes grupos de recursos.

Prerrequisitos

- Ha iniciado sesión en FusionInsight Manager.
- Se ha agregado un grupo de recursos.
- La cola de destino no está asociada con los grupos de recursos de otras colas, excepto el grupo de recursos predeterminado.

Procedimiento

Paso 1 En FusionInsight Manager, seleccione **Tenant Resources**.

Paso 2 Elija **Dynamic Resource Plan**.

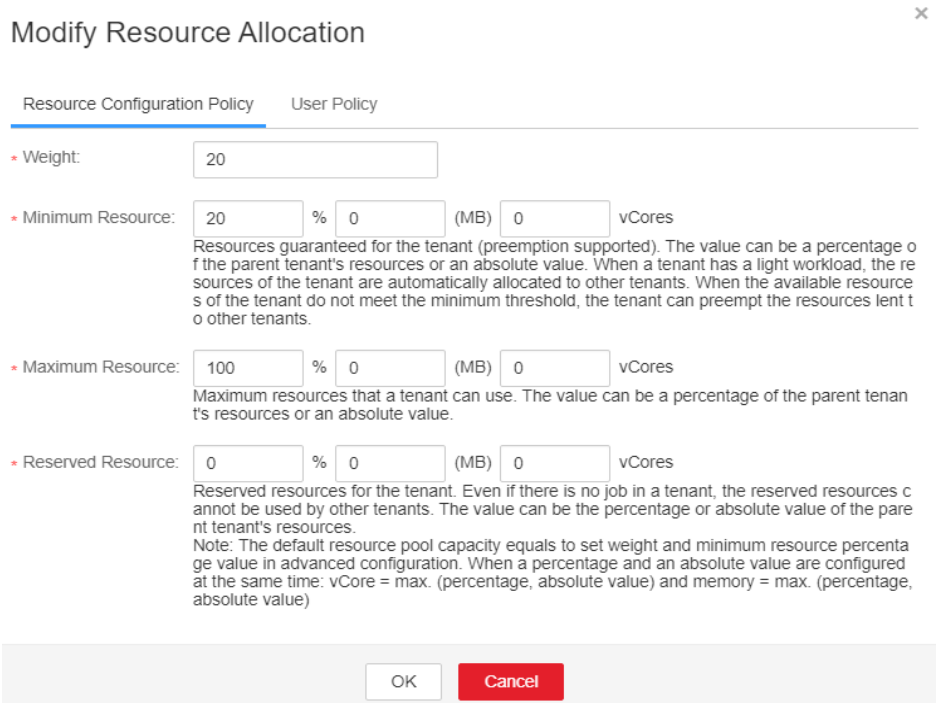
Paso 3 Haga clic en la pestaña **Resource Distribution Policy**.

Paso 4 Seleccione el nombre del clúster de destino en **Cluster** y seleccione un grupo de recursos en **Resource Pool**.

Paso 5 Busque la fila que contiene la cola de destino en el área **Resource Allocation** y haga clic en **Modify** en la columna **Operation**.

Paso 6 En la pestaña **Resource Configuration Policy** de la ventana **Modify Resource Allocation**, establezca la política de configuración de recursos de la cola en el grupo de recursos.

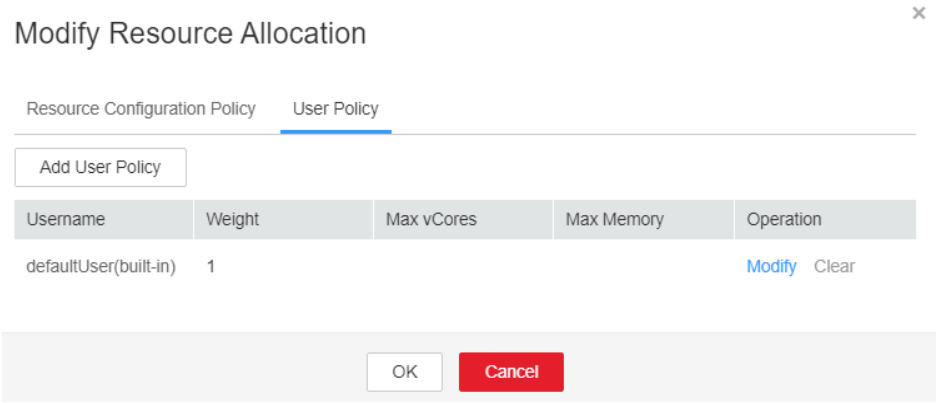
Figura 7-44 Política de configuración de recursos



- **Weight**: La cola de tareas con un peso mayor reemplaza los recursos primero cuando los recursos son insuficientes. Su valor inicial es el mismo que el porcentaje mínimo de recursos.
- **Minimum Resource**: indica los recursos mínimos que un tenant puede obtener.
- **Maximum Resource**: indica el máximo de recursos que un tenant puede obtener.
- **Reserved Resource**: indica los recursos que están reservados para las colas del tenant y no se pueden prestar a las colas de otros tenants.

Paso 7 Haga clic en la pestaña **User Policy** en la ventana **Modify Resource Allocation** y establezca la política de usuario.

Figura 7-45 Política de usuarios

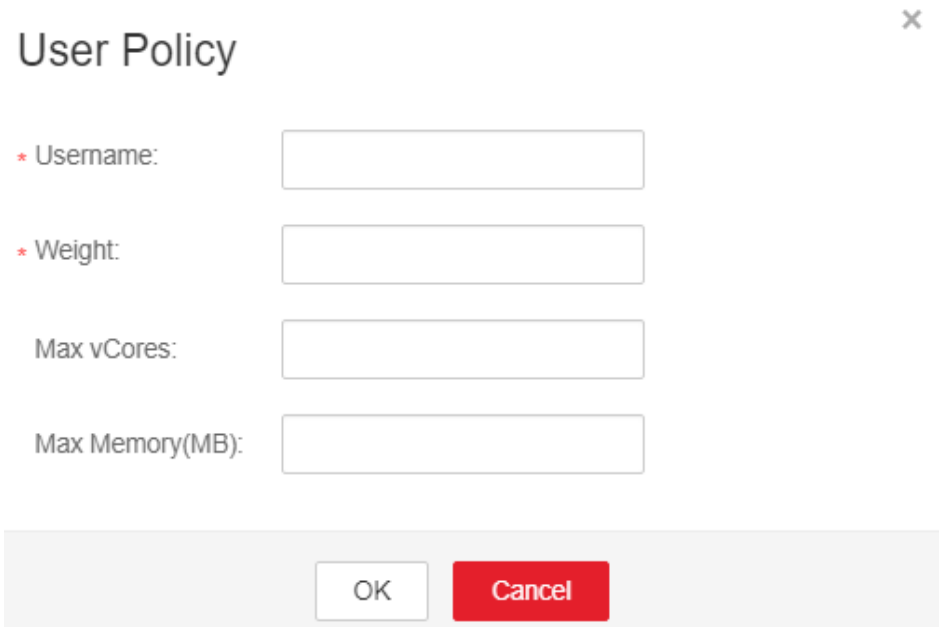


NOTA

defaultUser(built-in) indica que la política especificada para **defaultUser** se utiliza si un usuario no tiene una política. No se puede eliminar la política predeterminada.

- Haga clic en **Add User Policy** para agregar una política de usuario.

Figura 7-46 Adición de una política de usuario



  - **Username**: indica el nombre de un usuario.
  - **Weight**: La cola de tareas con un peso mayor reemplaza los recursos primero cuando los recursos son insuficientes.
  - **Max vCores**: indica el número máximo de núcleos virtuales que el usuario puede obtener.
  - **Max Memory(MB)**: indica la memoria máxima que el usuario puede obtener.
- Haga clic en **Modify** en la columna **Operation** para modificar una política de usuario existente.
- Haga clic en **Clear** en la columna **Operation** para eliminar una política de usuario existente.

Paso 8 Haga clic en **OK**.

----Fin

7.6.2.3.6 Borrar configuraciones de cola

Escenario

Puede borrar las configuraciones de una cola en FusionInsight MRS Manager cuando la cola no necesita recursos de un grupo de recursos o el grupo de recursos necesita estar desasociado de la cola. Al borrar las configuraciones de colas se cancela la política de capacidad de recursos de la cola en el grupo de recursos.

Prerrequisitos

Ha cambiado el grupo de recursos predeterminado de la cola a otro. Si se va a disociar una cola de un grupo de recursos, este grupo de recursos no puede servir como grupo de recursos predeterminado de la cola. Para obtener más información, consulte **Configuración de una cola**.

Procedimiento

Paso 1 Inicie sesión en FusionInsight Manager.

Paso 2 Elija **Tenant Resources** > **Dynamic Resource Plan**.

Paso 3 Seleccione el nombre del clúster de destino en **Cluster** y seleccione un grupo de recursos en **Resource Pool**.

Paso 4 Busque la fila que contiene el nombre del recurso de destino en el área **Resource Allocation** y haga clic en **Clear** en la columna **Operation**.

Paso 5 En el cuadro de diálogo mostrado, haga clic en **OK** para borrar las configuraciones de cola del grupo de recursos actual.

----Fin

7.6.2.4 Gestión de políticas globales de usuario

Escenario

Si un tenant utiliza un planificador Superior, puede configurar la política global para que los usuarios utilicen el planificador de recursos, que incluye:

- Máximo de aplicaciones en ejecución
- Máximo de aplicaciones pendientes
- Cola predeterminada

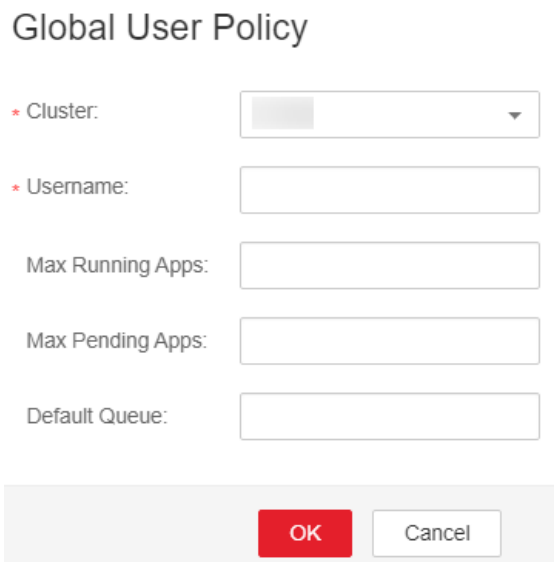
Procedimiento

- Agregue una política.
  a. En FusionInsight Manager, seleccione **Tenant Resources**.
  b. Elija **Dynamic Resource Plan**.
  c. Haga clic en la pestaña **Global User Policy**.

     NOTA

     defaults(default setting) indica que la política especificada para **defaults** se utiliza si un usuario no tiene una política global. No se puede eliminar la política predeterminada.
  d. Haga clic en **Create Global User Policy**. En el cuadro de diálogo que se muestra, establezca los siguientes parámetros:

Figura 7-47 Creación de una política de usuario global



- **Cluster**: Seleccione el clúster de destino.
- **Username**: indica el usuario para el que se controla la programación de recursos. Introduzca un nombre de usuario existente en el clúster actual.
- **Max Running Apps**: indica el número máximo de tareas que el usuario puede ejecutar en el clúster actual.
- **Max Pending Apps**: indica el número máximo de tareas que el usuario puede suspender en el clúster actual.
- **Default Queue**: indica la cola del usuario. Introduzca el nombre de una cola existente en el clúster actual.

- Modificar una política.
  a. En FusionInsight Manager, seleccione **Tenant Resources**.
  b. Elija **Dynamic Resource Plan**.
  c. Haga clic en la pestaña **Global User Policy**.
  d. En la fila que contiene la política de usuario deseada, haga clic en **Modify** en la columna **Operation**.
  e. En el cuadro de diálogo mostrado, modifique los parámetros y haga clic en **OK**.
- Eliminar una política.
  a. En FusionInsight Manager, seleccione **Tenant Resources**.
  b. Elija **Dynamic Resource Plan**.
  c. Haga clic en la pestaña **Global User Policy**.
  d. En la fila que contiene la política de usuario deseada, haga clic en **Delete** en la columna **Operation**.

     En el cuadro de diálogo que se muestra, haga clic en **OK**.

7.6.3 Uso del programador de Capacity

7.6.3.1 Creación de tenants

7.6.3.1.1 Adición de un tenant

Escenario

Puede crear tenants en FusionInsight Manager en función del consumo de recursos y la planificación de aislamiento y los requisitos de los servicios.

Prerrequisitos

- Se ha planificado un nombre de tenant en función de los requisitos de servicio. El nombre no puede ser el mismo que el de un rol, directorio HDFS o cola de Yarn que existe en el clúster actual.
- Los recursos que se asignarán al tenant actual se han previsto para garantizar que la suma de los recursos de subtenants en cada nivel no exceda de los recursos del tenant actual.

Procedimiento

Paso 1 Inicie sesión en el FusionInsight Manager y elija **Tenant Resources**.

Paso 2 Haga clic en . En la página que se muestra, configure los atributos de tenant de acuerdo con **Tabla 7-38**.

Tabla 7-38 Parámetros del tenant

Parámetro	Descripción
Cluster	Indica el clúster para el que desea crear un tenant.
Name	• Indica el nombre del tenant actual. El valor consta de 3 a 50 caracteres, incluidos dígitos, letras y guiones bajos (_). • Planifique un nombre de tenant en función de los requisitos de servicio. El nombre no puede ser el mismo que el de un rol, directorio HDFS o cola de Yarn que existe en el clúster actual.
Tenant Resource Type	Especifica si el tenant es un tenant de hoja. • Cuando se selecciona **Leaf Tenant Resource**, el tenant actual es un tenant de hoja y no se puede agregar ningún subtenant. • Cuando se selecciona **Non-leaf Tenant Resource**, el tenant actual no es un tenant de hoja y se pueden agregar subtenants al tenant actual.

Parámetro	Descripción
Computing Resource	Especifica los recursos de cálculo dinámicos para el tenant actual. ● Cuando se selecciona **Yarn**, el sistema crea automáticamente una cola en Yarn y la cola recibe el mismo nombre que el nombre del tenant. – Un tenant de hoja puede enviar trabajos directamente a la cola. – Un tenant que no sea de hoja no puede enviar trabajos directamente a la cola. Sin embargo, Yarn agrega una cola adicional (oculta) llamada **default** para que el tenant no hoja registre la capacidad de recursos restante del tenant. Los trabajos reales no se ejecutan en esta cola. ● Si **Yarn** no está seleccionado, el sistema no crea automáticamente una cola.
Configuration Mode	Indica el modo de configuración de los parámetros de recursos informáticos. ● Si selecciona **Basic**, solo tendrá que configurar **Default Resource Pool Capacity (%)**. ● Si selecciona **Advanced**, puede configurar manualmente la ponderación de asignación de recursos y los recursos mínimos, máximos y reservados del tenant.
Default Resource Pool Capacity (%)	Indica el porcentaje de recursos informáticos utilizados por el tenant actual en el grupo de recursos predeterminado. El valor oscila entre **0** y **100%**.
Weight	Indica la ponderación de asignación de recursos. El valor varía de **0** a **100**.
Minimum Resource	Indica los recursos garantizados para el tenant (se admite la preferencia). El valor puede ser un porcentaje o un valor absoluto de los recursos del tenant principal. Cuando un tenant tiene una carga de trabajo ligera, los recursos del tenant se asignan automáticamente a otros tenants. Cuando los recursos disponibles del tenant son menores que el valor de **Minimum Resource**, el tenant puede adelantarse a los recursos que se han prestado a otros tenants.
Maximum Resource	Indica el máximo de recursos que puede utilizar el tenant. El tenant no puede obtener más recursos que el valor configurado. El valor puede ser un porcentaje o un valor absoluto de los recursos del tenant principal.
Reserved Resource	Indica los recursos reservados para el tenant. Los recursos reservados no pueden ser utilizados por otros tenants aunque no se esté ejecutando ningún trabajo en los recursos actuales del tenant. El valor puede ser un porcentaje o un valor absoluto de los recursos del tenant principal.

Parámetro	Descripción
Storage Resource	Especifica los recursos de almacenamiento para el tenant actual. ● Cuando se selecciona **HDFS**, el sistema asigna automáticamente los recursos de almacenamiento. ● Cuando **HDFS** no está seleccionado, el sistema no asigna automáticamente los recursos de almacenamiento.
Quota	Indica la cuota de archivos y directorios.
Space Quota	Indica la cuota para el espacio de almacenamiento HDFS utilizado por el tenant actual. ● Si la unidad está establecida en **MB**, el valor varía entre **1** y **8796093022208**. Si la unidad está establecida en **GB**, el valor varía entre **1** y **8589934592**. ● Este parámetro indica el espacio de almacenamiento HDFS máximo que puede utilizar el tenant, pero no el espacio real utilizado. ● Si su valor es mayor que el tamaño del disco físico HDFS, el espacio máximo disponible es el espacio completo del disco físico HDFS.
Storage Path	Indica un directorio HDFS para los datos de recursos del tenant. ● El sistema crea automáticamente una carpeta con el nombre del tenant en el directorio **/tenant** de forma predeterminada. Por ejemplo, el directorio de almacenamiento HDFS predeterminado para el **ta1** del tenant es **/tenant/ta1**. ● Cuando se crea un tenant por primera vez, el sistema crea el directorio **/tenant** en el directorio raíz HDFS. La ruta de almacenamiento es personalizable.
Service	Especifica si se asocian recursos de otros servicios. Para obtener más información, consulte **Paso 4**.
Description	Indica la descripción del tenant actual.

NOTA

Los roles, los recursos informáticos y los recursos de almacenamiento se crean automáticamente cuando se crean los tenants.

- El nuevo rol tiene permisos sobre los recursos informáticos y de almacenamiento. Este rol y sus permisos son controlados automáticamente por el sistema y no se pueden gestionar manualmente eligiendo **System** > **Permission** > **Role**. El nombre del rol tiene el formato de *Tenant name_Cluster ID*. El ID del primer clúster no se muestra de forma predeterminada.
- Cuando utilice este tenant, cree un usuario del sistema y vincule al usuario al rol del tenant. Para obtener más información, consulte **Adición de un usuario y vinculación del usuario a un rol de tenant**.
- Durante la creación del tenant, el sistema crea automáticamente una cola de Yarn con el nombre del tenant. Si el nombre de la cola ya existe, la nueva cola se denomina **Tenant name-***N*. *N* indica un número natural a partir de **1**. Cuando existe un mismo nombre, el valor *N* aumenta automáticamente para diferenciar la cola de los demás. Por ejemplo, **saletenant**, **saletenant-1** y **saletenant-2**.

Paso 3 Compruebe si el tenant actual necesita estar asociado con recursos de otros servicios.

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 5**.

Paso 4 Haga clic en **Associate Service** para configurar otros recursos de servicio utilizados por el tenant actual.

- Establezca **Service** en **HBase** y **Association Type** en **Exclusive** o **Shared**.

  NOTA

  - **Exclusive** indica que los recursos de servicio son utilizados exclusivamente por el tenant y no pueden asociarse con otros tenants.
  - **Shared** indica que los recursos de servicio se pueden compartir con otros tenants.

NOTA

- Solo HBase puede asociarse con un nuevo tenant. Sin embargo, HDFS, HBase y Yarn pueden asociarse con tenants existentes.
- Para asociar un tenant existente a los recursos de servicio, haga clic en el tenant de destino en la lista de tenant, cambie a la página **Service Associations** y haga clic en **Associate Service** para configurar los recursos que se asociarán al tenant.
- Para desasociar un tenant existente de los recursos de servicio, haga clic en el tenant de destino en la lista de tenant, cambie a la página **Service Associations** y haga clic en **Delete** en la columna **Operation**. En el cuadro de diálogo que se muestra, seleccione **I have read the information and understand the impact** y haga clic en **OK**.

1. Haga clic en **OK**.

Paso 5 Haga clic en **OK**. Espere hasta que el sistema muestre un mensaje que indique que el tenant se ha creado correctamente.

----Fin

7.6.3.1.2 Adición de un subtenant

Escenario

Puede crear subtenants en FusionInsight Manager y asignar recursos del tenant actual a los subtenants en función del consumo de recursos y la planificación de aislamiento y los requisitos de los servicios.

Prerrequisitos

- Se ha agregado un tenant principal que no es de hoja.
- Se ha planificado un nombre de tenant en función de los requisitos de servicio. El nombre no puede ser el mismo que el de un rol, directorio HDFS o cola de Yarn que existe en el clúster actual.
- Los recursos que se asignarán al tenant actual se han previsto para garantizar que la suma de los recursos de subtenants en cada nivel no exceda de los recursos del tenant actual.

Procedimiento

Paso 1 Inicie sesión en el FusionInsight Manager y elija **Tenant Resources**.

Paso 2 En la lista de tenants de la izquierda, seleccione un tenant principal y haga clic en  . En la página para agregar un subtenant, establezca atributos para el subtenant según **Tabla 7-39**.

Tabla 7-39 Parámetros de subtenant

Parámetro	Descripción
Cluster	Indica el clúster al que pertenece el tenant principal.
Parent Tenant Resource	Indica el nombre del tenant principal.
Name	• Indica el nombre del tenant actual. El valor consta de 3 a 50 caracteres, incluidos dígitos, letras y guiones bajos (_). • Planifique un nombre de subtenant basado en los requisitos de servicio. El nombre no puede ser el mismo que el de un rol, directorio HDFS o cola de Yarn que existe en el clúster actual.
Tenant Type	Especifica si el tenant es un tenant de hoja. • Cuando se selecciona **Leaf Tenant**, el tenant actual es un tenant hoja y no se puede agregar ningún subtenant. • Cuando se selecciona **Non-leaf Tenant**, el tenant actual no es un tenant hoja y se pueden agregar subtenants al tenant actual. Sin embargo, la profundidad del tenant no puede exceder de 5 niveles.

Parámetro	Descripción
Computing Resource	Especifica los recursos de cálculo dinámicos para el tenant actual. ● Cuando se selecciona **Yarn**, el sistema crea automáticamente una cola en Yarn y la cola recibe el mismo nombre que el nombre del subtenant. – Un tenant de hoja puede enviar trabajos directamente a la cola. – Un tenant que no sea de hoja no puede enviar trabajos directamente a la cola. Sin embargo, Yarn agrega una cola adicional (oculta) llamada **default** para que el tenant no hoja registre la capacidad de recursos restante del tenant. Los trabajos reales no se ejecutan en esta cola. ● Si **Yarn** no está seleccionado, el sistema no crea automáticamente una cola.
Default Resource Pool Capacity (%)	Indica el porcentaje de recursos informáticos utilizados por el tenant actual. El valor base es el total de recursos del tenant principal.
Default Resource Pool Max Capacity (%)	Indica el porcentaje máximo de recursos informáticos utilizados por el tenant actual. El valor base es el total de recursos del tenant principal.
Storage Resource	Especifica los recursos de almacenamiento para el tenant actual. ● Cuando se selecciona **HDFS**, el sistema crea automáticamente una carpeta con el nombre del subtenant en el directorio de tenant principal de HDFS. ● Cuando **HDFS** no está seleccionado, el sistema no asigna automáticamente los recursos de almacenamiento.
Quota	Indica la cuota de archivos y directorios.
Space Quota	Indica la cuota para el espacio de almacenamiento HDFS utilizado por el tenant actual. ● Si la unidad está establecida en **MB**, el valor varía entre **1** y **8796093022208**. Si la unidad está establecida en **GB**, el valor varía entre **1** y **8589934592**. ● Este parámetro indica el espacio de almacenamiento HDFS máximo que puede utilizar el tenant, pero no el espacio real utilizado. ● Si su valor es mayor que el tamaño del disco físico HDFS, el espacio máximo disponible es el espacio completo del disco físico HDFS. ● Si esta cuota es mayor que la cuota del tenant principal, el espacio de almacenamiento real no excede la cuota del tenant principal.

Parámetro	Descripción
Storage Path	Indica el directorio de almacenamiento de HDFS para el tenant. ● El sistema crea automáticamente una carpeta con el nombre del subtenant en el directorio del tenant principal de forma predeterminada. Por ejemplo, si el subtenant es **ta1s** y el directorio principal es **/tenant/ta1**, la ruta de almacenamiento para el subtenant es entonces **/tenant/ta1/ta1s**. ● La ruta de almacenamiento se puede personalizar en el directorio principal.
Description	Indica la descripción del tenant actual.

NOTA

Los roles, los recursos informáticos y los recursos de almacenamiento se crean automáticamente cuando se crean los tenants.

- El nuevo rol tiene permisos sobre los recursos informáticos y de almacenamiento. Este rol y sus permisos son controlados automáticamente por el sistema y no se pueden gestionar manualmente eligiendo **System** > **Permission** > **Role**. El nombre del rol tiene el formato de *Tenant name*_*Cluster ID*. El ID del primer clúster no se muestra de forma predeterminada.
- Cuando utilice este tenant, cree un usuario del sistema y vincule al usuario al rol del tenant. Para obtener más información, consulte **Agregar un usuario y vincularlo a un rol de tenant**.
- El subtenant puede asignar además los recursos de su tenant principal. La suma de los porcentajes de recursos de subtenants directos bajo un tenant principal en cada nivel no puede exceder 100%. La suma de los porcentajes de recursos de computación de todos los tenants de nivel 1 no puede exceder el 100%.

Paso 3 Compruebe si el tenant actual necesita estar asociado con recursos de otros servicios.

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 5**.

Paso 4 Haga clic en **Associate Service** para configurar otros recursos de servicio utilizados por el tenant actual.

1. Ajusta **Services** a **HBase**.
2. Establezca **Association Type** de la siguiente manera:
   - **Exclusive** indica que los recursos de servicio son utilizados exclusivamente por el tenant y no pueden asociarse con otros tenants.
   - **Shared** indica que los recursos de servicio se pueden compartir con otros tenants.

NOTA

- Solo HBase puede asociarse con un nuevo tenant. Sin embargo, HDFS, HBase y Yarn pueden asociarse con tenants existentes.
- Para asociar un tenant existente a los recursos de servicio, haga clic en el tenant de destino en la lista de tenant, cambie a la página **Service Associations** y haga clic en **Associate Service** para configurar los recursos que se asociarán al tenant.
- Para desasociar un tenant existente de los recursos de servicio, haga clic en el tenant de destino en la lista de tenant, cambie a la página **Service Associations** y haga clic en **Delete** en la columna **Operation**. En el cuadro de diálogo que se muestra, seleccione **I have read the information and understand the impact** y haga clic en **OK**.

3. Haga clic en **OK**.

Paso 5 Haga clic en **OK**. Espere hasta que el sistema muestre un mensaje que indique que el tenant se ha creado correctamente.

----Fin

7.6.3.1.3 Adición de un usuario y vinculación del usuario a un rol de tenant

Escenario

Un tenant recién creado no puede iniciar sesión directamente en el clúster para acceder a los recursos. Debe agregar un usuario para el tenant en FusionInsight Manager y vincularlo al rol del tenant para asignar permisos de operación al usuario.

Prerrequisitos

Ha aclarado los requisitos de servicio y ha creado un tenant.

Procedimiento

Paso 1 Inicie sesión en FusionInsight Manager y elija **System** > **Permission** > **User**.

Paso 2 Si desea agregar un usuario al sistema, haga clic en **Create**.

Si desea enlazar roles de inquilino a un usuario existente en el sistema, busque la fila del usuario y haga clic en **Modify** en la columna **Operation**.

Establezca los atributos de usuario según **Tabla 7-40**.

Tabla 7-40 Parámetros del usuario

Parámetro	Descripción
Username	Especifica el nombre de usuario actual. El valor puede contener de 3 a 32 caracteres, incluidos dígitos, letras, guiones bajos (_), guiones (-) y espacios. ● El nombre de usuario no puede ser el mismo que el nombre de usuario del sistema operativo de cualquier nodo del clúster. De lo contrario, no se puede utilizar el usuario. ● No se permite un nombre de usuario que difiera solo en mayúsculas y minúsculas de un nombre de usuario existente. Por ejemplo, si **User1** se ha creado, no puede crear **user1**. Ingrese el nombre de usuario correcto cuando utilice **User1**.
User Type	Las opciones son **Human-Machine** y **Machine-Machine**. ● Usuario de **Human-Machine**: utilizado para FusionInsight Manager O&M y las operaciones del cliente de componentes. Si selecciona esta opción, establezca **Password** y **Confirm Password** en consecuencia. ● Usuario de **Machine-Machine**: utilizado para el desarrollo de aplicaciones. Si selecciona esta opción, la contraseña se genera aleatoriamente.
Password	Este parámetro es obligatorio si **User Type** tiene el valor de **Human-Machine**. La contraseña debe contener de 8 a 64 caracteres de al menos cuatro tipos de los siguientes: letras mayúsculas, minúsculas, dígitos, caracteres especiales y espacios. La contraseña no puede ser el nombre de usuario o el nombre de usuario escrito al revés.
Confirm Password	Vuelva a ingresar la contraseña.
User Group	En el área **User Group**, haga clic en **Add** y seleccione grupos de usuarios para agregar el usuario a los grupos. ● Si se han agregado roles a los grupos de usuarios, se pueden conceder al usuario los permisos de los roles. ● Por ejemplo, agregue el usuario al grupo de usuarios de Hive para asignar permisos de Hive al usuario.
Primary Group	Seleccione un grupo como grupo principal para que el usuario cree directorios y archivos. La lista desplegable contiene todos los grupos seleccionados en **User Group**.
Role	Haga clic en **Add** para vincular un rol de tenant al usuario. **NOTA** Si un usuario desea utilizar los recursos del tenant **tenant1** y agregar o eliminar subtenants para **tenant1**, debe estar enlazado a los roles **Manager_tenant** y **tenant1**_*Cluster ID*.

Parámetro	Descripción
Description	Indica la descripción del usuario actual.

Paso 3 Haga clic en **OK**.

----Fin

7.6.3.2 Gestión de tenants

7.6.3.2.1 Gestión de directorios de tenant

Escenario

Puede gestionar los directorios de almacenamiento de HDFS que utilizan los tenants especificados en función de los requisitos de servicio del FusionInsight Manager, como agregar directorios de tenant, cambiar las cuotas para directorios y archivos y para espacio de almacenamiento, y eliminar directorios.

Prerrequisitos

Se ha agregado un tenant con recursos de almacenamiento de HDFS.

Ver un directorio de tenant

Paso 1 En el FusionInsight Manager, seleccione **Tenant Resources**.

Paso 2 En la lista de tenant de la izquierda, haga clic en el tenant de destino.

Paso 3 Haga clic en la pestaña **Resource**.

Paso 4 Vea la tabla **HDFS Storage**.

- La columna **File Number Threshold** proporciona la cuota para los archivos y directorios del directorio del tenant.
- La columna **Space Quota** proporciona el tamaño del espacio de almacenamiento del directorio del tenant.

----Fin

Adición de un directorio de tenant

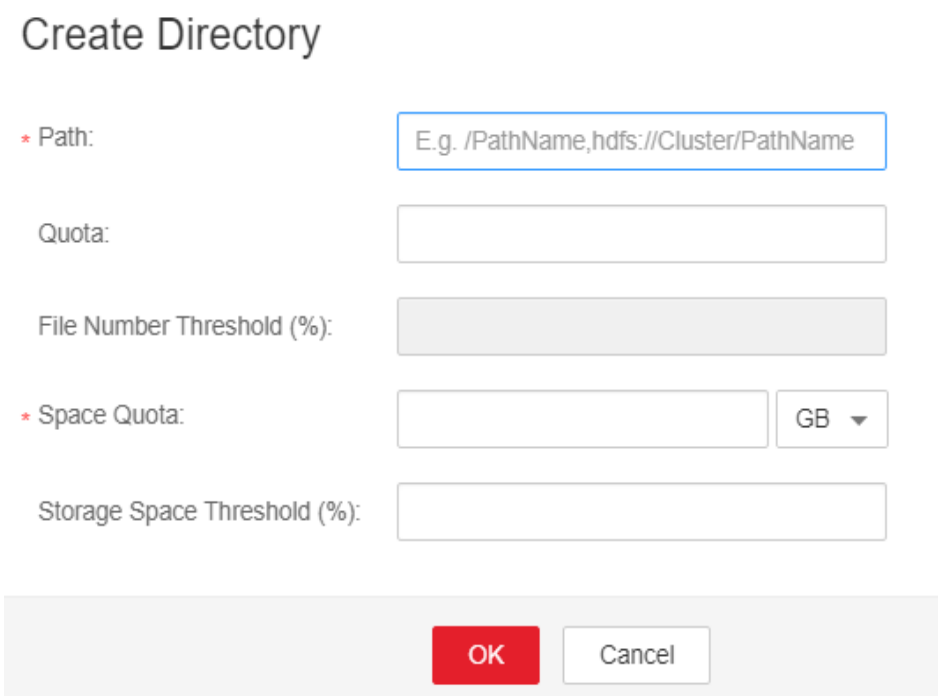
Paso 1 En el FusionInsight Manager, seleccione **Tenant Resources**.

Paso 2 En la lista de tenant de la izquierda, haga clic en el tenant de destino.

Paso 3 Haga clic en la pestaña **Resource**.

Paso 4 En el área **HDFS Storage**, haga clic en **Create Directory**.

Figura 7-48 Creación de un directorio



- **Parent Directory**: indica el directorio de almacenamiento utilizado por el tenant principal del inquilino actual.

  NOTA

  Este parámetro no se muestra si el tenant actual no es un subtenant.

- Establezca **Path** en una ruta de directorio del tenant.

  NOTA

  Si el tenant actual no es un subtenant, la nueva ruta se crea en el directorio raíz de HDFS.

- Establezca **Quota** en la cuota de archivos y directorios.
- **File Number Threshold (%)** sólo es válido cuando **Quota** está establecido. Si la relación entre el número de archivos usados y el valor de **Quota** excede el valor de este parámetro, se genera una alarma. Si no se especifica este parámetro, no se notifica ninguna alarma en este escenario.

  NOTA

  El número de archivos usados se recopila cada hora. Por lo tanto, la alarma que indica que la relación de archivos usados excede el umbral se retrasa.

- Establezca **Space Quota** en el tamaño del espacio de almacenamiento del directorio del tenant.
- Si la relación entre el espacio de almacenamiento usado y el valor de **Space Quota** excede el valor **Storage Space Threshold (%)**, se genera una alarma. Si no se especifica este parámetro, no se notifica ninguna alarma en este escenario.

  NOTA

  El espacio de almacenamiento utilizado se recoge cada hora. Por lo tanto, la alarma que indica que la relación de espacio de almacenamiento usado excede el umbral se retrasa.

Paso 5 Haga clic en **OK**.

----Fin

Modificación de un directorio de tenant

Paso 1 En el FusionInsight Manager, seleccione **Tenant Resources**.

Paso 2 En la lista de tenant de la izquierda, haga clic en el tenant de destino.

Paso 3 Haga clic en la pestaña **Resource**.

Paso 4 En la tabla **HDFS Storage**, haga clic en **Modify** en la columna **Operation** del directorio de tenant especificado.

- Establezca **Quota** en la cuota de archivos y directorios.
- **File Number Threshold (%)** sólo es válido cuando **Quota** está establecido. Si la relación entre el número de archivos usados y el valor de **Quota** excede el valor de este parámetro, se genera una alarma. Si no se especifica este parámetro, no se notifica ninguna alarma en este escenario.
- Establezca **Space Quota** en el tamaño del espacio de almacenamiento del directorio del tenant.
- Si la relación entre el espacio de almacenamiento usado y el valor de **Space Quota** excede el valor **Storage Space Threshold (%)**, se genera una alarma. Si no se especifica este parámetro, no se notifica ninguna alarma en este escenario.

Paso 5 Haga clic en **OK**.

----Fin

Eliminación de un directorio de tenant

Paso 1 En el FusionInsight Manager, seleccione **Tenant Resources**.

Paso 2 En la lista de tenant de la izquierda, haga clic en el tenant de destino.

Paso 3 Haga clic en la pestaña **Resource**.

Paso 4 En la tabla **HDFS Storage**, haga clic en **Delete** en la columna **Operation** del directorio de tenant especificado.

NOTA

No se puede eliminar el directorio del tenant creado por el sistema durante la creación del tenant.

Paso 5 Haga clic en **OK**.

----Fin

7.6.3.2.2 Restauración de datos de tenant

Escenario

Los datos del tenant se almacenan en el FusionInsight Manager y en los componentes del clúster. Cuando los componentes se recuperan de fallas o se reinstalan, algunos datos de configuración de todos los tenants pueden volverse anormales. En este caso, debe restaurar manualmente los datos de configuración en el FusionInsight Manager.

Procedimiento

Paso 1 Inicie sesión en el FusionInsight Manager y elija **Tenant Resources**.

Paso 2 En la lista de tenant de la izquierda, haga clic en el tenant de destino.

Paso 3 Compruebe el estado de los datos del tenant.

1. En la página **Summary**, verifique **Tenant Status**. Un icono verde indica que el tenant está disponible y gris indica que el tenant no está disponible.
2. Haga clic en **Resource** y compruebe los iconos a la izquierda de **Yarn** y **HDFS Storage**. Un icono verde indica que el recurso está disponible y el gris indica que el recurso no está disponible.
3. Haga clic en **Service Associations** y compruebe la columna **Status** de los servicios asociados. **Normal** indica que el componente puede proporcionar servicios para el tenant asociado. **Not Available** indica que el componente no puede proporcionar servicios al tenant.
4. Si alguno de los elementos de comprobación anteriores es anormal, vaya a **Paso 4** para restaurar los datos del tenant.

Paso 4 Haga clic en  . En el cuadro de diálogo que se muestra, introduzca la contraseña del usuario de inicio de sesión actual y haga clic en **OK**.

Paso 5 En la ventana **Restore Tenant Resource Data**, seleccione uno o más componentes para restaurar los datos y haga clic en **OK**. El sistema restaura automáticamente los datos del tenant.

----Fin

7.6.3.2.3 Eliminación de un tenant

Escenario

Puede eliminar tenants que ya no se utilizan en FusionInsight Manager según los requisitos de servicio para liberar recursos ocupados por los tenants.

Prerrequisitos

- Se ha agregado un tenant.
- El tenant no tiene sub-tenants. Si el tenant tiene sub-tenants, elimínelos; de lo contrario, no se puede eliminar el tenant.
- El rol del tenant no está asociado con ningún usuario o grupo de usuarios.

Procedimiento

Paso 1 Inicie sesión en el FusionInsight Manager y elija **Tenant Resources**.

Paso 2 En la lista de tenant de la izquierda, haga clic en el tenant de destino y haga clic en  .

NOTA

- Si desea conservar los datos del tenant, seleccione **Reserve the data of this tenant resource**. De lo contrario, se eliminará el espacio de almacenamiento del tenant.
- Para eliminar un tenant sin conservar los datos del tenant como un usuario que no pertenece al supergrupo, primero debe iniciar sesión en el cliente HDFS como un usuario que pertenece al supergrupo y, a continuación, borrar manualmente el espacio de almacenamiento de ese tenant para evitar datos residuales.

Paso 3 Haga clic en **OK**.

Se tarda unos minutos en guardar la configuración. Después de eliminar el tenant, el rol y el espacio de almacenamiento del tenant también se eliminan.

NOTA

Después de eliminar el tenant, la cola del tenant todavía existe en Yarn. La cola del tenant no se muestra en la página de gestión de roles en Yarn.

----Fin

7.6.3.2.4 Borrar colas no asociadas de un tenant

Escenario

Si Yarn utiliza el Capacity scheduler, eliminar un tenant solo establece la capacidad de cola del tenant en **0** y el estado del tenant en **STOPPED** pero no borra las colas del tenant en Yarn. Limitado por el mecanismo de Yarn, las colas no se pueden eliminar dinámicamente. Puede ejecutar comandos para eliminar manualmente las colas residuales.

Impacto en el sistema

- Durante la ejecución del script, se reinicia el servicio Controller, se sincronizan las configuraciones de Yarn y se reinician los ResourceManagers activo y en espera.
- FusionInsight Manager se vuelve inaccesible durante el reinicio del servicio Controller.
- Después de reiniciar las ResourceManagers activa y en espera, se genera una alarma que indica que Yarn y los componentes que dependen de Yarn no están disponibles temporalmente.

Prerrequisitos

Todavía existen colas de un tenant eliminado.

Procedimiento

Paso 1 Compruebe que las colas del tenant eliminado todavía existen.

1. En FusionInsight Manager, elija **Cluster**, haga clic en el nombre del clúster de destino y elija **Services** > **Yarn**. Haga clic en el enlace del ResourceManager activo de **ResourceManager WebUI** para ir a la interfaz de usuario web ResourceManager.
2. Haga clic en **Scheduler** en el árbol de navegación de la izquierda. En el panel derecho, puede ver que las colas del tenant todavía existen en el estado **STOPPED** y su **Configured Capacity** es **0**.

Paso 2 Inicie sesión en el nodo de gestión activo como usuario **omm**.

Paso 3 Cambie el directorio y ejecute el script **cleanQueuesAndRestartRM.sh**.

cd ${BIGDATA_HOME}/om-server/om/sbin

./cleanQueuesAndRestartRM.sh -c *Cluster ID*

NOTA

Puede elegir **Cluster**, hacer clic en el nombre del clúster y elegir **Cluster Properties** en FusionInsight Manager para ver el ID del clúster.

Durante la ejecución del script, debe ingresar **yes** y la contraseña.

```
Running the script will restart Controller and restart ResourceManager.
Are you sure you want to continue connecting (yes/no)?yes
Please input admin password:
Begin to backup queues ...
...
```

Paso 4 Una vez que el script se ejecute correctamente, inicie sesión en el Administrador de FusionInsight, elija **Cluster**, haga clic en el nombre del clúster y elija **Services** > **Yarn**. Haga clic en el enlace del ResourceManager activo de **ResourceManager WebUI** para ir a la interfaz de usuario web ResourceManager.

Paso 5 Haga clic en **Scheduler** en el árbol de navegación de la izquierda. En el panel derecho, puede ver que las colas del inquilino se han borrado.

----Fin

7.6.3.3 Gestión de recursos

7.6.3.3.1 Adición de un grupo de recursos

Escenario

En un clúster, puede agrupar lógicamente NodeManagers de Yarn en grupos de recursos de Yarn. Cada NodeManager pertenece a un solo grupo de recursos. Puede crear un grupo de recursos personalizado en FusionInsight Manager y agregar los hosts que no se han agregado a ningún grupo de recursos personalizado a este grupo de recursos para que las colas especificadas puedan usar los recursos informáticos proporcionados por estos hosts.

El sistema contiene un grupo de recursos **default** de forma predeterminada. Todas las NodeManagers que no se agregan a grupos de recursos personalizados pertenecen a este grupo de recursos.

Procedimiento

Paso 1 Inicie sesión en FusionInsight Manager.

Paso 2 Elija **Tenant Resources** > **Resource Pool**.

Paso 3 Haga clic en **Add Resource Pool**.

Paso 4 Establezca los atributos del grupo de recursos.

- **Cluster**: Seleccione el clúster al que se va a agregar el grupo de recursos.
- **Name**: Introduzca el nombre del grupo de recursos. El nombre contiene de 1 a 50 caracteres, incluidos dígitos, letras y guiones bajos (_), y no puede comenzar con un guion bajo (_).

- **Resource Label**: Introduzca la etiqueta de recursos del grupo de recursos. El valor puede contener de 1 a 50 caracteres, incluidos dígitos, letras, guiones bajos (_), y guiones (-), y debe comenzar con un dígito o letra.
- **Resource**: En el área **Available Hosts**, seleccione los hosts especificados y haga clic en >> para agregar los hosts al área **Selected Hosts**. Solo se pueden seleccionar los hosts del clúster. La lista de hosts del grupo de recursos se puede dejar en blanco.

  NOTA

  Puede filtrar hosts por nombre de host, número de núcleos de CPU, memoria, sistema de operación o tipo de plataforma según los requisitos del servicio.

Paso 5 Haga clic en **OK**.

Después de crear el grupo de recursos, puede ver su nombre, miembros y modo en la lista del grupo de recursos. Los hosts que se agregan al grupo de recursos personalizado ya no son miembros del grupo de recursos **default**.

----Fin

7.6.3.3.2 Modificación de un grupo de recursos

Escenario

Cuando es necesario ajustar los hosts de un grupo de recursos en función de los requisitos de servicio, puede modificar los miembros del grupo de recursos en FusionInsight Manager.

Procedimiento

Paso 1 Inicie sesión en FusionInsight Manager.

Paso 2 Elija **Tenant Resources** > **Resource Pool**.

Paso 3 Busque la fila que contiene el grupo de recursos especificado y haga clic en **Edit** en la columna **Operation**.

Paso 4 En el área **Resource**, modifique hosts.

- Agregar hosts: Seleccione los hosts deseados en **Available Hosts** y haga clic en >> para agregarlos al grupo de recursos.
- Eliminar hosts: Seleccione los hosts deseados de **Selected Hosts** y haga clic en << para quitarlos del grupo de recursos. La lista de hosts del grupo de recursos se puede dejar en blanco.

Paso 5 Haga clic en **OK**.

----Fin

7.6.3.3.3 Eliminación de un grupo de recursos

Escenario

Si ya no se utiliza un grupo de recursos en función de los requisitos de servicio, puede eliminarlo en FusionInsight Manager.

Prerrequisitos

- Cualquier cola del clúster no utiliza el grupo de recursos que se eliminará como el grupo de recursos predeterminado. Antes de eliminar el grupo de recursos, cancele el grupo de recursos predeterminado. Para obtener más información, consulte **Configuración de una cola**.
- Las políticas de distribución de recursos de todas las colas se han borrado del grupo de recursos que se van a eliminar. Para obtener más información, consulte **Borrar configuraciones de cola**.

Procedimiento

Paso 1 Inicie sesión en FusionInsight Manager.

Paso 2 Elija **Tenant Resources** > **Resource Pool**.

Paso 3 Busque la fila que contiene el grupo de recursos especificado y haga clic en **Delete** en la columna **Operation**.

Paso 4 En el cuadro de diálogo que se muestra, haga clic en **OK**.

----Fin

7.6.3.3.4 Configuración de una cola

Escenario

Puede modificar las configuraciones de cola de un tenant especificado en FusionInsight Manager.

Prerrequisitos

Se ha agregado un tenant que utiliza el programador de capacidad.

Procedimiento

Paso 1 Inicie sesión en FusionInsight Manager.

Paso 2 Elija **Tenant Resources** > **Dynamic Resource Plan**.

La página **Resource Distribution Policy** se muestra de forma predeterminada.

Paso 3 Haga clic en la pestaña **Queue Configurations**.

Paso 4 Establezca **Cluster** en el nombre del clúster de destino. En el área **All tenants resources**, busque la fila que contiene el recurso de tenant de destino y haga clic en **Modify** en la columna **Operation**.

NOTA

- También puede acceder a la página **Modify Queue Configuration** de la siguiente manera: En la lista de tenant de la página **Tenant Resources Management**, haga clic en el tenant de destino, haga clic en la pestaña **Resource** y haga clic en junto a **Queue Configurations (*Queue name*)**.
- Una cola puede estar enlazada a un solo grupo de recursos no predeterminado. Es decir, un grupo de recursos recién agregado se puede enlazar a una cola para servir como el grupo de recursos predeterminado de la cola.

Tabla 7-41 Parámetros de configuración de cola

Parámetro	Descripción
Tenant Resources Name (Queue)	Indica el nombre del tenant y el nombre de la cola.
Maximum Applications	Indica el número máximo de aplicaciones.
Maximum AM Resource Percent	Indica el porcentaje máximo de recursos que se pueden utilizar para ejecutar el ApplicationMaster en un clúster.
Minimum User Resource Upper-Limit Percent (%)	Indica la garantía mínima de recursos (porcentaje) de un usuario. Los recursos para cada usuario en una cola están limitados en cualquier momento. Si las aplicaciones de varios usuarios se ejecutan al mismo tiempo en una cola, el uso de recursos de cada usuario fluctúa entre el valor mínimo y el valor máximo. El valor mínimo se determina por el número de aplicaciones en ejecución, mientras que el valor máximo se determina por este parámetro. Por ejemplo, supongamos que este parámetro está establecido en **25**. Si dos usuarios envían aplicaciones a la cola, cada usuario puede usar un máximo del 50% de recursos; si tres usuarios envían aplicaciones a la cola, cada usuario puede usar un máximo del 33% de recursos; si cuatro usuarios envían aplicaciones a la cola, cada usuario puede utilizar un máximo del 25% de recursos.
User Resource Upper-Limit Factor	Indica el factor límite del uso máximo de recursos de usuario. El porcentaje máximo de uso de recursos de usuario se puede obtener multiplicando el factor límite por el porcentaje del uso real de recursos del tenant en el clúster.
Status	Indica el estado actual de un plan de recursos. El valor puede ser **running** o **stopped**.
Default Resource Pool	Indica el grupo de recursos utilizado por la cola. El valor predeterminado es **default**. Si desea cambiar el grupo de recursos, configure primero la capacidad de la cola. Para obtener más información, consulte **Configuración de la política de capacidad de cola de un grupo de recursos**.

Paso 5 Haga clic en **OK**.

----Fin

7.6.3.3.5 Configuración de la política de capacidad de cola de un grupo de recursos

Escenario

Después de agregar un grupo de recursos, puede configurar la política de capacidad de los recursos disponibles para las colas de Yarn para que los trabajos de las colas se puedan

ejecutar correctamente en el grupo de recursos. Una cola puede tener la política de capacidad de cola de un solo grupo de recursos.

Puede ver las colas y configurar políticas de capacidad de cola en cualquier grupo de recursos. Una vez configuradas las políticas de cola, las colas de Yarn se asocian a grupos de recursos.

Prerrequisitos

Se ha agregado una cola, es decir, se ha creado un tenant asociado con recursos informáticos.

Procedimiento

Paso 1 Inicie sesión en FusionInsight Manager.

Paso 2 Elija **Tenant Resources** > **Dynamic Resource Plan**.

La página **Resource Distribution Policy** se muestra de forma predeterminada.

Paso 3 Seleccione el nombre del clúster de destino en **Cluster** y seleccione un grupo de recursos en **Resource Pool**.

Paso 4 Busque la fila que contiene el nombre del recurso de destino en el área **Resource Allocation** y haga clic en **Modify** en la columna **Operation**.

Paso 5 En la ventana **Modify Resource Allocation**, configure la política de capacidad de recursos de la cola en el grupo de recursos.

- **Capacity (%)**: indica el porcentaje de recursos informáticos utilizados por el tenant actual.
- **Maximum Capacity (%)**: indica el porcentaje máximo de recursos informáticos utilizados por el tenant actual.

Paso 6 Haga clic en **OK**.

NOTA

Después de eliminar y guardar los valores de capacidad de recursos de una cola, se cancela la política de capacidad de recursos de la cola en el grupo de recursos, lo que indica que la cola está desasociada del grupo de recursos. Para lograr esto, debe cambiar el grupo de recursos predeterminado de la cola a otro. Para obtener más información, consulte **Configuración de una cola**.

----Fin

7.6.3.3.6 Borrar configuraciones de cola

Escenario

Puede borrar las configuraciones de una cola en FusionInsight MRS Manager cuando la cola no necesita recursos de un grupo de recursos o el grupo de recursos necesita estar desasociado de la cola. Al borrar las configuraciones de colas, se cancela la política de capacidad de recursos de la cola en el grupo de recursos.

Prerrequisitos

Ha cambiado el grupo de recursos predeterminado de la cola a otro. Si se va a disociar una cola de un grupo de recursos, este grupo de recursos no puede servir como grupo de recursos predeterminado de la cola. Para obtener más información, consulte **Configuración de una cola**.

Procedimiento

Paso 1 Inicie sesión en FusionInsight Manager.

Paso 2 Elija **Tenant Resources** > **Dynamic Resource Plan**.

Paso 3 Seleccione el nombre del clúster de destino en **Cluster** y seleccione un grupo de recursos en **Resource Pool**.

Paso 4 Busque la fila que contiene el nombre del recurso de destino en el área **Resource Allocation** y haga clic en **Clear** en la columna **Operation**.

Paso 5 En el cuadro de diálogo mostrado, haga clic en **OK** para borrar las configuraciones de cola del grupo de recursos actual.

----Fin

7.6.4 Cambio del programador

Escenario

El clúster de recién instalado utiliza el programador Superior de forma predeterminada. Si el clúster se actualiza desde una versión anterior, puede cambiar el programador YARN del programador de Capacity al programador Superior con unos pocos clics.

Prerrequisitos

- La conectividad de red del clúster es adecuada y segura, y el estado del servicio YARN es normal.
- Durante la conmutación del programador, los tenants no se pueden agregar, eliminar o modificar. Además, los servicios no se pueden iniciar o detener.

Impacto en el sistema

- Debido a que el ResourceManager se reinicia durante la conmutación del programador, el envío de trabajos a YARN fallará en ese momento.
- Durante la conmutación del programador, las tareas de un trabajo que se está ejecutando en YARN continuarán, pero no se pueden iniciar nuevas tareas.
- Una vez completada la conmutación del programador, los trabajos ejecutados en YARN pueden fallar, causando interrupciones del servicio.
- Una vez completada la conmutación del programador, se utilizan parámetros del programador Superior para la gestión de tenant.
- Una vez completada la conmutación del programador, las colas de tenant cuya capacidad es 0 en el programador de Capacity no se pueden asignar recursos en el programador Superior. Como resultado, los trabajos enviados a estas colas de tenant no se pueden ejecutar. Por lo tanto, se recomienda no establecer la capacidad de una cola de tenant en 0 en el programador de Capacity.
- Una vez completada la conmutación del programador, no se pueden agregar o eliminar grupos de recursos, etiquetas de nodo YARN ni tenants durante el período de observación. Si se realiza una operación de este tipo, el programador no se puede revertir al progrmador de Capacity.

NOTA

- El período de observación recomendado para el cambio del programador es de una semana. Si durante este período se agregan o eliminan grupos de recursos, etiquetas de nodo YARN o tenants, el período de observación finaliza inmediatamente.

- La reversión del programador puede provocar la pérdida de información parcial o total del trabajo YARN.

Cambio del programador de Capacity al programador Superior

Paso 1 Modifique los parámetros del servicio YARN y asegúrese de que el estado del servicio YARN sea normal.

1. Inicie sesión en FusionInsight Manager como administrador.
2. Inicie sesión en FusionInsight Manager y elija **Cluster** > **Services** > **Yarn**. Haga clic en **Configurations**, luego en **All Configurations**, busque **yarn.resourcemanager.webapp.pagination.enable** y compruebe si el valor es **true**.
   - En caso afirmativo, vaya a **Paso 1.3**.
   - Si no, establezca el parámetro en **true** y haga clic en **Save** para guardar la configuración. En la página de pestaña **Dashboard** de YARN, elija **More** > **Restart Service** verifique la identidad y haga clic en **OK**. Una vez reiniciado el servicio, vaya a **Paso 1.3**.
3. Seleccione **Cluster** > *Name of the desired cluster* > **Services**, y compruebe si el estado del servicio YARN es normal.

Paso 2 Inicie sesión en el nodo de gestión activo como usuario **omm**.

Paso 3 Cambie el programador.

Los siguientes modos de conmutación están disponibles:

0: convierte las configuraciones del programador de Capacity en las configuraciones del programador Superior y, a continuación, cambia el programador de Capacity al programador Superior.

1: convierte las configuraciones del programador de Capacity en las configuraciones del programador de Superior solamente.

2: cambia el programador de Capacity al programador de Superior solamente.

- Se recomienda el modo **0** si el entorno de clúster es simple y el número de tenants es inferior a 20.

  Ejecute el siguiente comando:

  sh ${BIGDATA_HOME}/om-server/om/sbin/switchScheduler.sh -c *Cluster ID* **-m 0**

  NOTA

  Puede elegir **Cluster**, hacer clic en el nombre del clúster y elegir **Cluster Properties** en FusionInsight Manager para ver el ID del clúster.

  ```
  Start to convert Capacity scheduler to Superior Scheduler, clusterId=1
  Start to convert Capacity scheduler configurations to Superior. Please wait...
  Convert configurations successfully.
  Start to switch the Yarn scheduler to Superior. Please wait...
  Switch the Yarn scheduler to Superior successfully.
  ```

- Si el entorno del clúster o la información del tenant es compleja y necesita conservar las configuraciones de cola del programador de Capacity en el programador de Superior, se

recomienda que utilice el modo **1** primero para convertir las configuraciones del programador de Capacity, verifique las configuraciones convertidas, y luego utilice el modo **2** para cambiar el programador de Capacity al programador de Superior.

a. Ejecute el siguiente comando para convertir las configuraciones del programador de Capacity en las configuraciones del programador de Superior:

sh ${BIGDATA_HOME}/om-server/om/sbin/switchScheduler.sh -c *Cluster ID* **-m 1**

```
Start to convert Capacity scheduler to Superior Scheduler, clusterId=1
Start to convert Capacity scheduler configurations to Superior. Please
wait...
Convert configurations successfully.
```

b. Ejecute el siguiente comando para cambiar el programador de Capacity al programador de Superior:

sh ${BIGDATA_HOME}/om-server/om/sbin/switchScheduler.sh -c *Cluster ID* **-m 2**

```
Start to convert Capacity scheduler to Superior Scheduler, clusterId=1
Start to switch the Yarn scheduler to Superior. Please wait...
Switch the Yarn scheduler to Superior successfully.
```

- Si no necesita conservar las configuraciones de cola del programador de Capacity, use modo **2**.

  a. Inicie sesión en FusionInsight Manager y elimine todos los tenants excepto el tenant predeterminado.

  b. En FusionInsight Manager, elimine todos los grupos de recursos excepto el grupo de recursos predeterminado.

  Ejecute el siguiente comando para cambiar el programador de Capacity al programador de Superior:

  sh ${BIGDATA_HOME}/om-server/om/sbin/switchScheduler.sh -c *Cluster ID* **-m 2**

```
Start to convert Capacity scheduler to Superior Scheduler, clusterId=1
Start to switch the Yarn scheduler to Superior. Please wait...
Switch the Yarn scheduler to Superior successfully.
```

NOTA

Puede consultar los registros de conmutación del programador en el nodo de gestión activo.

- ${BIGDATA_LOG_HOME}/controller/aos/switch_scheduler.log
- ${BIGDATA_LOG_HOME}/controller/aos/aos.log

----Fin

Operaciones de reversión

Puede cambiar manualmente el programador de Superior de nuevo al programador de Capacity. Sin embargo, esta operación es solo una solución alternativa y no está permitida en la mayoría de los casos.

Si el cliente tiene requisitos especiales para volver al programador de Capacity, deben cumplirse las siguientes condiciones:

- El período de observación no ha expirado.
- Durante el período de observación no se agrega ni se elimina ningún grupo de recursos, etiqueta de nodo YARN o tenant.

AVISO

Si se agregan o eliminan grupos de recursos, etiquetas de nodo YARN o tenants, es posible que no existan grupos de recursos o colas después de que el programador Superior se cambie de nuevo al programador de Capacity. Como resultado, el programador de Capacity no puede ejecutarse correctamente.

El procedimiento es el siguiente:

Paso 1 Cambie el programador al programador de Capacity e inicie YARN.

1. Inicie sesión en FusionInsight Manager.
2. Vaya a la página **Configurations** de YARN y modifique los parámetros listados en **Tabla 7-42**.

   Tabla 7-42 Modificación de elementos de configuración de YARN

Parámetro	Descripción
yarn.resourcemanager.scheduler.class	org.apache.hadoop.yarn.server.resourcemanager.scheduler.capacity.CapacityScheduler
yarn.http.rmwebapp.external.classes	Dejado vacío
hadoop.http.rmwebapp.scheduler.page.classes	Dejado vacío
yarn.resourcemanager.webapp.pagination.enable	falso

3. Haga clic en **Save** y, a continuación, haga clic en **OK** en el cuadro de diálogo mostrado.
4. Reinicie el servicio YARN, ingrese la contraseña y haga clic en **OK**.

Paso 2 Inicie sesión en el nodo de gestión activo y reinicie el servicio AOS.

1. Inicie sesión en el servidor OMS activo como usuario **omm** mediante PuTTY.
2. Ejecute el siguiente comando para deshabilitar el cierre de sesión al finalizar el tiempo de espera:

   TMOUT=0

   NOTA

   Una vez completadas las operaciones de esta sección, ejecute el comando **TMOUT=***Timeout interval* para restaurar el intervalo de tiempo de espera de manera oportuna. Por ejemplo, **TMOUT=600** indica que un usuario ha cerrado sesión si el usuario no realiza ninguna operación en 600 segundos.
3. Ejecute el siguiente comando para reiniciar el servicio AOS:

   ${BIGDATA_HOME}/om-server/om/sbin/aos_cmd.sh restart

----Fin

7.7 Sistema

7.7.1 Configuración de permisos

7.7.1.1 Gestión de usuarios

7.7.1.1.1 Creación de un usuario

Escenario

FusionInsight Manager admite un máximo de usuarios de 50,000 (incluidos los usuarios integrados). De forma predeterminada, solo el usuario **admin** tiene los permisos de operación más altos del FusionInsight Manager. Debe crear usuarios en el FusionInsight Manager y asignar permisos de operación a los usuarios en función de los requisitos de servicio.

Procedimiento

Paso 1 Inicie sesión en FusionInsight Manager.

Paso 2 Elija **System** >**Permission** >**User**.

Paso 3 En la página **User**, haga clic en **Create**.

Paso 4 Ajusta a **Username**. El nombre de usuario puede contener dígitos, letras, guiones bajos (_), guiones (-) y espacios. Es insensible a mayúsculas y minúsculas y no puede ser el mismo que cualquier nombre de usuario existente en el sistema o el sistema operativo.

Paso 5 Establezca **User Type** en **Human-Machine** o **Machine-Machine**.

- Usuario de **Human-Machine**: utilizado para FusionInsight Manager O&M y las operaciones del cliente de componentes. Si selecciona esta opción, también necesita seleccionar la política de contraseñas y establecer **Password** y **Confirm Password**.
- Usuario de **Machine-Machine**: utilizado para el desarrollo de aplicaciones de componentes. Si selecciona esta opción, la contraseña se genera aleatoriamente.

Paso 6 En el área **User Group**, haga clic en **Add** para agregar uno o más grupos de usuarios a la lista.

NOTA

- Si el grupo de usuarios seleccionado está enlazado a un rol o se ha configurado una política de permisos en Ranger, el usuario puede obtener los permisos correspondientes.
- Después de instalar el FusionInsight Manager, algunos grupos de usuarios generados por defecto tienen permisos especiales. Seleccione los grupos de usuarios deseados en función de las descripciones de la interfaz de usuario.
- Si los grupos de usuarios existentes no pueden cumplir sus requisitos, haga clic en **Create User Group** para crear un grupo de usuarios. Para obtener más información, consulte **Crear un grupo de usuarios**.

Paso 7 Seleccione un grupo de la lista desplegable **Primary Group** para crear directorios y archivos.

La lista desplegable contiene todos los grupos seleccionados en **User Group**.

NOTA

Un usuario puede pertenecer a varios grupos (incluidos el grupo primario y los grupos secundarios). El grupo principal está configurado para facilitar el mantenimiento y cumplir con el mecanismo de permisos de la comunidad Hadoop. El grupo principal tiene la misma funcionalidad de control de permisos que otros grupos.

Paso 8 En el área **Role**, haga clic en **Add** para enlazar roles al usuario.

NOTA

- Al agregar un rol al crear un usuario se pueden especificar los permisos de usuario.
- Si los permisos concedidos al usuario desde el grupo de usuarios no pueden cumplir con los requisitos de servicio, puede vincular otros roles creados al usuario. También puede hacer clic en **Create Role** para crear un rol primero. Para obtener más información, consulte **Creación de un rol**.

  Se tarda 3 minutos en hacer que la asignación de permisos de rol al usuario surta efecto. Si los permisos obtenidos del grupo de usuarios son suficientes, no es necesario agregar un rol.
- Después de habilitar la autenticación de Ranger para un componente, debe configurar las políticas de Ranger para asignar permisos al usuario, excepto los permisos del grupo o rol de usuarios predeterminados.
- Si no se agrega un usuario a un grupo de usuarios ni se le asigna un rol, el usuario no puede ver información ni realizar operaciones después de iniciar sesión en FusionInsight Manager.

Paso 9 Introduce la información en **Description**.

Paso 10 Haga clic en **OK**.

Después de crear un usuario humano-máquina, debe cambiar la contraseña inicial como se le indique después de iniciar sesión en FusionInsight Manager.

----Fin

7.7.1.1.2 Modificación de la información de usuario

Escenario

Puede modificar la información del usuario en FusionInsight Manager, incluido el grupo de usuarios, el grupo principal, la asignación de permisos de rol y la descripción del usuario.

Procedimiento

Paso 1 Inicie sesión en FusionInsight Manager.

Paso 2 Elija **System** >**Permission** >**User**.

Paso 3 Busque la fila que contiene el usuario de destino y haga clic en **Modify** en la columna **Operation**.

Modifique los parámetros según los requisitos de servicio.

NOTA

Se tarda tres minutos como máximo para que el cambio del grupo de usuarios o los permisos de rol surtan efecto.

MRS 3.1.2 o posterior:

- Los usuarios (excepto **admin**) no pueden modificar sus propias políticas de contraseñas.
- Los usuarios bloqueados no pueden modificar sus políticas de contraseñas.
- Una vez modificada la política de contraseñas vinculada a un usuario, la modificación surte efecto cuando el usuario cambie la contraseña la próxima vez.
- Después de modificar la política de contraseña vinculada a un usuario, si el período de validez de contraseña restante es mayor que el período de validez de contraseña en la nueva política de contraseña, el período de validez de contraseña se establece en el período de validez en la nueva política de contraseña. Si el período de validez de contraseña restante es menor que el período de validez de contraseña en la nueva política de contraseña, el período de validez de contraseña permanece sin cambios.

Paso 4 Haga clic en **OK**.

----Fin

7.7.1.1.3 Exportación de información de usuario

Escenario

Puede exportar información sobre todos los usuarios creados en FusionInsight Manager.

Procedimiento

Paso 1 Inicie sesión en FusionInsight Manager.

Paso 2 Elija **System** >**Permission** >**User**.

Paso 3 Haga clic en **Export All** para exportar toda la información de usuario a la vez.

La información de usuario exportada contiene el nombre de usuario, la hora de creación, la descripción, el tipo de usuario (El **0** indica una cuenta hombre-máquina, el **1** indica una cuenta máquina-máquina) grupo principal, lista de grupos de usuarios y roles enlazados al usuario.

Paso 4 Establezca **Save AS** en **TXT** o **CSV**. Haga clic en **OK**.

----Fin

7.7.1.1.4 Bloqueo de un usuario

Escenario

Un usuario puede ser suspendido por un largo período de tiempo debido a cambios en el servicio. Por motivos de seguridad, puede bloquear a dicho usuario.

Puede bloquear a un usuario utilizando cualquiera de los métodos siguientes:

- Bloqueo automático: Puede configurar **Password Retries** en la política de contraseñas para bloquear automáticamente al usuario cuyos intentos de inicio de sesión excedan este valor de parámetro. Para obtener más información, consulte **Configuración de políticas de contraseñas**.

- Bloqueo manual: Usted bloquea manualmente a un usuario.

En esta sección se describe cómo bloquear manualmente a un usuario. Los usuarios de máquina-máquina no se pueden bloquear.

Impacto en el sistema

Un usuario bloqueado no puede iniciar sesión en FusionInsight Manager ni realizar la autenticación de identidad en el clúster. Un usuario bloqueado solo puede ser utilizado después de ser desbloqueado manualmente o el tiempo de bloqueo expira.

Procedimiento

Paso 1 Inicie sesión en FusionInsight Manager.

Paso 2 Elija **System** >**Permission** >**User**.

Paso 3 Busque la fila que contiene el usuario de destino y haga clic en **Lock** en la columna **Operation**.

Paso 4 En la ventana que se muestra, seleccione **I have read the information and understand the impact**. Haga clic en **OK**.

----Fin

7.7.1.1.5 Desbloquear un usuario

Escenario

Puede desbloquear un usuario en FusionInsight Manager si el usuario ha sido bloqueado porque el número de intentos de inicio de sesión excede el umbral. Solo se pueden desbloquear los usuarios creados en FusionInsight Manager.

Procedimiento

Paso 1 Inicie sesión en FusionInsight Manager.

Paso 2 Elija **System** >**Permission** >**User**.

Paso 3 Busque la fila que contiene el usuario de destino y haga clic en **Unlock** en la columna **Operation**.

Paso 4 En la ventana que se muestra, seleccione **I have read the information and understand the impact**. Haga clic en **OK**.

----Fin

7.7.1.1.6 Eliminación de usuarios

Escenario

En función de los requisitos de servicio, puede eliminar usuarios del sistema que ya no se utilizan en FusionInsight Manager.

NOTA

- Después de eliminar un usuario, el vale de concesión de vales (TGT) aprovisionados sigue siendo válido dentro de las 24 horas. El usuario puede utilizar el TGT para la autenticación de seguridad y acceder al sistema.
- Si un nuevo usuario tiene el mismo nombre que el usuario eliminado, el nuevo usuario heredará todos los permisos de propietario del usuario eliminado. Se recomienda que determine si desea eliminar los recursos propiedad del usuario eliminado en función de los requisitos de servicio, por ejemplo, archivos de HDFS.
- No se puede eliminar el usuario **admin** predeterminado.

Procedimiento

Paso 1 Inicie sesión en FusionInsight Manager.

Paso 2 Elija **System** >**Permission** >**User**.

Paso 3 Busque la fila que contiene el usuario de destino, haga clic en **More** y seleccione **Delete**.

NOTA

Para eliminar usuarios en lotes, seleccione los usuarios a la vez y haga clic en **Delete**.

Paso 4 En el cuadro de diálogo que se muestra, haga clic en **OK**.

----Fin

7.7.1.1.7 Modificación de contraseña de un usuario

Escenario

Por motivos de seguridad, la contraseña de un usuario humano-máquina debe cambiarse periódicamente.

Si los usuarios tienen permiso para usar FusionInsight Manager, pueden cambiar sus contraseñas en FusionInsight Manager.

Si los usuarios no tienen permiso para usar FusionInsight Manager, pueden cambiar sus contraseñas en el cliente.

Prerrequisitos

- Ha obtenido la política de contraseñas actual.
- El usuario ha instalado el cliente en cualquier nodo del clúster y ha obtenido la dirección IP del nodo. La contraseña del usuario de instalación del cliente se puede obtener del administrador.

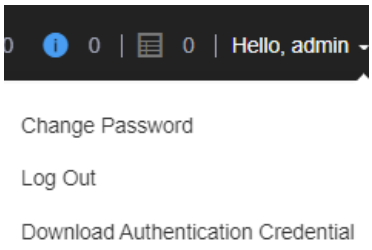
Cambiar la contraseña en FusionInsight Manager

Paso 1 Inicie sesión en FusionInsight Manager.

Paso 2 Mueva el cursor al nombre de usuario en la esquina superior derecha de la página.

En el menú desplegable de la cuenta de usuario, seleccione **Change Password**.

Figura 7-49 Cambio de contraseña



Paso 3 En la página que se muestra, establezca **Current Password**, **New Password** y **Confirm Password** y haga clic en **OK**.

La contraseña debe cumplir los siguientes requisitos de complejidad:

- Contiene al menos 8 caracteres.
- Contiene al menos cuatro tipos de los siguientes: letras mayúsculas, minúsculas, números, espacios y caracteres especiales (`~!@#$%^&*()-_=+|[{}];',<.>/\?).
- No puede ser el mismo que el nombre de usuario o el nombre de usuario escrito al revés.
- No puede ser una contraseña común fácil de descifrar.
- No puede ser la misma que la contraseña utilizada en los últimos *N* veces. *N* indica el valor de **Repetition Rule** configurada en **Configuración de políticas de contraseñas**.

----Fin

Cambio de la contraseña en el cliente

Paso 1 Inicie sesión en el nodo donde está instalado el cliente como el usuario de instalación del cliente.

Paso 2 Ejecute el siguiente comando para cambiar al directorio del cliente, por ejemplo **/opt/client**:

cd /opt/client

Paso 3 Ejecute el siguiente comando para configurar las variables de entorno:

source bigdata_env

Paso 4 Cambie la contraseña de usuario. Esta operación tiene efecto para todos los servidores.

kpasswd *System username*

Por ejemplo, si desea cambiar la contraseña del usuario de sistema **test1**, ejecute el comando **kpasswd test1**.

La contraseña debe cumplir los siguientes requisitos de complejidad:

- Contiene al menos 8 caracteres.
- Contiene al menos cuatro tipos de los siguientes: letras mayúsculas, minúsculas, números, espacios y caracteres especiales (`~!@#$%^&*()-_=+|[{}];',<.>/\?).
- No puede ser el mismo que el nombre de usuario o el nombre de usuario escrito al revés.
- No puede ser una contraseña común fácil de descifrar.
- No puede ser la misma que la contraseña utilizada en los últimos *N* veces. *N* indica el valor de **Repetition Rule** configurada en **Configuración de políticas de contraseñas**.

NOTA

Si se produce un error durante la ejecución del comando **kpasswd**, pruebe las siguientes operaciones:

- Detenga la sesión SSH y vuelva a iniciarla.
- Ejecute el comando **kdestroy** y, a continuación, vuelva a ejecutar el comando **kpasswd**.

----Fin

7.7.1.1.8 Inicializar una contraseña

Escenario

Si un usuario olvida la contraseña o la contraseña de la cuenta pública necesita cambiarse periódicamente, puede inicializar la contraseña en FusionInsight Manager. Después de que se inicialice la contraseña, el usuario del sistema debe cambiar la contraseña en el primer inicio de sesión.

NOTA

Esta operación solo se aplica a usuarios hombre-máquina.

Procedimiento

Paso 1 Inicie sesión en FusionInsight Manager.

Paso 2 Elija **System** >**Permission** >**User**.

Paso 3 Busque la fila que contiene el usuario de destino, haga clic en **More** y seleccione **Initialize Password**. En el cuadro de diálogo que se muestra, introduzca la contraseña del usuario de inicio de sesión actual y haga clic en **OK**. En el cuadro de diálogo **Initialize Password**, haga clic en **OK**.

Paso 4 Establezca **New Password** y **Confirm Password** y haga clic en **OK**.

La contraseña debe cumplir los siguientes requisitos de complejidad:

- Contiene al menos 8 caracteres.
- Contiene al menos cuatro tipos de los siguientes: letras mayúsculas, minúsculas, números, espacios y caracteres especiales (`~!@#$%^&*()-_=+|[{}];',<.>/\?).
- No puede ser el mismo que el nombre de usuario o el nombre de usuario escrito al revés.
- No puede ser una contraseña común fácil de descifrar.
- No puede ser la misma que la contraseña utilizada en los últimos tiempos de *N*. *N* indica el valor de **Repetition Rule** configurada en **Configuración de políticas de contraseñas**.

----Fin

7.7.1.1.9 Exportación de un archivo de credenciales de autenticación

Escenario

Si un usuario utiliza un clúster de modo de seguridad para desarrollar aplicaciones, es necesario obtener el archivo keytab del usuario para la autenticación de seguridad. Puede exportar archivos keytab en FusionInsight Manager.

NOTA

Después de cambiar una contraseña de usuario, el archivo keytab exportado no es válido y debe exportar un archivo keytab de nuevo.

Prerrequisitos

Antes de descargar el archivo keytab de un usuario humano-máquina, la contraseña del usuario debe cambiarse al menos una vez en el portal de Manager o en un cliente; de lo contrario, no se puede usar el archivo keytab descargado. Para obtener más información, consulte **Modificación de contraseña de un usuario**.

Procedimiento

Paso 1 Inicie sesión en FusionInsight Manager.

Paso 2 Elija **System** >**Permission** >**User**.

Paso 3 Busque la fila que contiene el usuario cuyo archivo keytab debe exportarse, elija **More** > **Download Authentication Credential** y especifique la ruta de guardado después de que el archivo se genere automáticamente y mantenga el archivo correctamente.

La credencial de autenticación incluye el archivo **krb5.conf** del servicio Kerberos.

Después de descomprimir el archivo de credenciales de autenticación, puede obtener los dos archivos siguientes:

- El archivo **krb5.conf** contiene la información de conexión del servicio de autenticación.
- El archivo **user.keytab** contiene información de autenticación del usuario.

----Fin

7.7.1.2 Gestión de grupos de usuarios

Escenario

FusionInsight Manager admite un máximo de 5000 grupos de usuarios (incluidos los grupos de usuarios integrados). Puede crear y gestionar diferentes grupos de usuarios en función de los escenarios de servicio en FusionInsight Manager. Un grupo de usuarios está enlazado a un rol para obtener permisos de operación. Después de agregar un usuario a un grupo de usuarios, el usuario puede obtener los permisos de operación del grupo de usuarios. Un grupo de usuarios se puede utilizar para clasificar usuarios y gestionar varios usuarios.

Prerrequisitos

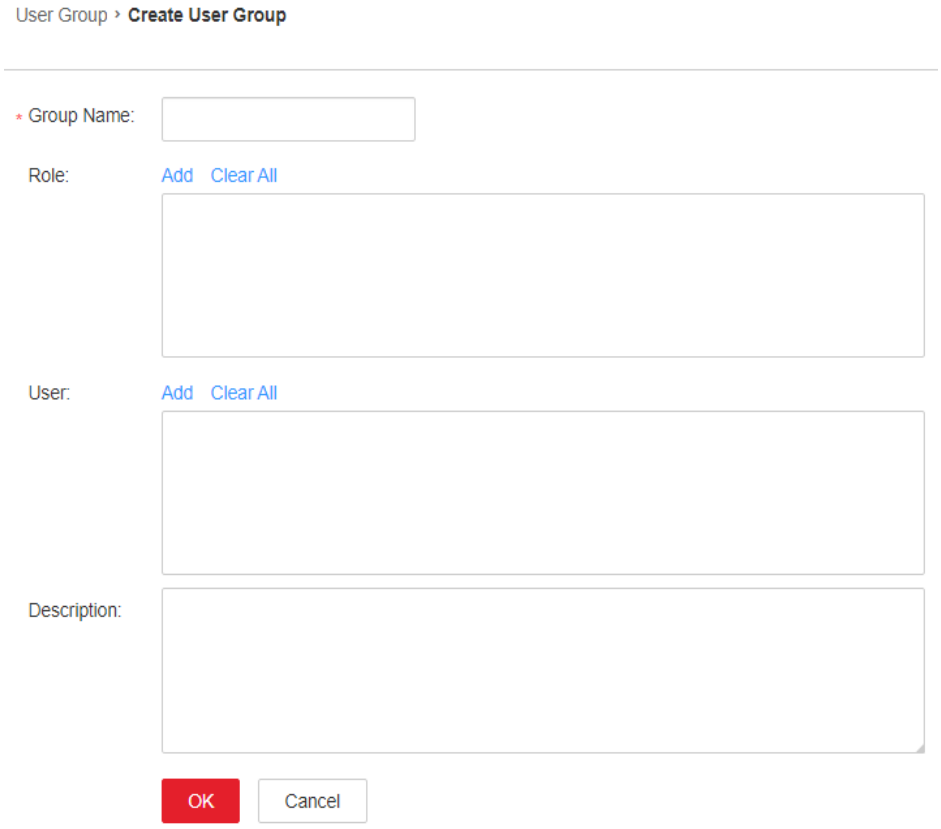
- Ha aprendido los requisitos de servicio y ha creado los roles requeridos por los escenarios de servicio.
- Ha iniciado sesión en FusionInsight Manager.

Crear un grupo de usuarios

Paso 1 Elija **System** >**Permission** >**User Group**.

Paso 2 Encima de la lista de grupos de usuarios, haga clic en **Create User Group**.

Figura 7-50 Crear un grupo de usuarios



Paso 3 Establecer **Group Name** y **Description**.

El nombre del grupo contiene de 1 a 64 caracteres, incluidos letras que no distinguen entre mayúsculas y minúsculas, dígitos, guiones bajos (_), guiones (-) y espacios. No puede ser lo mismo que un nombre de grupo de usuarios existente en el sistema.

Paso 4 En el área **Role**, haga clic en **Add** para seleccionar un rol y agregarlo.

NOTA

- Para los componentes (excepto HDFS y Yarn) para los que se ha habilitado la autorización de Ranger, los permisos de los roles no predeterminados en Manager no tienen efecto. Es necesario configurar las políticas de Ranger para asignar permisos a los grupos de usuarios.
- Si las solicitudes de recursos de HDFS y Yarn están más allá de las políticas de Ranger, las reglas de ACL de los componentes todavía tienen efecto.

Paso 5 En el área **User**, haga clic en **Add** para seleccionar un usuario y agregarlo.

Paso 6 Haga clic en **OK**.

Se crea el grupo de usuarios.

----Fin

Consulta de la información del grupo de usuarios

De forma predeterminada, todos los grupos de usuarios se muestran en la lista de grupos de usuarios. Puede hacer clic en la flecha situada a la izquierda del nombre de un grupo de usuarios para ver detalles sobre el grupo de usuarios, incluida la cantidad de usuarios, los usuarios específicos y las funciones enlazadas del grupo de usuarios.

Modificación de información acerca de un grupo de usuarios

Busque la fila que contiene el grupo de usuarios de destino y haga clic en **Modify** para modificar su información.

Exportación de información acerca de un grupo de usuarios

Haga clic en **Export All** para exportar toda la información de grupo de usuarios a la vez en formato **TXT** o **CSV**.

La información del grupo de usuarios exportado contiene el nombre del grupo de usuarios, la descripción, la lista de usuarios y la lista de roles.

Eliminación de un grupo de usuarios

Busque la fila que contiene el grupo de usuarios de destino y haga clic en **Delete**. Para eliminar varios grupos de usuarios en lotes, seleccione los grupos de usuarios de destino y haga clic en **Delete** encima de la lista de grupos de usuarios. No se puede eliminar un grupo de usuarios que contenga usuarios. Para eliminar un grupo de usuarios de este tipo, elimine todos sus usuarios modificando primero el grupo de usuarios.

7.7.1.3 Gestión de roles

Escenario

FusionInsight Manager admite un máximo de 5000 roles (incluidos los roles integrados en el sistema pero excluidos los roles creados automáticamente por tenants). En función de los diferentes requisitos de servicio, debe crear y gestionar diferentes roles en el FusionInsight Manager y realizar la gestión de autorizaciones para FusionInsight Manager y los componentes mediante roles.

Prerrequisitos

- Ha aprendido los requisitos de servicio.
- Ha iniciado sesión en FusionInsight Manager.

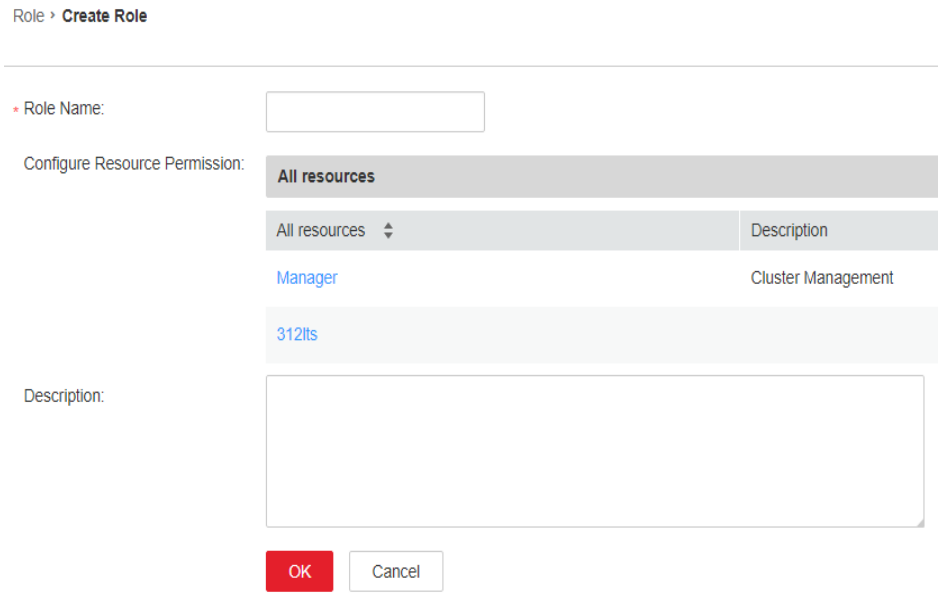
Creación de un rol

Paso 1 Elija **System** >**Permission** >**Role**.

Paso 2 En la página mostrada, haga clic en **Create Role** y complete **Role Name** y **Description**.

El nombre del rol consta de 3 a 50 caracteres, incluidos dígitos, letras y guiones bajos (_). No puede ser lo mismo que un nombre de rol existente en el sistema. El nombre del rol no puede comenzar por **Manager**, **System** ni **default**. Por ejemplo, el nombre del rol no puede ser **Manager_test**.

Figura 7-51 Creación de un rol



Paso 3 En el área **Configure Resource Permission**, haga clic en el clúster cuyos permisos se van a agregar y seleccione los permisos de servicio para el rol.

Al establecer permisos para un componente, escriba un nombre de recurso en el cuadro de texto de búsqueda en la esquina superior derecha y haga clic en el icono de búsqueda para ver el resultado de la búsqueda.

El resultado de la búsqueda solo contiene directorios, pero no subdirectorios. La búsqueda por palabra clave admite coincidencia difusa y no distingue entre mayúsculas y minúsculas.

NOTA

- Para los componentes (excepto HDFS y Yarn) para los que se ha habilitado la autorización de Ranger, los permisos de los roles no predeterminados en Manager no tienen efecto. Es necesario configurar las políticas de Ranger para asignar permisos a los grupos de usuarios.
- Si las solicitudes de recursos de HDFS y Yarn están más allá de las políticas de Ranger, las reglas de ACL de los componentes todavía tienen efecto.
- Se puede establecer un máximo de 1000 permisos para un componente a la vez.

Paso 4 Haga clic en **OK**.

----Fin

Modificación de información de rol

Busque la fila que contiene el rol de destino y haga clic en **Modify**.

Exportación de información de rol

Haga clic en **Export All** para exportar toda la información de rol a la vez en formato **TXT** o **CSV**.

La información del rol exportado contiene el nombre del rol, la descripción y si el rol es el rol predeterminado.

Eliminación de un rol

Busque la fila que contiene el rol de destino y haga clic en **Delete**. Para eliminar varios roles en lotes, seleccione los roles de destino y haga clic en **Delete** encima de la lista de roles. No se puede eliminar un rol enlazado a un usuario. Para eliminar dicho rol, disocie el rol del usuario modificando primero al usuario.

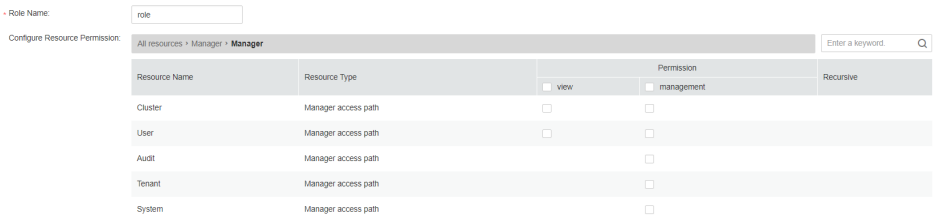
Ejemplo de tarea (Creación de un rol de Manager)

Paso 1 Elija **System** >**Permission** >**Role**.

Paso 2 En la página mostrada, haga clic en **Create Role** y complete **Role Name** y **Description**.

Paso 3 En el área **Configure Resource Permission**, haga clic en **Manager** y establezca permisos para el rol.

Figura 7-52 Configuración de permisos



Permisos de Manager:

- Cluster
  - Permiso de **view**: permiso para ver información en la página **Cluster** y ver alarmas y eventos en **O&M** > **Alarm**.
  - Permiso de **management**: permiso para la gestión en las páginas **Cluster** y **O&M**.
- User
  - Permiso de **view**: permiso para ver información en páginas bajo **System** > **Permission**.
  - Permiso de **management**: permiso para la gestión de páginas bajo **System** > **Permission**.
- Audit

  Permiso de **management**: permiso para la gestión en la página **Audit**.
- Tenant

  permiso de **management**: permiso para la gestión en la página **Tenant** y permiso para ver alarmas y eventos en **O&M** > **Alarm**.
- System

  permiso de **management**: permiso para gestión en todas las páginas excepto en las que se encuentran bajo **Permission** en la página **System** y permiso para ver alarmas y eventos bajo **O&M** > **Alarm**.

Paso 4 Haga clic en **OK**.

----Fin

7.7.1.4 Políticas de seguridad

7.7.1.4.1 Configuración de políticas de contraseñas

Escenario

Para mantenerse al día con los requisitos de seguridad del servicio, puede establecer reglas de seguridad de contraseñas, reglas de seguridad de inicio de sesión de usuario y reglas de bloqueo de usuario en FusionInsight Manager.

AVISO

- Modifique las políticas de contraseñas en función de los requisitos de seguridad del servicio, ya que implican la seguridad de gestión de usuarios. De lo contrario, se pueden incurrir en riesgos de seguridad.
- Cambie la contraseña de usuario después de modificar la política de contraseñas y, a continuación, la nueva política de contraseñas tendrá efecto.

Modificación de una política de contraseñas (Versiones anteriores a MRS 3.1.2)

Paso 1 Inicie sesión en FusionInsight Manager.

Paso 2 Elija **System** > **Permission** > **Security Policy** > **Password Policy**.

Paso 3 Haga clic en **Modify** en la columna **Operation** y modifique la política de contraseñas según se le indique.

Para obtener más información sobre los parámetros, consulte **Tabla 7-43**.

Figura 7-53 Modificación de una política de contraseñas

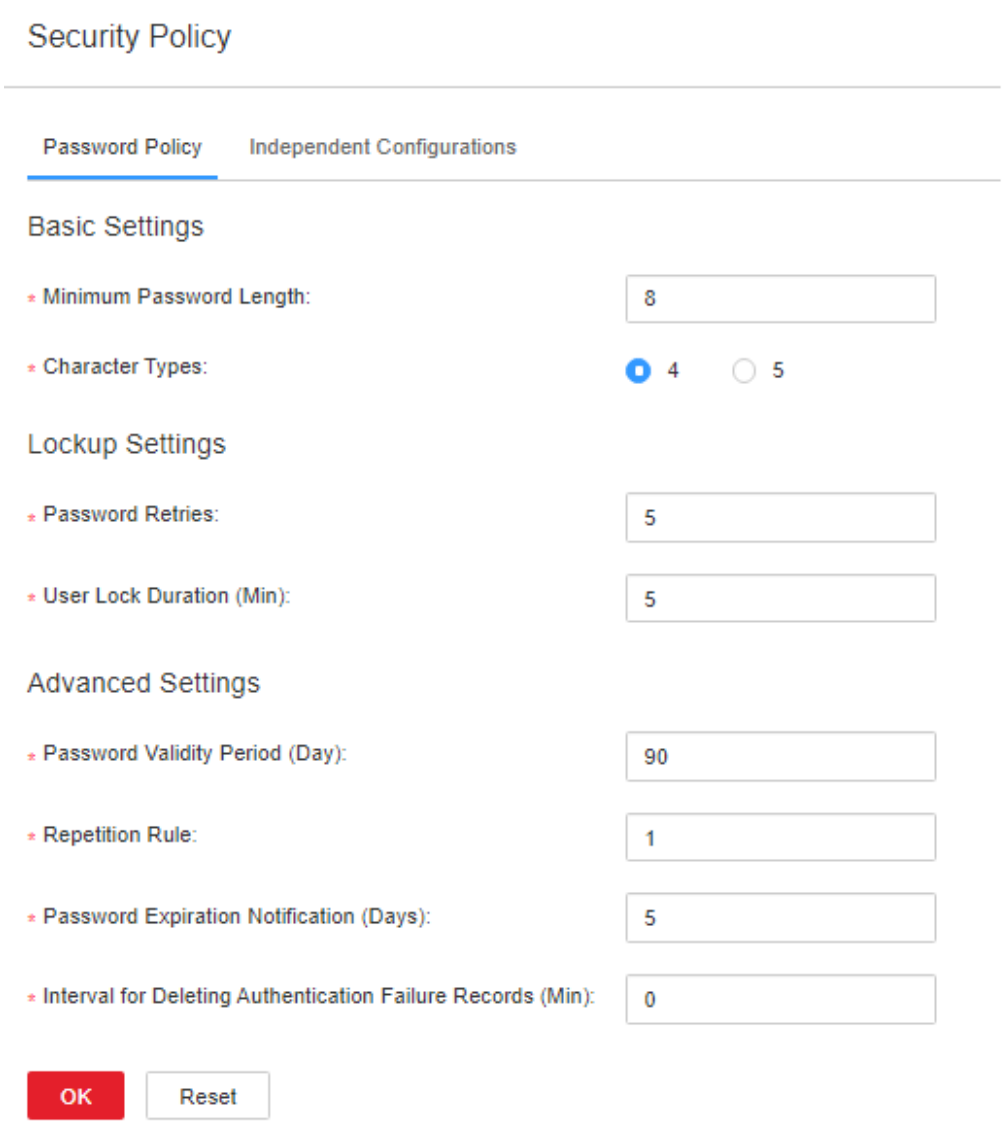


Tabla 7-43 Parámetros de política de contraseñas

Parámetro	Descripción
Minimum Password Length	Indica el número mínimo de caracteres que contiene una contraseña. El valor oscila entre **8** y **32**. El valor predeterminado es **8**.
Character Types	Indica cuántos tipos de caracteres puede contener una contraseña como mínimo: letras mayúsculas, minúsculas, dígitos, espacios y caracteres especiales (~`!?,.:;-_'(){}[]/<>@#$%^&*+|\=). El valor puede ser **4** o **5**. El valor predeterminado es **4**, lo que significa que una contraseña puede contener letras mayúsculas, minúsculas, dígitos y caracteres especiales. Si establece el parámetro en **5**, una contraseña puede contener los cinco tipos de caracteres mencionados anteriormente.

Parámetro	Descripción
Password Retries	Indica el número de intentos de contraseña erróneos consecutivos permitidos antes de que el sistema bloquee al usuario. El valor oscila entre **3** y **30**. El valor predeterminado es de **5**.
User Lock Duration (Min)	Indica el período de tiempo en el que un usuario está bloqueado cuando se cumplen las condiciones de bloqueo del usuario. El valor oscila entre **5** y **120**. El valor predeterminado es de **5**.
Password Validity Period (Day)	Indica el período de validez de una contraseña. El valor oscila entre **0** y **90**. **0** indica que la contraseña es válida de forma permanente. El valor predeterminado es **90**.
Repetition Rule	Indica el número de contraseñas anteriores que no se pueden reutilizar al cambiar la contraseña. El valor oscila entre **1** y **5**. El valor predeterminado es **1**. Esta política se aplica solo a las cuentas hombre-máquina.
Password Expiration Notification (Days)	Indica el número de días de antelación que se notifica a los usuarios que sus contraseñas están a punto de caducar. Después de establecer el valor, si la diferencia entre el tiempo de clúster y el tiempo de caducidad de la contraseña es menor que este valor, el usuario recibe notificaciones de caducidad de la contraseña. Al iniciar sesión en FusionInsight Manager, se notificará al usuario que la contraseña está a punto de caducar y se mostrará un mensaje pidiéndole que cambie la contraseña. El valor varía de **0** a *X* (*X* debe establecerse en la mitad del período de validez de la contraseña y redondearse hacia abajo). El valor **0** indica que no se envía ninguna notificación. El valor predeterminado es de **5**.
Interval for Deleting Authentication Failure Records (Min)	Indica el intervalo de retención de intentos de contraseña incorrectos. El valor oscila entre **0** y **1440**. **0** indica que los intentos de contraseña incorrectos se conservan permanentemente y **1440** indica que los intentos de contraseña incorrectos se conservan durante un día. El valor predeterminado es de **5**.

Paso 4 Haga clic en **OK** para guardar las configuraciones. Cambie la contraseña de usuario después de modificar la política de contraseñas y, a continuación, la nueva política de contraseñas tendrá efecto.

----Fin

Adición de una política de contraseñas (MRS 3.1.2 o posterior)

Paso 1 Inicie sesión en FusionInsight Manager.

Paso 2 Elija **System** > **Permission** > **Security Policy** > **Password Policy**.

Paso 3 Haga clic en **Add Password Policy** y modifique la política de contraseñas como se le solicite.

Para obtener más información sobre los parámetros, consulte **Tabla 7-44**.

Tabla 7-44 Parámetros de política de contraseñas

Parámetro	Descripción
Password Policy Name	El valor es una cadena de 3 a 32 caracteres, incluidos letras insensibles a mayúsculas y minúsculas, dígitos, guiones bajos (_), y guiones (-). No puede comenzar con un guion (-).
Minimum Password Length	Indica el número mínimo de caracteres que contiene una contraseña. El valor oscila entre **8** y **32**.
Character Types	Indica cuántos tipos de caracteres puede contener una contraseña como mínimo: letras mayúsculas, minúsculas, dígitos, espacios y caracteres especiales (~`!?,.:;-_'(){}[]/<>@#$%^&*+|\=). El valor puede ser **4** o **5**. El valor predeterminado es **4**, lo que significa que una contraseña puede contener letras mayúsculas, minúsculas, dígitos y caracteres especiales. Si establece el parámetro en **5**, una contraseña puede contener los cinco tipos de caracteres mencionados anteriormente.
Password Retries	Indica el número de intentos de contraseña erróneos consecutivos permitidos antes de que el sistema bloquee al usuario. El valor oscila entre **3** y **30**.
User Lock Duration (Min)	Indica el período de tiempo en el que un usuario está bloqueado cuando se cumplen las condiciones de bloqueo del usuario. El valor oscila entre **5** y **120**.
Password Validity Period (Day)	Indica el período de validez de una contraseña. El valor oscila entre **0** y **90**. **0** indica que la contraseña es válida de forma permanente.
Repetition Rule	Indica el número de contraseñas anteriores que no se pueden reutilizar al cambiar la contraseña. El valor oscila entre **1** y **5**. El valor predeterminado es **1**. Esta política se aplica solo a las cuentas hombre-máquina.
Password Expiration Notification (Days)	Indica el número de días de antelación que se notifica a los usuarios que sus contraseñas están a punto de caducar. Después de establecer el valor, si la diferencia entre el tiempo de clúster y el tiempo de caducidad de la contraseña es menor que este valor, el usuario recibe notificaciones de caducidad de la contraseña. Al iniciar sesión en FusionInsight Manager, se notificará al usuario que la contraseña está a punto de caducar y se mostrará un mensaje pidiéndole que cambie la contraseña. El valor varía de **0** a *X* (*X* debe establecerse en la mitad del período de validez de la contraseña y redondearse hacia abajo). El valor **0** indica que no se envía ninguna notificación.
Interval for Deleting Authentication Failure Records (Min)	Indica el intervalo de retención de intentos de contraseña incorrectos. El valor oscila entre **0** y **1440**. **0** indica que los intentos de contraseña incorrectos se conservan permanentemente y **1440** indica que los intentos de contraseña incorrectos se conservan durante un día.

Paso 4 Haga clic en **OK** para guardar las configuraciones.

Un usuario nuevo utiliza la política de contraseñas predeterminada. Después de crear una nueva política de contraseñas, puede seleccionar manualmente la política de contraseñas al crear un usuario. Puede modificar la política de contraseñas de un usuario existente. Para obtener más información, consulte **Modificación de la información de usuario**.

----Fin

NOTA

Se puede crear un máximo de 32 políticas de contraseñas.

Modificación de una política de contraseñas (MRS 3.1.2 o posterior)

Paso 1 Inicie sesión en FusionInsight Manager.

Paso 2 Elija **System** > **Permission** > **Security Policy** > **Password Policy**.

Paso 3 Haga clic en **Modify** en la fila que contiene la política de contraseñas de destino. En la página **Modify Password Policy**, modifique la política de contraseñas según se le indique.

Para obtener más información sobre los parámetros, consulte **Tabla 7-44**.

Paso 4 Haga clic en **OK** para guardar las configuraciones.

----Fin

NOTA

- Los usuarios (excepto **admin**) no pueden modificar sus propias políticas de contraseñas.
- Después de modificar la política de contraseña vinculada a un usuario, si el período de validez de contraseña restante es mayor que el período de validez de contraseña en la nueva política de contraseña, el período de validez de contraseña se establece en el período de validez en la nueva política de contraseña. Si el período de validez de contraseña restante es menor que el período de validez de contraseña en la nueva política de contraseña, el período de validez de contraseña permanece sin cambios.

Eliminación de una política de contraseñas (MRS 3.1.2 o posterior)

Paso 1 Inicie sesión en FusionInsight Manager.

Paso 2 Elija **System** > **Permission** > **Security Policy** > **Password Policy**.

Paso 3 Haga clic en **Delete** en la fila que contiene la política de contraseñas de destino. En el cuadro de diálogo que se muestra, haga clic en **OK**.

----Fin

NOTA

La política de contraseñas predeterminada y la política de contraseñas enlazadas a un usuario no se pueden eliminar.

7.7.1.4.2 Configuración del atributo independiente

Escenario

Usuario **admin** o los administradores vinculados al rol Manager_administrator pueden configurar el atributo independiente en FusionInsight Manager para que los usuarios comunes (todos los usuarios de servicio del clúster) puedan establecer o cancelar sus propios atributos independientes.

Después de activar la opción de atributo independiente, los usuarios del servicio deben iniciar sesión en el sistema y establecer el atributo independiente.

Restricciones

- Los administradores no pueden establecer ni cancelar el atributo independiente de un usuario.
- Los administradores no pueden obtener las credenciales de autenticación de usuarios independientes.

Prerrequisitos

Usted ha obtenido el nombre de usuario y contraseña de administrador requeridos.

Procedimiento

Activar o desactivar el atributo independiente

Paso 1 Inicie sesión en FusionInsight Manager como usuario **admin** o un usuario enlazado al rol Manager_administrator.

Paso 2 Seleccione **System** > **Permission** > **Security Policy** > **Independent Configurations**.

Paso 3 Active o desactive **Independent Attribute**, escriba la contraseña según se le solicite y haga clic en **OK**.

Paso 4 Una vez autenticada la identidad, espere hasta que se modifique la configuración de OMS y haga clic en **Finish**.

NOTA

Después de deshabilitar el atributo independiente:

- Un usuario que tiene el atributo puede cancelarlo desde la lista desplegable del nombre de usuario en la esquina superior derecha de la página. El usuario no puede establecer de nuevo el atributo independiente una vez que se cancela. Una vez cancelado el atributo, las tablas independientes existentes conservarán el atributo. Sin embargo, el usuario no puede crear tablas independientes de nuevo.
- Los usuarios sin este atributo no pueden establecer o cancelar el atributo.

Configuración del atributo independiente

Paso 5 Inicie sesión en FusionInsight Manager como usuario del servicio.

AVISO

Los administradores no pueden inicializar la contraseña del usuario después de establecer el atributo independiente. Si se olvida la contraseña de usuario, la contraseña no se puede recuperar.

Usuario **admin** no puede establecer el atributo independiente.

Paso 6 Mueva el cursor al nombre de usuario en la esquina superior derecha de la página.

Paso 7 Seleccione **Set Independent** o **Cancel Independent**.

NOTA

- Si el atributo independiente está activado y se ha establecido para el usuario del servicio, se muestra **Cancel Independent**.
- Si el atributo independiente está activado pero se ha cancelado para el usuario del servicio, se muestra **Set Independent**.
- Si el atributo independiente está desactivado pero se ha definido para el usuario del servicio, se muestra **Cancel Independent**.
- Si el atributo independiente está desactivado y se ha cancelado para el usuario del servicio, no se muestra ninguna opción relacionada con el atributo independiente.

Paso 8 Ingrese la contraseña como se le solicite y haga clic en **OK**.

Paso 9 Una vez autenticada la identidad, haga clic en **OK** en el cuadro de diálogo.

----Fin

7.7.2 Configuración de internconexiones

7.7.2.1 Configuración de parámetros en dirección norte de SNMP

Escenario

Si los usuarios necesitan ver las alarmas y los datos de monitorización de un clúster en la plataforma O&M, puede utilizar el protocolo simple de gestión de red (SNMP) en el FusionInsight Manager para informar los datos relacionados al sistema de gestión de red (NMS).

Procedimiento

Paso 1 Inicie sesión en FusionInsight Manager.

Paso 2 Elija **System** >**Interconnection** >**SNMP**.

Paso 3 Active **SNMP Service**.

El servicio SNMP está deshabilitado de forma predeterminada.  indica que el servicio está habilitado.

Paso 4 Establezca los parámetros de interconexión según **Tabla 7-45**.

Tabla 7-45 Parámetros de interconexión

Parámetro	Descripción
Version	Especifica la versión de SNMP, que puede ser: ● **V2C**: Esta es una versión anterior con poca seguridad. ● **V3**: Esta es una versión posterior con mayor seguridad que SNMP V2C. Se recomienda SNMP V3.
Local Port	Especifica el puerto local. El valor predeterminado es **20000**. El valor oscila entre **1025** y **65535**.
Read Community Name	Especifica el nombre de la comunidad de sólo lectura. Este parámetro solo está disponible cuando **Version** está establecido en **V2C**.
Write Community Name	Especifica el nombre de la comunidad de escritura. Este parámetro solo está disponible cuando **Version** está establecido en **V2C**.
Security Username	Especifica el nombre de usuario de seguridad SNMP. Este parámetro solo está disponible cuando **Version** está establecido en **V3**.
Authentication Protocol	Especifica el protocolo de autenticación. Este parámetro solo está disponible cuando **Version** está establecido en **V3**. Se recomienda SHA.
Authentication Password	Especifica la contraseña de autenticación. Este parámetro solo está disponible cuando **Version** está establecido en **V3**.
Confirm Password	Se utiliza para confirmar la contraseña de autenticación. Este parámetro solo está disponible cuando **Version** está establecido en **V3**.
Encryption Protocol	Especifica el protocolo de encriptación. Este parámetro solo está disponible cuando **Version** está establecido en **V3**. Se recomienda AES256.
Encryption Password	Especifica la contraseña de encriptación. Este parámetro solo está disponible cuando **Version** está establecido en **V3**.
Confirm Password	Se utiliza para confirmar la contraseña de encriptación. Este parámetro solo está disponible cuando **Version** está establecido en **V3**.

NOTA

- El valor de **Security Username** no puede contener cadenas repetidas con la longitud de unidad como un factor común de 64 (como 1, 2, 4 y 8), por ejemplo, **abab** y **abcdabcd**.
- El **Authentication Password** y el **Encryption Password** deben contener de 8 a 16 caracteres, incluidos al menos tres tipos de los siguientes caracteres: letras mayúsculas, letras minúsculas, dígitos y caracteres especiales. Las dos contraseñas deben ser diferentes. Las dos contraseñas no pueden ser las mismas que el nombre de usuario de seguridad o el reverso del nombre de usuario de seguridad.
- Por motivos de seguridad, cambie periódicamente la contraseña de autenticación y la contraseña de encriptación cuando se utilice el protocolo SNMP.
- Si se utiliza SNMP v3, un usuario de seguridad se bloqueará después de cinco fallas de autenticación consecutivos en 5 minutos. El usuario se desbloqueará automáticamente 5 minutos más tarde.

Paso 5 Haga clic en **Create Trap Target** en el área **Trap Target**. En el cuadro de diálogo que se muestra, establezca los siguientes parámetros:

- **Target Symbol**: especifica el ID de destino de captura, que es el ID del NMS o del host que recibe trap. El valor consta de 1 a 255 caracteres, incluidas letras o dígitos.
- **Target IP Address Mode**: especifica el modo de la dirección IP de destino. El valor puede ser **IPv4** o **IPv6**.
- **Target IP Address**: especifica la dirección IP de destino, que puede comunicarse con la dirección IP del plano de gestión del nodo de gestión.
- **Target Port**: especifica el puerto que recibe trap. El número de puerto debe ser coherente con el extremo del par y oscila entre 0 y 65535.
- **Trap Community Name**: Este parámetro solo está disponible cuando **Version** está establecido en **V2C** y se utiliza para informar el nombre de la comunidad.

Haga clic en **OK**.

El cuadro de diálogo **Create Trap Target** está cerrado.

Paso 6 Haga clic en **OK**.

----Fin

7.7.2.2 Configuración de parámetros de dirección norte de Syslog

Escenario

Si los usuarios necesitan ver las alarmas y eventos de un clúster en la plataforma unificada de informes de alarmas, puede utilizar el protocolo Syslog en FusionInsight Manager para informar datos relacionados a la plataforma de alarmas.

AVISO

Si el protocolo Syslog no está cifrado, los datos pueden ser robados.

Procedimiento

Paso 1 Inicie sesión en FusionInsight Manager.

Paso 2 Elija **System** >**Interconnection** >**Syslog**.

Paso 3 Active **Syslog Service**.

El servicio Syslog está deshabilitado de forma predeterminada. indica que el servicio está habilitado.

Paso 4 Establezca los parámetros en dirección norte según **Tabla 7-46**.

Tabla 7-46 Parámetros de interconexión de Syslog

Área de parámetro	Parámetro	Descripción
Protocolo de Syslog	Server IP Address Mode	Especifica el modo de dirección IP del servidor interconectado. El valor puede ser **IPV4** o **IPV6**.
	Server IP Address	Especifica la dirección IP del servidor interconectado.
	Server Port	Especifica el número de puerto para la interconexión.
	Protocol	Especifica el tipo de protocolo. Las opciones son las siguientes: ● **TCP** ● **UDP**
	Severity Level	Especifica la gravedad del mensaje notificado. Las opciones son las siguientes: ● **Emergency** ● **Alert** ● **Critical** ● **Error** ● **Warning** ● **Notice** ● **Informational** (valor predeterminado) ● **Debug** **NOTA** **Severity Level** y **Facility** determinan la prioridad del mensaje enviado. **Priority** = **Facility** × 8 + **Severity Level** Para obtener más información sobre los valores de **Severity Level** y **Facility**, consulte **Tabla 7-47**.
	Facility	Especifica el módulo donde se genera el registro. Para obtener más información sobre los valores disponibles de este parámetro, consulte **Tabla 7-47**. Se recomienda el valor predeterminado **local use 0 (local0)**.

Área de parámetro	Parámetro	Descripción
	Identifier	Especifica el ID del producto. El valor predeterminado es **FusionInsight Manager**. El identificador puede contener un máximo de 256 caracteres, incluidos letras, dígitos, guiones bajos (_), puntos (.), guiones (-), espacios y el siguiente characters: | $ { }
Mensaje de informe	Report Format	Especifica el formato de mensaje del informe de alarma. Para obtener más información, consulte la información de ayuda en la página. El formato del informe puede contener un máximo de 1024 caracteres, incluidos letras, dígitos, guiones bajos (_), puntos (.), guiones (-), espacios y el siguiente characters: | $ { } **NOTA** Para obtener más información sobre cada campo del formato de informe, consulte **Tabla 7-48**.
	Alarm Type	Especifica el tipo de alarma que se va a notificar.
	Alarm Severities	Especifica el nivel de la alarma que se va a informar.
Informes de alarma no borrados	Periodic Uncleared Alarm Reporting	Especifica si informar alarmas no borradas en un período específico. Puede activar o desactivar la función. La función está desactivada por defecto.
	Report Interval (min)	Especifica el intervalo para informar periódicamente de alarmas no borradas. Este parámetro sólo es válido cuando **Periodic Uncleared Alarm Reporting** está habilitado. El valor predeterminado es **15** en minutos. El valor oscila entre **5** y **1440** (un día).
Ajustes de latidos del corazón	Heartbeat Reporting	Especifica si se deben informar periódicamente los mensajes de latidos de Syslog. Puede activar o desactivar la función. La función está desactivada por defecto.
	Heartbeat Interval (minutes)	Especifica el intervalo para informar periódicamente los mensajes de latidos del corazón. Este parámetro sólo es válido cuando **Heartbeat Reporting** está habilitado. El valor predeterminado es **15** en minutos. El valor oscila entre **1** y **60**.
	Heartbeat Packet	Especifica el mensaje de latido del corazón que se va a informar. Este parámetro es válido cuando **Heartbeat Reporting** está activado y no se puede dejar en blanco. El valor puede contener un máximo de 256 caracteres, incluidos dígitos, letras, guiones bajos (_), barras verticales (|), dos puntos (:), espacios, comas (,), y puntos (.).

NOTA

Después de que se habilite la función de paquete de latidos periódicos, los paquetes pueden interrumpirse durante la recuperación automática de alguna tolerancia a errores de clúster (por ejemplo, conmutación OMS activa/en espera). En este caso, espere a la recuperación automática.

Paso 5 Haga clic en **OK**.

----Fin

Información relacionada

Tabla 7-47 Códigos numéricos de **Severity Level** y **Facility**

Nivel de seguridad	Facility	Código numérico
Emergency	kernel messages	0
Alert	user-level messages	1
Critical	mail system	2
Error	system daemons	3
Warning	security/authorization messages (note 1)	4
Notice	messages generated internally by syslog	5
Informational	line printer subsystem	6
Debug	network news subsystem	7
-	UUCP subsystem	8
-	clock daemon (note 2)	9
-	security/authorization messages (note 1)	10
-	FTP daemon	11
-	NTP subsystem	12
-	log audit (note 1)	13
-	log alert (note 1)	14
-	clock daemon (note 2)	15
-	local use 0~7 (local0 ~ local7)	16 to 23

Tabla 7-48 Campos de información de formato de informe

Campo de información	Descripción
dn	Nombre del clúster
id	ID de alarma
name	Nombre de alarma
serialNo	Número de serie de alarma **NOTA** Los números de serie de las alarmas de falla y las alarmas de borrado correspondientes son los mismos.
category	Tipo de alarma. Las opciones son las siguientes: ● **0**: alarma de falla ● **1**: borrar alarma ● **2**: evento
occurTime	Hora en que se generó la alarma
clearTime	Hora en que se borró esta alarma
isAutoClear	Si una alarma se borra automáticamente. Las opciones son las siguientes: ● **1**: sí ● **0**: no
locationInfo	Ubicación donde se generó la alarma
clearType	Tipo de borrado de alarma. Las opciones son las siguientes: ● **-1**: no borrado ● **0**: borrado automáticamente ● **2**: borrado manualmente
level	Severidad. Las opciones son las siguientes: ● **1**: alarma crítica ● **2**: alarma mayor ● **3**: alarma menor ● **4**: alarma de advertencia
cause	Causa de la alarma
additionalInfo	Información adicional
object	Objeto de la alarma

7.7.2.3 Configuración del volcado de métricas de monitoreo

Escenario

La función de informe de datos de monitoreo escribe los datos de monitoreo recogidos en el sistema en un archivo de texto y carga el archivo a un servidor especificado en modo FTP o SFTP.

Antes de utilizar esta función, debe realizar configuraciones relacionadas en FusionInsight Manager.

Procedimiento

Paso 1 Inicie sesión en FusionInsight Manager.

Paso 2 Elija **System** >**Interconnection** >**Upload Performance Data**.

Paso 3 Alterne **Upload Performance Data**.

El servicio de carga de datos de rendimiento está deshabilitado de forma predeterminada. indica que el servicio está habilitado.

Paso 4 Establezca los parámetros de carga según **Tabla 7-49**.

Tabla 7-49 Parámetros de carga

Parámetro	Descripción
FTP IP Address Mode	Especifica el modo de dirección IP del servidor. Este parámetro es obligatorio. El valor puede ser **IPV4** o **IPV6**.
FTP IP Address	Especifica la dirección IP del servidor FTP para almacenar archivos de monitoreo después de interconectar los datos de la métrica de monitoreo. Este parámetro es obligatorio.
FTP Port	Especifica el puerto para conectarse al servidor FTP. Este parámetro es obligatorio.
FTP Username	Especifica el nombre de usuario para iniciar sesión en el servidor FTP. Este parámetro es obligatorio.
FTP Password	Especifica la contraseña para iniciar sesión en el servidor FTP. Este parámetro es obligatorio.
Save Path	Especifica la ruta de acceso para almacenar los archivos de monitoreo en el servidor FTP. Este parámetro es obligatorio.
Dump Interval (second)	Especifica el intervalo en el que los archivos de monitoreo se almacenan periódicamente en el servidor FTP, en segundos. Este parámetro es obligatorio.
Dump Mode	Especifica el protocolo utilizado para enviar archivos de monitoreo. Este parámetro es obligatorio. El valor puede ser **SFTP** o **FTP**. Se recomienda utilizar el modo SFTP basado en SSH v2. De lo contrario, se pueden incurrir en riesgos de seguridad.

Parámetro	Descripción
SFTP Service Public Key	Especifica la clave pública del servidor FTP. Este parámetro es opcional. Solo es válido cuando **Dump Mode** está establecido en **SFTP**.

Paso 5 Haga clic en **OK**.

NOTA

Si el modo de volcado es SFTP y la clave pública del servicio SFTP está vacía, el sistema muestra una advertencia de riesgo de seguridad. Debe evaluar el riesgo de seguridad y luego guardar la configuración.

----Fin

Formato de datos

Una vez completada la configuración, la función de informe de datos de monitorización escribe periódicamente datos de monitorización en el clúster en archivos de texto e informa de los archivos al servicio FTP/SFTP correspondiente basándose en el período de informe configurado.

- Principios para generar archivos de monitorización
  - Las métricas de monitorización se escriben en archivos generados cada 30, 60 y 300 segundos basándose en el período de recopilación de métricas.

    30s: métricas en tiempo real que se recopilan cada 30s de forma predeterminada

    60s: métricas en tiempo real que se recopilan cada 60s de forma predeterminada

    300s: todas las métricas que no se recopilan cada 30s o 60s
  - Formato de nombre de archivo: *metric_{Interval}_{File creation time YYYYMMDDHHMMSS}.log*

    Ejemplo: **metric_60_20160908085915.log**

    metric_300_20160908085613.log
- Monitorización del contenido de archivos
  - Formato de archivos de monitorización:

    "Cluster ID|Cluster name|Displayed name|Service name|Metric ID|Collection time|Collection host@m@Sub-metric|Unit|Metric value", where fields are separated using vertical bars (|). Por ejemplo:

    ```
    1|xx1|Host|Host|10000413|2019/06/18 10:05:00|189-66-254-146|KB/s|309.910
    1|xx1|Host|Host|10000413|2019/06/18 10:05:00|189-66-254-152|KB/s|72.870
    2|xx2|Host|Host|10000413|2019/06/18 10:05:00|189-66-254-163|KB/s|100.650
    ```

    Nota: Los archivos reales no están en ese formato.
  - Intervalo para cargar archivos de monitorización:

    El intervalo para cargar archivos de monitorización se puede establecer utilizando el parámetro **Dump Interval (second)** de la página. Actualmente, el intervalo puede variar de **30** a **300**. Una vez completada la configuración, el sistema carga periódicamente archivos al servidor FTP/SFTP correspondiente en el intervalo especificado.
- Archivo de descripción de métricas de monitoreo

- Archivo de conjuntos de métricas

  El archivo de conjunto de métricas **all-shown-metric-zh_CN** contiene información detallada sobre todas las métricas. Después de obtener los ID de métricas de los archivos notificados por el sistema de terceros, puede consultar detalles sobre las métricas del archivo de conjunto de métricas.

  Ubicación del archivo de conjunto de métricas:

  Nodos de OMS activos y en espera: {*FusionInsight installation path*} **/om-server/om/etc/om/all-shown-metric-zh_CN**

  Content of the metric set file:

  ```
  Real-Time Metric ID,5-Minute Metric ID,Metric Name,Metric Collection
  Period (s),Collected by Default,Service Belonged To,Role Belonged To
  00101,10000101,JobHistoryServer non-heap memory
  usage,30,false,Mapreduce,JobHistoryServer
  00102,10000102,JobHistoryServer non-heap memory allocation
  volume,30,false,Mapreduce,JobHistoryServer
  00103,10000103,JobHistoryServer heap memory
  usage,30,false,Mapreduce,JobHistoryServer
  00104,10000104,JobHistoryServer heap memory allocation
  volume,30,false,Mapreduce,JobHistoryServer
  00105,10000105,Number of blocked
  threads,30,false,Mapreduce,JobHistoryServer
  00106,10000106,Number of running
  threads,30,false,Mapreduce,JobHistoryServer
  00107,10000107,GC time,30,false,Mapreduce,JobHistoryServer
  00110,10000110,JobHistoryServer CPU
  usage,30,false,Mapreduce,JobHistoryServer
  ...
  ```

- Descripción de campo de las métricas críticas

  Real-Time Metric ID: indica el ID de la métrica cuyo período de recopilación es 30s o 60s.

  5-Minute Metric ID: indica el ID de una métrica de 5 minutos (300s).

  Metric Collection Period (s): indica el período de recopilación de métricas en tiempo real. El valor puede ser **30** o **60**.

  Service Belonged To: indica el nombre del servicio al que pertenece una métrica, por ejemplo, HDFS y HBase.

  Role Belonged To: indica el nombre del rol al que pertenece una métrica, por ejemplo, JobServer y RegionServer.

- Descripción

  Para las métricas cuyo período de recopilación es 30s/60s, puede encontrar la descripción de la métrica correspondiente haciendo referencia a la primera columna, es decir, **Real-Time Metric ID**.

  Para las métricas cuyo período de recopilación es de 300 segundos, puede encontrar la descripción de la métrica correspondiente haciendo referencia a la segunda columna, es decir, **5-Minute Metric ID**.

7.7.3 Importación de un certificado

Escenario

Los certificados de CA se utilizan para cifrar datos durante la comunicación entre los módulos de FusionInsight Manager y entre los clientes de componentes de clúster y los servidores para garantizar la seguridad. Los certificados de CA se pueden importar rápidamente a

FusionInsight Manager para la seguridad del producto. Importe certificados de CA en los siguientes escenarios:

- Cuando se instala el clúster por primera vez, debe reemplazar el certificado de empresa.
- Si el certificado de empresa ha caducado o es necesario reforzar la seguridad, debe reemplazarlo por un nuevo certificado.

Impacto en el sistema

- Durante la sustitución de certificados, es necesario reiniciar el clúster. En este caso, el sistema se vuelve inaccesible y no puede proporcionar servicios.
- Después de reemplazar el certificado, los certificados utilizados por todos los componentes y módulos del FusionInsight Manager se actualizan automáticamente.
- Después de reemplazar el certificado, debe volver a instalar el certificado en el entorno local donde el certificado no es de confianza.

Prerrequisitos

- Ha generado el archivo de certificado y el archivo de clave u obtenido del administrador de certificados de empresa.
- Ha obtenido los archivos que se van a importar al clúster, incluidos el archivo de certificado de CA (***.crt**), el archivo de clave (***.key**) y el archivo que guarda la contraseña del archivo de clave (**password.property**). El nombre del certificado y el nombre de la clave pueden contener letras mayúsculas, minúsculas y dígitos. Una vez generados los archivos anteriores, comprimirlos en un paquete TAR.
- Ha obtenido una contraseña para acceder al archivo de clave, por ejemplo, **Userpwd@123**.

  Para evitar posibles riesgos de seguridad, la contraseña debe cumplir los siguientes requisitos de complejidad:

  – Contiene al menos 8 caracteres.

  – Contiene al menos cuatro tipos de los siguientes: letras mayúsculas, minúsculas, números y caracteres especiales (~`!?,.;-_'(){}[]/<>@#$%^&*+|\=).
- Al solicitar certificados del administrador de certificados, ha proporcionado la contraseña para acceder al archivo de clave y ha solicitado los archivos de certificado en formatos CRT, CER, CERT y PEM y los archivos de clave en formatos KEY y PEM. Los certificados solicitados deben tener la función de emisión.

Procedimiento

Paso 1 Inicie sesión en FusionInsight Manager y elija **System** > **Certificate**.

Paso 2 Haga clic en ··· a la derecha de **Upload Certificate**. En la ventana de selección de archivos, busque para seleccionar el paquete TAR obtenido de los archivos de certificado.

Paso 3 Haga clic en **Upload**.

Manager carga el paquete comprimido e importa automáticamente el paquete.

Paso 4 Después de importar el certificado, el sistema muestra un mensaje pidiéndole que sincronice la configuración del clúster y reinicie el servicio web para que el nuevo certificado surta efecto. Haga clic en **OK**.

Paso 5 En el cuadro de diálogo que se muestra, introduzca la contraseña del usuario de inicio de sesión actual y haga clic en **OK**. La configuración del clúster se sincroniza automáticamente y el servicio web se reinicia.

Paso 6 Después de reiniciar el clúster, introduzca la dirección URL para acceder al FusionInsight Manager en el cuadro de direcciones del navegador y compruebe si la página web del FusionInsight Manager se puede mostrar correctamente.

Paso 7 Inicie sesión en FusionInsight Manager.

Paso 8 Elija **Cluster**, haga clic en el nombre del clúster de destino, elija **Dashboard**, haga clic en **More** y seleccione **Restart**.

Paso 9 En el cuadro de diálogo que se muestra, introduzca la contraseña del usuario de inicio de sesión actual y haga clic en **OK**.

----Fin

7.7.4 Gestión de OMS

7.7.4.1 Descripción de la página OMS

Descripción

Inicie sesión en FusionInsight Manager y elija **System** > **OMS**. Puede realizar operaciones de mantenimiento en la página OMS, incluida la visualización de información básica, el estado del servicio de los módulos de servicio OMS y la activación manual de comprobaciones de estado.

NOTA

OMS es el nodo de gestión del sistema O&M. Generalmente, hay dos nodos OMS que funcionan en modo activo/en espera.

Información básica

La información asociada a OMS se muestra en FusionInsight Manager, tal como aparece en la lista de **Tabla 7-50**.

Tabla 7-50 Información OMS

Concepto	Descripción
Versión	Indica la versión de OMS, que es coherente con la versión del FusionInsight Manager.
Modo IP	Indica el modo de dirección IP de la red de clúster actual.
Modo HA	Indica el modo de trabajo de OMS, que especifica el archivo de configuración durante la instalación de FusionInsight Manager.
Activo actual	Indica el nombre de host del nodo OMS activo, es decir, el nombre de host del nodo de gestión activo. Haga clic en un nombre de host para ir a la página de detalles de host.

Concepto	Descripción
Actual en espera	Indica el nombre de host del nodo OMS en espera, es decir, el nombre de host del nodo de gestión en espera. Haga clic en un nombre de host para ir a la página de detalles de host.
Duración	Indica la duración para iniciar el proceso OMS.

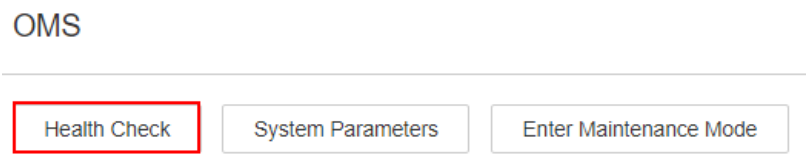
Estado del servicio OMS

FusionInsight Manager muestra el estado de ejecución de todos los módulos de servicio de OMS. Si el estado de cada módulo de servicio se muestra como , el OMS se está ejecutando correctamente.

Comprobación de estado

Puede hacer clic en **Health Check** en la página OMS para comprobar el estado de OMS. Si algunos elementos de comprobación son defectuosos, puede ver la descripción de la comprobación para la solución de problemas.

Figura 7-54 Comprobación de estado



Entrar o salir del modo de mantenimiento

Configure OMS para entrar o salir del modo de mantenimiento.

Parámetros del sistema

Conéctese al clúster DMPS en escenarios de clúster a gran escala.

7.7.4.2 Modificación de los parámetros de configuración del servicio OMS

Escenario

En función de los requisitos de seguridad del entorno de usuario, puede modificar las configuraciones de Kerberos y LDAP en OMS en FusionInsight Manager.

Impacto en el sistema

Después de modificar los parámetros de configuración del servicio OMS, es necesario reiniciar el módulo OMS correspondiente. En este caso, no se puede utilizar FusionInsight Manager.

Procedimiento

Modificación de la configuración de okerberos

Paso 1 Inicie sesión en FusionInsight Manager y elija **System** > **OMS**.

Paso 2 Busque la fila que contiene okerberos y haga clic en **Modify Configuration**.

Paso 3 Modifique los parámetros según **Tabla 7-51**.

Tabla 7-51 parámetros de okerberos

Parámetro	Descripción
KDC Timeout (ms)	Tiempo de espera de una aplicación para conectarse a Kerberos, en milisegundos. El valor debe ser un entero.
Max Retries	Número máximo de reintentos para que una aplicación se conecte a Kerberos, en segundos. El valor debe ser un entero.
LDAP Timeout (ms)	Tiempo de espera para que Kerberos se conecte a LDAP, en milisegundos.
LDAP Search Timeout (ms)	Tiempo de espera para que Kerberos consulte la información del usuario en LDAP, en milisegundos.
Kadmin Listening Port	Número de puerto del servicio Kadmin.
KDC Listening Port	Número de puerto del servicio kinit.
Kpasswd Listening Port	Número de puerto del servicio Kpasswd.
Reset LDAP Account Password	Usuarios máquina-máquina (**cn=krbadmin,ou=Users,dc=hadoop,dc=com** y **cn=krbkdc,ou=Users,dc=hadoop,dc=com**) utilizados por Kerberos para acceder a LDAP. Si se selecciona este parámetro, las contraseñas serán reemplazadas por contraseñas aleatorias. **NOTA** Este parámetro solo está disponible en MRS 3.1.2 o posterior.

Paso 4 Haga clic en **OK**.

En el cuadro de diálogo que se muestra, introduzca la contraseña del usuario de inicio de sesión actual y haga clic en **OK**. En el cuadro de diálogo de confirmación que se muestra, haga clic en **OK**.

Modificación de la configuración de oldap

Paso 5 Busque la fila que contiene el oldap y haga clic en **Modify Configuration**.

Paso 6 Modifique los parámetros según **Tabla 7-52**.

Tabla 7-52 parámetros de OLDAP

Parámetro	Descripción
LDAP Listening Port	Número de puerto del servicio LDAP.
Reset LDAP Account Password	Usuarios máquina-máquina (**cn=root,dc=hadoop,dc=com** y **cn=pg_search_dn,ou=Users,dc=hadoop,dc=com**) utilizados por LDAP para la gestión de datos, sincronización y comprobación de estado. Si se selecciona este parámetro, las contraseñas serán reemplazadas por contraseñas aleatorias. **NOTA** Este parámetro solo está disponible en MRS 3.1.2 o posterior.

Paso 7 Haga clic en **OK**.

En el cuadro de diálogo que se muestra, introduzca la contraseña del usuario de inicio de sesión actual y haga clic en **OK**. En el cuadro de diálogo de confirmación que se muestra, haga clic en **OK**.

NOTA

Para restablecer la contraseña de la cuenta LDAP, debe reiniciar ACS. El procedimiento es el siguiente:

1. Inicie sesión en el nodo de gestión activo como usuario **omm** mediante PuTTY y ejecute el siguiente comando para actualizar la configuración del dominio:

   sh ${BIGDATA_HOME}/om-server/om/sbin/restart-RealmConfig.sh

   El comando se ejecuta correctamente si se muestra la siguiente información:

   ```
   Modify realm successfully. Use the new password to log into FusionInsight again.
   ```

2. Ejecute el comando **sh $CONTROLLER_HOME/sbin/acs_cmd.sh stop** para detener el ACS.
3. Ejecute el comando **sh $CONTROLLER_HOME/sbin/acs_cmd.sh start** para iniciar ACS.

Reinicio del clúster

Paso 8 Inicie sesión en FusionInsight Manager y reinicie el clúster haciendo referencia a **Realización de un reinicio continuo de un clúster**.

----Fin

7.8 Gestión de clúster

7.8.1 Gestión de confianza mutua en clústeres

7.8.1.1 Descripción de la confianza mutua entre clústeres

Descripción de función

De forma predeterminada, los usuarios de un clúster de big data en modo de seguridad solo pueden acceder a los recursos del clúster, pero no pueden realizar la autenticación de identidad ni acceder a los recursos de otros clústeres en modo de seguridad.

Descripción de características

- **Dominio**

  El alcance de uso seguro de los usuarios en cada sistema se denomina dominio. Cada FusionInsight Manager debe tener un nombre de dominio único. El acceso a Cross-Manager permite a los usuarios utilizar recursos en todos los dominios.

- **Encriptación de usuario**

  La confianza mutua se puede configurar entre FusionInsight Managers. El servidor Kerberos actual solo admite los tipos de encriptación aes256-cts-hmac-sha1-96:normal y aes128-cts-hmac-sha1-96:normal para cifrar usuarios entre dominios, y los tipos de encriptación no se pueden cambiar.

- **Autenticación de usuario**

  Después de configurar la confianza mutua entre administradores, si existe un usuario con el mismo nombre en dos sistemas y el usuario en el sistema del mismo nivel tiene el permiso para acceder a un recurso en ese sistema, este usuario también puede acceder al recurso remoto.

- **Confianza mutua directa**

  El sistema guarda el vale de confianza mutua del sistema del mismo nivel en dos clústeres con la confianza mutua configurada y utiliza el vale de confianza mutua para acceder al sistema del mismo nivel.

7.8.1.2 Cambiar el nombre de dominio de Manager

Escenario

El alcance de uso seguro de los usuarios en cada sistema se denomina dominio. Cada sistema debe tener un nombre de dominio único. El nombre de dominio de FusionInsight Manager se genera durante la instalación. El administrador del sistema puede cambiar el nombre de dominio en FusionInsight Manager.

AVISO

- Cambiar el nombre de dominio del sistema es una operación de alto riesgo. Antes de realizar las operaciones de esta sección, asegúrese de que se ha realizado una copia de seguridad de los datos OMS haciendo referencia a **Copia de respaldo de los datos del Manager**.

Impacto en el sistema

- Durante la configuración, todos los clústeres deben reiniciarse y no están disponibles durante el reinicio.
- Después de cambiar el nombre de dominio, se inicializarán las contraseñas del administrador de Kerberos y del administrador de Kerberos de OMS. Es necesario utilizar las contraseñas predeterminadas y luego cambiar las contraseñas. Si un usuario componente cuya contraseña es generada aleatoriamente por el sistema se utiliza para la autenticación de identidad, vea **Exportación de un archivo de credenciales de autenticación** para descargar el archivo keytab de nuevo.
- Después de cambiar el nombre de dominio, las contraseñas del usuario **admin**, usuario de componente y usuario de hombre-máquina agregadas por el administrador del sistema

antes del cambio de nombre de dominio se restablecerán a la misma. Cambie estas contraseñas. La contraseña de restablecimiento consta de dos partes: una parte es generada por el sistema y la otra es establecida por el usuario. La parte generadora del sistema es **Admin@123** que es la contraseña por defecto. Para obtener más información sobre la parte definida por el usuario, consulte las descripciones de **Password Suffix** en **Tabla 7-54**. Por ejemplo, si el sistema genera **Admin@123** y el usuario establece **Test#$%@123**, la nueva contraseña después del reinicio será **Admin@123Test#$%@123**.

- La nueva contraseña debe cumplir las políticas de contraseñas. Para obtener la nueva contraseña de usuario de humano-máquina, inicie sesión en el OMS activo como usuario **omm** y ejecute el siguiente script:

  sh ${BIGDATA_HOME}/om-server/om/sbin/get_reset_pwd.sh *Password suffix user_name*

  – *Password suffix* es un parámetro establecido por el usuario. Si no se especifica, se utiliza el valor predeterminado **Admin@123**.

  – *user_name* es opcional. El valor predeterminado es **admin**.

  Ejemplo:

  sh ${BIGDATA_HOME}/om-server/om/sbin/get_reset_pwd.sh Test#$%@123

  ```
  Para obtener la contraseña de restablecimiento después de cambiar el nombre
  de dominio del clúster.
    pwd_min_len      : 8
    pwd_char_types   : 4
  The password reset after changing cluster domain name is: "Admin@123Test#$
  %@123"
  ```

  En este ejemplo, **pwd_min_len** y **pwd_char_types** indican la longitud mínima de contraseña y el número de tipos de caracteres de contraseña definidos respectivamente en las políticas de contraseña. **Admin@123Test#$%@123** indica la contraseña del usuario de humano-máquina después de cambiar el nombre de dominio del sistema.

- Después de cambiar el nombre de dominio del sistema, la contraseña de restablecimiento consta de dos partes: una parte es generada por el sistema y la otra es establecida por el usuario. La contraseña de restablecimiento debe cumplir las políticas de contraseñas. Si la contraseña no es lo suficientemente larga, se agregan uno o varios (@) entre **Admin@123** y la parte definida por el usuario. Si hay cinco tipos de caracteres, se agrega un espacio después de **Admin@123**.

  Cuando la parte definida por el usuario es **Test@123** y se utiliza la política de contraseñas de usuario predeterminada, la nueva contraseña es **Admin@123Test@123**. La contraseña contiene 17 caracteres de cuatro tipos. Para cumplir con la política de contraseñas actual, la nueva contraseña se procesa de acuerdo con **Tabla 7-53**.

Tabla 7-53 Procesamiento de contraseñas

Mínima longitud de contraseña	Número de tipos de caracteres	Procesamiento contra la política de contraseñas	Contraseña nueva
8 a 17 caracteres	4	Se cumple la política de contraseñas de usuario.	Admin@123Test@123
18 caracteres	4	Agregar un signo de arroba (@).	Admin@123@Test@123
19 caracteres	4	Agregar dos signos de arroba (@).	Admin@123@@Test@123

Mínima longitud de contraseña	Número de tipos de caracteres	Procesamiento contra la política de contraseñas	Contraseña nueva
8 a 18 caracteres	5	Agregar un espacio.	Admin@123 Test@123
19 caracteres	5	Agregar un espacio y un signo de arroba (@).	Admin@123 @Test@123
20 caracteres	5	Agregar un espacio y dos arrobas (@).	Admin@123 @@Test@123

- Después de cambiar el nombre de dominio del sistema, descargue el archivo **keytab** para el usuario máquina-máquina agregado por el administrador del sistema antes de cambiar el nombre de dominio.
- Después de cambiar el nombre de dominio del sistema, descargue e instale el cliente de nuevo.
- Después de cambiar el nombre de dominio del sistema, si hay alguna instancia de cómputo de en ejecución, reinicie la instancia.

Prerrequisitos

- El administrador del sistema ha aclarado los requisitos de servicio y ha planificado los nombres de dominio para los sistemas.

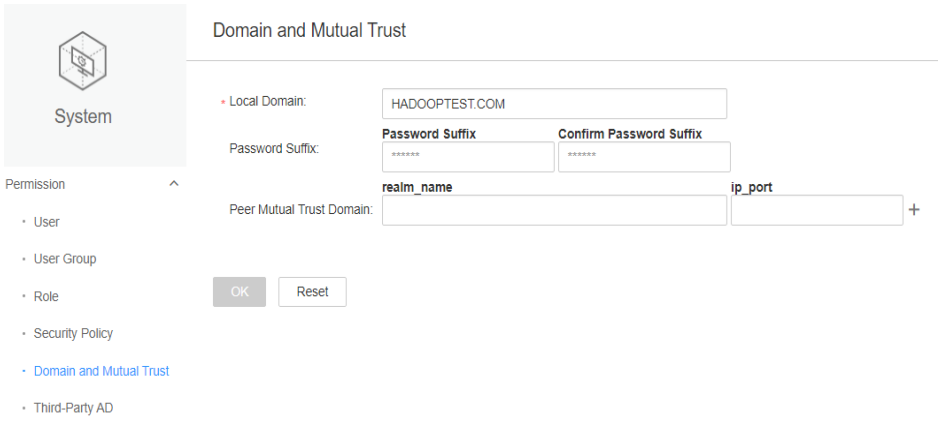
  Un nombre de dominio puede contener solo letras mayúsculas, números, (.), de puntos y guiones bajos (_), y debe comenzar con letras o números, por ejemplo, **DOMAINA.HW** y **DOMAINB.HW**.
- El estado de ejecución de todos los componentes de los clústeres de Manager es de **Normal**.
- El parámetro **acl.compare.shortName** del servicio ZooKeeper de todos los clústeres del Manager se establece en el valor predeterminado **true**. De lo contrario, cambie el valor a **true** y reinicie el servicio ZooKeeper.

Procedimiento

Paso 1 Inicie sesión en FusionInsight Manager.

Paso 2 Elija **System** >**Permission** >**Domain and Mutual Trust**.

Figura 7-55 Dominio y confianza mutua



Paso 3 Modifique los parámetros requeridos.

Tabla 7-54 Parámetros relacionados

Parámetro	Descripción
Local Domain	Nombre de dominio planificado del sistema.
Password Suffix	Parte de la contraseña establecida por el usuario después de restablecer la contraseña del usuario humano-máquina. Este parámetro es obligatorio. El valor predeterminado es **Admin@123**. **NOTA** Este parámetro solo tiene efecto después de modificar **Local Domain**. Deben cumplirse las siguientes condiciones: ● La contraseña oscila entre 8 y 16 caracteres. ● La contraseña debe contener al menos tres tipos de los siguientes: letras mayúsculas, minúsculas, números y caracteres especiales (`~!@#$ %^&*()-_=+|[{}];:',<.>/? y espacios).

Paso 4 Haga clic en **OK**. Continúe con los pasos siguientes sólo después de que se complete la modificación.

Paso 5 Inicie sesión en el nodo de gestión activo como usuario **omm**.

Paso 6 Ejecute el siguiente comando para actualizar la configuración del dominio:

sh ${BIGDATA_HOME}/om-server/om/sbin/restart-RealmConfig.sh

El comando se ejecuta correctamente si se muestra la siguiente información:

```
Modify realm successfully. Use the new password to log into FusionInsight again.
```

NOTA

Después del reinicio, no se puede acceder a algunos hosts y servicios y se genera una alarma. Este problema se puede resolver automáticamente en aproximadamente 1 minuto después de ejecutar **restart-RealmConfig.sh**.

Paso 7 Inicie sesión en FusionInsight Manager con la nueva contraseña de usuario **admin** (por ejemplo, **Admin@123Admin@123**). En el panel de control, haga clic en ▪▪▪ junto al nombre del clúster de destino y seleccione **Restart**.

En el cuadro de diálogo que se muestra, introduzca la contraseña del usuario de inicio de sesión actual y haga clic en **OK**.

En el cuadro de diálogo que se muestra, haga clic en **OK**. Espere un momento hasta que se muestre un mensaje que indique que la operación se ha realizado correctamente. Haga clic en **Finish**.

Paso 8 Cierre la sesión de FusionInsight Manager y vuelva a iniciar sesión. Si el inicio de sesión se realiza correctamente, la configuración se realiza correctamente.

Paso 9 Inicie sesión en el nodo de gestión activo como usuario **omm** y ejecute el siguiente comando para actualizar las configuraciones del cliente de envío de trabajos:

sh /opt/executor/bin/refresh-client-config.sh

Paso 10 Si se está ejecutando una instancia de cómputo de, reinicie la instancia de cómputo.

1. Inicie sesión en FusionInsight Manager como el usuario que se utiliza para acceder a la interfaz de usuario web del **HetuEngine**.
2. Seleccione **Cluster** > **Services** > **HetuEngine** para ir a la página de servicio de **HetuEngine**.
3. En el área **Basic Information** de la página **Dashboard**, haga clic en el enlace situado junto a **HSConsole WebUI**. Se muestra la página HSConsole.
4. Para una instancia de cálculo en ejecución, haga clic en **Stop** en la columna **Operation**. Una vez que la instancia de cómputo esté en el estado **Stopped**, haga clic en **Start** para reiniciar la instancia de cómputo.

----Fin

7.8.1.3 Configuración de la confianza mutua Cross-Manager entre clústeres

Escenario

Cuando dos clústeres en modo de seguridad gestionados por diferentes FusionInsight Managers necesitan tener acceso a los recursos del otro, el administrador del sistema puede configurar la confianza mutua entre Manager.

El alcance de uso seguro de los usuarios en cada sistema se denomina dominio. Cada FusionInsight Managers debe tener un nombre de dominio único. El acceso a Cross-Manager permite a los usuarios utilizar recursos en todos los dominios.

NOTA

Se puede configurar un máximo de 500 clústeres de confianza mutua.

Impacto en el sistema

- Después de configurar la confianza mutua del clúster de cross-Manager, los usuarios de un sistema externo se pueden utilizar en el sistema local. El administrador del sistema debe comprobar periódicamente los permisos de usuario en Manager según los requisitos de seguridad y servicio de la empresa.
- Cuando se configura la confianza mutua de clústeres de cross-Manager, es necesario detener todos los clústeres, lo que provoca interrupciones del servicio.
- Después de configurar la confianza mutua del clúster de cross-Manager, los usuarios internos de Kerberos **krbtgt**/*Local cluster domain name@External cluster domain name*

y **krbtgt/***External cluster domain name***@***Local cluster domain name* se agregan a los dos clústeres de confianza mutua. Los usuarios internos no se pueden eliminar. El administrador del sistema debe cambiar las contraseñas periódicamente en función de los requisitos de seguridad y servicio de la empresa. Las contraseñas de estos cuatro usuarios en los dos sistemas deben ser las mismas. Cuando se cambian las contraseñas, la conectividad entre aplicaciones de servicio entre clústeres puede verse afectada.

- Después de configurar la confianza mutua del clúster de cross-Manager, los clientes de cada clúster deben descargarse e instalarse de nuevo.
- Después de configurar la confianza mutua del clúster de cross-Manager, debe comprobar si el sistema funciona correctamente y cómo acceder a los recursos del sistema del mismo nivel como usuario del sistema local. Para obtener más información, consulte **Asignación de permisos de usuario después de configurar la confianza mutua entre clústeres**.

Prerrequisitos

- El administrador del sistema ha aclarado los requisitos de servicio y ha planificado los nombres de dominio para los sistemas. Un nombre de dominio puede contener solo letras mayúsculas, números, (.), de puntos y guiones bajos (_), y debe comenzar con letras o números, por ejemplo, **DOMAINA.HW** y **DOMAINB.HW**.
- Los nombres de dominio de los dos Manager son diferentes. Cuando se crea un clúster ECS o BMS en MRS, se genera aleatoriamente un nombre de dominio de sistema único. Por lo general, no es necesario cambiar el nombre de dominio del sistema.
- Los dos clústeres no tienen el mismo nombre de host o la misma dirección IP.
- La hora del sistema de los dos clústeres es consistente y los servicios NTP en los dos sistemas usan la misma fuente de reloj.
- El estado de ejecución de todos los componentes de los clústeres de Manager es de **Normal**.
- El parámetro **acl.compare.shortName** del servicio ZooKeeper de todos los clústeres del Manager se establece en el valor predeterminado **true**. De lo contrario, cambie el valor a **true** y reinicie el servicio ZooKeeper.
- Los dos clústeres están en la misma VPC. Si no lo son, cree una conexión de pares de VPC entre ellos. Para obtener más información, consulte **Interconexión de VPC**.

Procedimiento

Paso 1 Inicie sesión en un FusionInsight Manager.

Paso 2 Detenga todos los clústeres en la página de inicio.

Haga clic en ··· junto al clúster de destino y seleccione **Stop**. Introduzca la contraseña del administrador del clúster. En el cuadro de diálogo **Stop Cluster** que se muestra, haga clic en **OK**. Espere hasta que se detenga el clúster.

Paso 3 Elija **System** >**Permission** >**Domain and Mutual Trust**.

Paso 4 Modifique **Peer Mutual Trust Domain**.

Tabla 7-55 Parámetros relacionados

Parámetro	Descripción
realm_name	Introduzca el nombre de dominio del sistema del mismo nivel.
ip_port	Introduzca la dirección KDC del sistema del mismo nivel. Formato de valor: *Dirección IP del nodo que alberga el servicio Kerberos en el sistema par: Número de puerto* ● En redes de doble plano, introduzca la dirección IP del plano de servicio. ● Si se utiliza una dirección IPv6, la dirección IP debe estar entre corchetes ([]). ● Utilice comas (,) para separar las direcciones KDC si se despliegan los servicios Kerberos activos y en espera o si varios clústeres en el sistema del mismo nivel necesitan establecer confianza mutua con el sistema local. ● Puede obtener el número de puerto del parámetro **kdc_ports** del servicio KrbServer. El valor predeterminado es **21732**. Para obtener la dirección IP del nodo donde se despliega el servicio, haga clic en la pestaña **Instance** de la página KrbServer y vea el **Service IP Address** del rol KerberosServer. Por ejemplo, si el servicio Kerberos se despliega en los nodos de **10.0.0.1** y **10.0.0.2** que han establecido confianza mutua con el sistema local, el valor del parámetro es **10.0.0.1:21732,10.0.0.2:21732**.

NOTA

Si necesita configurar la confianza mutua para varios Managers, haga clic en + para agregar un nuevo elemento y establecer parámetros. Se puede confiar mutuamente en un máximo de 16 sistemas. Haga clic en — para eliminar las configuraciones innecesarias.

Paso 5 Haga clic en **OK**.

Paso 6 Inicie sesión en el nodo de gestión activo como usuario **omm** y ejecute el siguiente comando para actualizar la configuración del dominio:

sh ${BIGDATA_HOME}/om-server/om/sbin/restart-RealmConfig.sh

El comando se ejecuta correctamente si se muestra la siguiente información:

```
Modify realm successfully. Use the new password to log into FusionInsight again.
```

Después del reinicio, no se puede acceder a algunos hosts y servicios y se genera una alarma. Este problema se puede resolver automáticamente en aproximadamente 1 minuto después de ejecutar **restart-RealmConfig.sh**.

Paso 7 Inicie sesión en FusionInsight Manager e inicie todos los clústeres.

Haga clic en ··· junto al nombre del clúster de destino y seleccione **Start**. En el cuadro de diálogo **Start Cluster** que se muestra, haga clic en **OK**. Espere hasta que se inicie el clúster.

Paso 8 Inicie sesión en el otro FusionInsight Manager y repita las operaciones anteriores.

----Fin

7.8.1.4 Asignación de permisos de usuario después de configurar la confianza mutua entre clústeres

Escenario

Después de configurar la confianza mutua del clúster entre administradores, asigne permisos de acceso de usuario en FusionInsight Manager para que estos usuarios puedan realizar operaciones de servicio en los Managers de confianza mutua.

Prerrequisitos

Se ha configurado la confianza mutua entre los dos Managers.

Procedimiento

Paso 1 Inicie sesión en FusionInsight Manager local.

Paso 2 Elija **System** > **Permission** > **User** para comprobar si existe el usuario de destino.

- En caso afirmativo, vaya a **Paso 3**.
- Si no, vaya a **Paso 4**.

Paso 3 Haga clic en ⌄ a la izquierda del usuario de destino y compruebe si los permisos asignados al grupo de usuarios del usuario y los roles cumplen con los requisitos de servicio. Si no es así, cree un rol y vincule el rol al usuario haciendo referencia a **Configuración de permisos** o modifique el grupo de usuarios o los permisos de rol del usuario.

Paso 4 Cree un usuario requerido por las operaciones de servicio y asocie el grupo o rol de usuario requerido. Para obtener más información, consulte **Creación de un usuario**.

Paso 5 Inicie sesión en el otro FusionInsight Manager y repita **Paso 2** a **Paso 4** para crear un usuario con el mismo nombre y establecer permisos.

----Fin

7.8.2 Configuración de la copia de respaldo programada de la información de alarma y auditoría

Escenario

Puede modificar el archivo de configuración para realizar periódicamente copias de respaldo de la información de alarma del FusionInsight Manager, la información de auditoría del FusionInsight Manager y la información de auditoría de todos los servicios en la ubicación de almacenamiento especificada.

La copia de respaldo se puede realizar mediante FTP o SFTP. FTP no cifra los datos, lo que puede causar riesgos de seguridad. Por lo tanto, se recomienda SFTP.

Procedimiento

Paso 1 Inicie sesión en el nodo de gestión activo como usuario **omm**.

NOTA

Realice esta operación sólo en el nodo de gestión activo. La copia de respaldo programada no se admite en el nodo de gestión en espera.

Paso 2 Ejecute el siguiente comando para cambiar el directorio:

cd ${BIGDATA_HOME}/om-server/om/sbin

Paso 3 Ejecute el siguiente comando para configurar la copia de respaldo programada de la información de auditoría y alarma del FusionInsight Manager o la información de auditoría de servicio:

./setNorthBound.sh -t *Information type* **-i** *Remote server IP address* **-p** *SFTP or FTP port used by the server*-**u** *Username* **-d** *Save path* **-c** *Interval (minutes)* **-m** *Number of records in each file* **-s** *Whether to enable backup* **-e** *Protocol*

Ejemplo:

./setNorthBound.sh -t alarm -i 10.0.0.10 -p 22 -u sftpuser -d /tmp/ -c 10 -m 100 -s true -e sftp

Este script modifica el archivo de configuración de copia de respaldo de alarma **alarm_collect_upload.properties**. La ruta de guardado del archivo es **${BIGDATA_HOME}/om-server/tomcat/webapps/web/WEB-INF/classes/config**.

./setNorthBound.sh -t audit -i 10.0.0.10 -p 22 -u sftpuser -d /tmp/ -c 10 -m 100 -s true -e sftp

Este script modifica el archivo de configuración de copia de respaldo de auditoría **audit_collect_upload.properties**. La ruta de guardado del archivo es **${BIGDATA_HOME}/om-server/tomcat/webapps/web/WEB-INF/classes/config**.

./setNorthBound.sh -t service_audit -i 10.0.0.10 -p 22 -u sftpuser -d /tmp/ -c 10 -m 100 -s true -e sftp

Este script modifica el archivo de configuración de copia de respaldo de auditoría de servicio **service_audit_collect_upload.properties**. La ruta de guardado del archivo es **${BIGDATA_HOME}/om-server/tomcat/webapps/web/WEB-INF/classes/config**.

Paso 4 Ingrese la contraseña como se le solicite. La contraseña se cifra y se guarda en el archivo de configuración.

```
Please input sftp/ftp server password:
```

Paso 5 Compruebe el resultado de la configuración. Si se muestra la siguiente información, la configuración se realiza correctamente. El archivo de configuración se sincronizará automáticamente con el nodo de gestión en espera.

```
execute command syncfile successfully.
Config Succeed.
```

----Fin

7.8.3 Modificación de la tabla de enrutamiento de FusionInsight Manager

Escenario

Cuando se instala FusionInsight Manager, se crean automáticamente dos piezas de información de enrutamiento en el nodo de gestión activa. Puede ejecutar el comando **ip rule list** para ver la información de enrutamiento, como se muestra en el siguiente ejemplo:

```
0:from all lookup local
32764:from all to 10.10.100.100 lookup ntp_rt   #NTP routing information created
by FusionInsight Manager (this information is unavailable if no external NTP
clock source is configured).
32765:from 192.168.0.117 lookup om_rt   #OM routing information created by the
FusionInsight Manager.
32766:from all lookup main
32767:from all lookup default
```

NOTA

Si no se ha configurado ningún servidor NTP externo, solo se creará la información de enrutamiento OM.

Si la información de enrutamiento creada por FusionInsight Manager entra en conflicto con la información de enrutamiento configurada en la planificación de red empresarial, el administrador del clúster puede usar **autoroute.sh** para deshabilitar o habilitar la información de enrutamiento creada por FusionInsight Manager.

Impacto en el sistema

Después de deshabilitar la información de enrutamiento creada por FusionInsight Manager y antes de establecer la nueva información de enrutamiento, no se puede acceder al FusionInsight Manager, pero los clústeres se ejecutan correctamente.

Prerrequisitos

Se ha instalado el FusionInsight Manager.

Ha obtenido información de enrutamiento sobre la dirección IP flotante de WS.

Deshabilitar la información de enrutamiento creada por el sistema

Paso 1 Inicie sesión en el nodo de gestión activo como usuario **omm**. Ejecute los siguientes comandos para deshabilitar la información de enrutamiento creada por el sistema:

cd ${BIGDATA_HOME}/om-server/om/sbin

./autoroute.sh disable

```
Deactivating Route.
Route operation (disable) successful.
```

Paso 2 Ejecute el siguiente comando para ver el resultado de la ejecución:

ip rule list

```
0:from all lookup local
32766:from all lookup main
32767:from all lookup default
```


Paso 3 Ejecute el siguiente comando e introduzca la contraseña de usuario **root** para cambiar a usuario **root**:

su - root

Paso 4 Ejecute los siguientes comandos para crear manualmente la información de enrutamiento sobre la dirección IP flotante de WS:

ip route add *Network segment of the WS floating IP address/Subnet mask of the WS floating IP address* **scope link src** *WS floating IP address* **dev** *NIC of the WS floating IP address* **table om_rt**

ip route add default via *Gateway of the WS floating IP address* **dev** *NIC of the WS floating IP address* **table om_rt**

ip rule add from *WS floating IP address* **table om_rt**

Ejemplo:

ip route add 192.168.0.0/255.255.255.0 scope link src 192.168.0.117 dev eth0:ws table om_rt

ip route add default via 192.168.0.254 dev eth0:ws table om_rt

ip rule add from 192.168.0.117 table om_rt

NOTA

Si se utilizan direcciones IPv6, ejecute el comando **ip -6 route add**.

Paso 5 Ejecute los siguientes comandos para crear manualmente la información de enrutamiento de servicio NTP. Omita este paso cuando no hay una fuente de reloj NTP externa está configurada.

ip route add default via *IP gateway of the NTP service* **dev** *NIC of the local IP address* **table ntp_rt**

ip rule add to *ntpIP* **table ntp_rt**

NIC of the local IP address indica la NIC que puede comunicarse con el segmento de red donde se encuentra el servidor NTP.

Ejemplo:

ip route add default via 10.10.100.254 dev eth0 table ntp_rt

ip rule add to 10.10.100.100 table ntp_rt

Paso 6 Consulte el resultado de la ejecución.

En el siguiente ejemplo, si el resultado del comando contiene **om_rt** y **ntp_rt**, la operación se realiza correctamente.

ip rule list

```
0:from all lookup local
32764:from all to 10.10.100.100 lookup ntp_rt  #This information is not displayed
if no external NTP clock source is configured.
32765:from 192.168.0.117 lookup om_rt
32766:from all lookup main
32767:from all lookup default
```

----Fin

Habilitar la información de enrutamiento creada por el sistema

Paso 1 Inicie sesión en el nodo de gestión activo como usuario **omm**.

Paso 2 Ejecute los siguientes comandos para habilitar la información de enrutamiento creada por el sistema:

cd ${BIGDATA_HOME}/om-server/om/sbin

./autoroute.sh enable

```
Activating Route.
Route operation (enable) successful.
```

Paso 3 Consulte el resultado de la ejecución.

En el siguiente ejemplo, si el resultado del comando contiene **om_rt** y **ntp_rt**, la operación se realiza correctamente.

ip rule list

```
0:from all lookup local
32764:from all to 10.10.100.100 lookup ntp_rt  #This information is not displayed if no external NTP clock source is configured.
32765:from 192.168.0.117 lookup om_rt
32766:from all lookup main
32767:from all lookup default
```

----Fin

7.8.4 Cambio al modo de mantenimiento

Escenario

FusionInsight Manager le permite establecer clústeres, servicios, hosts u OMSs en el modo de mantenimiento. Los objetos en modo de mantenimiento no reportan alarmas. Esto evita que el sistema genere un gran número de alarmas innecesarias durante los cambios de mantenimiento, como la actualización, porque estas alarmas pueden influir en el juicio del personal de O&M sobre el estado del clúster.

- Modo de mantenimiento del clúster

  Si un clúster no se pone en línea o se ha puesto fuera de línea debido a operaciones O&M (por ejemplo, actualización no móvil), puede configurar el clúster completo en el modo de mantenimiento.

- Modo de mantenimiento de servicio

  Al realizar operaciones de mantenimiento en un servicio específico (por ejemplo, realizar operaciones de puesta en marcha que afecten al servicio, como el reinicio por lotes de instancias de servicio, encender o apagar directamente los nodos del servicio, o reparar el servicio), solo puede configurar este servicio en el modo de mantenimiento.

- Modo de mantenimiento del host

  Al realizar operaciones de mantenimiento en un host (como encender o apagar, aislar o reinstalar el host, actualizar su sistema operativo o reemplazar el host), solo puede configurar este host en el modo de mantenimiento.

- Modo de mantenimiento de OMS

  Al reiniciar, reemplazar o reparar un nodo OMS, puede establecer el nodo OMS en el modo de mantenimiento.

Impacto en el sistema

Después de establecer el modo de mantenimiento, las alarmas causadas por operaciones de no mantenimiento se suprimen y no se pueden informar. Las alarmas solo pueden notificarse cuando las fallas persisten después de que el sistema salga del modo de mantenimiento. Por lo tanto, tenga cuidado al configurar el modo de mantenimiento.

Procedimiento

Paso 1 Inicie sesión en FusionInsight Manager.

Paso 2 Establezca el modo de mantenimiento.

Determine el objeto para establecer el modo de mantenimiento basado en el escenario de servicio. Para obtener más información, consulte **Tabla 7-56**.

Tabla 7-56 Ajuste al modo de mantenimiento

Escenario	Operación
Configurar un clúster para entrar en el modo de mantenimiento.	1. En FusionInsight Manager, haga clic en ··· junto al nombre del clúster de destino y seleccione **Enter Maintenance Mode**. 2. En el cuadro de diálogo que se muestra, haga clic en **OK**. Una vez que el clúster entra en el estado de mantenimiento, el estado del clúster pasa a ser . Una vez finalizado el mantenimiento, haga clic en **Exit Maintenance Mode**. A continuación, el clúster sale del modo de mantenimiento.
Configurar un servicio para entrar en el modo de mantenimiento.	1. En FusionInsight Manager, elija **Cluster** y haga clic en el nombre del clúster que desee, elija **Services** y haga clic en el nombre del servicio. 2. En la página de detalles del servicio, haga clic en **More** y seleccione **Enter Maintenance Mode**. 3. En el cuadro de diálogo que se muestra, haga clic en **OK**. Después de que un servicio entra en el modo de mantenimiento, el estado del servicio se convierte en en la lista de servicios. Una vez finalizado el mantenimiento, haga clic en **Exit Maintenance Mode**. A continuación, el servicio sale del modo de mantenimiento. **NOTA** Al configurar un servicio para entrar en el modo de mantenimiento, se recomienda configurar los servicios de capa superior que dependen de este servicio también en el modo de mantenimiento.

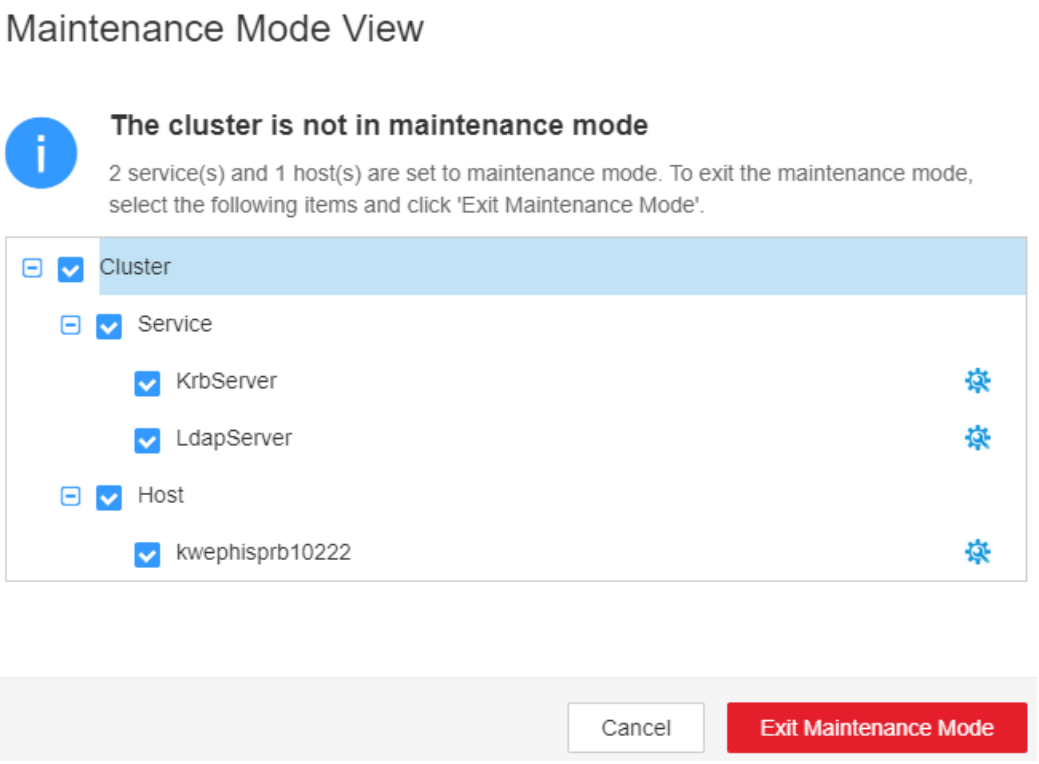
Escenario	Operación
Configurar un host en el modo de mantenimiento.	1. En FusionInsight Manager, seleccione **Hosts**. 2. En la página **Hosts**, seleccione el host de destino, haga clic en **More** y seleccione **Enter Maintenance Mode**. 3. En el cuadro de diálogo que se muestra, haga clic en **OK**. Después de que el host entra en el modo de mantenimiento, el estado del host se convierte en  en la lista de hosts. Una vez finalizado el mantenimiento, haga clic en **Exit Maintenance Mode**. A continuación, el host sale del modo de mantenimiento.
Configurar el OMS para entrar en el modo de mantenimiento.	1. En FusionInsight Manager, elija **System** > **OMS** > **Enter Maintenance Mode**. 2. En el cuadro de diálogo que se muestra, haga clic en **OK**. Una vez que el OMS entra en el estado de mantenimiento, el estado de OMS pasa a ser  . Una vez finalizado el mantenimiento, haga clic en **Exit Maintenance Mode**. A continuación, el OMS sale del modo de mantenimiento.

Paso 3 Compruebe la vista de mantenimiento del clúster.

En FusionInsight Manager, haga clic en  junto al nombre del clúster y seleccione **Maintenance Mode View**. En la ventana mostrada, puede ver los servicios y hosts en modo de mantenimiento en el clúster.

Una vez finalizado el mantenimiento, puede seleccionar servicios y hosts en lotes en la vista de modo de mantenimiento y hacer clic en **Exit Maintenance Mode** para que salgan del modo de mantenimiento.

Figura 7-56 Salir del modo de mantenimiento por lotes



----Fin

7.8.5 Mantenimiento de rutina

Para garantizar el funcionamiento estable y a largo plazo del sistema, los administradores o ingenieros de mantenimiento deben comprobar periódicamente los elementos enumerados en **Tabla 7-57** y rectificar las fallas detectados en función de los resultados de la comprobación. Se recomienda que los administradores o ingenieros registren el resultado en cada escenario de tarea y firmen según las normas de gestión empresarial.

Tabla 7-57 Artículos de verificación de mantenimiento de rutina

Frecuencia de mantenimiento rutinario	Escenario de tareas	Elemento de comprobación
Diario	Comprobar el estado del servicio del clúster.	● Compruebe si el estado de ejecución y el estado de configuración de cada servicio son normales y si los iconos de estado son verdes. ● Compruebe si el estado de ejecución y el estado de configuración de las instancias de rol en cada servicio son normales y si los iconos de estado son verdes. ● Compruebe si el estado activo/en espera de las instancias de rol en cada servicio se puede mostrar correctamente. ● Compruebe si el panel de control de los servicios y las instancias de rol se pueden mostrar correctamente.
	Comprobar el estado del host del clúster.	● Compruebe si el estado de ejecución de cada host es normal y si el icono de estado es verde. ● Compruebe el uso actual del disco, el uso de la memoria y el uso de la CPU de cada host. Compruebe si el uso actual de la memoria y el uso de la CPU están aumentando.
	Comprobar la información de alarma del clúster.	Compruebe si se generaron alarmas para las excepciones no controladas el día anterior, incluidas las alarmas que se eliminaron automáticamente.
	Comprobar la información de auditoría del clúster.	Compruebe si las operaciones críticas y principales se realizan el día anterior y si las operaciones son válidas.
	Comprobar el estado de la copia de respaldo del clúster.	Compruebe si OMS, DBService, NameNodeOMS, DBServiceOMS, y LDAP se han respaldado automáticamente el día anterior.
	Ver el resultado de la comprobación de estado.	Realice una comprobación de estado en FusionInsight Manager y descargue el informe de comprobación de estado para comprobar si el clúster actual es anormal. Se recomienda activar la comprobación automática de estado, exportar el resultado más reciente de la comprobación de estado del clúster y reparar los elementos no saludables basándose en el resultado.

Frecuencia de mantenimiento rutinario	Escenario de tareas	Elemento de comprobación
	Comprobar la comunicación de la red.	Compruebe el estado de la red del clúster y verifique si la comunicación de red entre nodos está retrasada.
	Comprobar el estado de almacenamiento.	Compruebe si el volumen total de almacenamiento de datos del clúster aumenta bruscamente. ● Compruebe si el uso del disco está cerca del umbral. En caso afirmativo, localice las causas. Por ejemplo, compruebe si los datos no deseados o los datos de uso bajo dejados por los servicios necesitan ser borrados. ● Compruebe si es necesario ampliar las particiones de disco según la tendencia de crecimiento del servicio.
	Comprobar los registros.	● Comprueba si hay tareas de MapReduce y Spark fallidas o que no responden. Compruebe el archivo de registro **/tmp/logs/${username}/logs/${application id}** en HDFS y rectifique las fallas. ● Compruebe los registros de tareas de Yarn, vea los registros de las tareas fallidas y que no responden y elimine los datos duplicados. ● Comprueba los registros de worker de Storm. ● Haga una copia de respaldo de los registros en el servidor de almacenamiento.
Semanal	Gestionar usuarios.	Compruebe si la contraseña de usuario está a punto de caducar y notifique al usuario si la cambia. Para cambiar la contraseña de un usuario máquina-máquina, debe descargar el archivo keytab de nuevo.
	Analizar las alarmas.	Exportar y analizar las alarmas generadas en un período especificado.
	Analizar discos.	Compruebe el estado del disco. Se recomienda utilizar una herramienta de comprobación de disco dedicada.
	Recopilar estadísticas sobre el almacenamiento.	Compruebe en lotes si los datos del disco de los nodos del clúster se almacenan uniformemente, filtre los discos cuyos datos aumenten significativamente o sean insuficientes, y compruebe si los discos son normales.

Frecuencia de mantenimiento rutinario	Escenario de tareas	Elemento de comprobación
	Cambios de registro.	Organice y registre las operaciones en los parámetros y archivos de configuración del clúster para proporcionar una referencia para el análisis y el manejo de falla.
Mensual	Analizar los registros.	● Recopile y analice registros de hardware de servidores de nodos de clúster, como registros del sistema BMC. ● Recopile y analice los registros del sistema operativo de los servidores del nodo del clúster. ● Recopile y analice registros de clúster.
	Diagnosticar la red.	Analice el estado de salud de la red del clúster.
	Gestionar el hardware.	Compruebe el ambiente de la sala de equipos y limpie los dispositivos.

7.9 Gestión de registros

7.9.1 Acerca de los registros

Descripción del registro

Los registros de clúster de se almacenan en el directorio **/var/log/Bigdata**. En la siguiente tabla se enumeran los tipos de registro.

Tabla 7-58 Tipos de registro

Tipo de registro	Descripción
Registros de instalación	Los registros de instalación registran información sobre FusionInsight Manager, el clúster y la instalación de servicios para ayudar a los usuarios a localizar errores de instalación.
Registros de ejecución	Los registros de ejecución registran la información de la pista de ejecución, la información de depuración, los cambios de estado, los problemas potenciales y la información de error generada durante la ejecución de los servicios.

Tipo de registro	Descripción
Registros de auditoría	Los registros de auditoría registran información sobre las actividades de los usuarios y las instrucciones de operación, que se pueden utilizar para localizar las causas de errores en los eventos de seguridad y determinar quiénes son los responsables de estos errores.

En la siguiente tabla se enumeran los directorios de registro de.

Tabla 7-59 Directorios de registro

Directorio	Registro
/var/log/Bigdata/audit	Registro de auditoría de componentes.
/var/log/Bigdata/controller	Registro de script de recolección de registro. Registro de proceso de controller. Registro de monitoreo de controller.
/var/log/Bigdata/dbservice	Registro de DBService.
/var/log/Bigdata/flume	Registro de Flume.
/var/log/Bigdata/hbase	Registro de HBase.
/var/log/Bigdata/hdfs	Registro de HDFS.
/var/log/Bigdata/hive	Registro de Hive.
/var/log/Bigdata/hetuengine	Registro de HetuEngine.
/var/log/Bigdata/httpd	Registro de HTTPd.
/var/log/Bigdata/hue	Registro de Hue.
/var/log/Bigdata/kerberos	Registro de Kerberos.
/var/log/Bigdata/ldapclient	Registro de cliente de LDAP.
/var/log/Bigdata/ldapserver	Registro del servidor de LDAP.
/var/log/Bigdata/loader	Registro de Loader.
/var/log/Bigdata/logman	Registro de gestión de registro de scripts de Logman.
/var/log/Bigdata/mapreduce	Registro de MapReduce.
/var/log/Bigdata/nodeagent	Registro de NodeAgent.
/var/log/Bigdata/okerberos	Registro de Kerberos de OMS.
/var/log/Bigdata/oldapserver	Registro de LDAP de OMS.
/var/log/Bigdata/metric_agent	Archivo de registro de ejecución de MetricAgent.

Directorio	Registro
/var/log/Bigdata/omm	**oms**: registro de procesamiento de eventos complejos, registro de servicio de alarma, registro de HA, registro de gestión de autenticación y autorización y registro de ejecución de servicio de monitoreo del servidor OMM. **oma**: registro de instalación y registro de ejecución del agente OMM. **core**: registro de volcado generado cuando el agente OMM y el proceso HA están suspendidos.
/var/log/Bigdata/spark2x	Registro de Spark2x.
/var/log/Bigdata/sudo	Registro generado cuando el comando **sudo** es ejecutado por el usuario **omm**.
/var/log/Bigdata/timestamp	Registro de gestión de sincronización de tiempo.
/var/log/Bigdata/tomcat	Registro de Tomcat.
/var/log/Bigdata/watchdog	Registro de Watchdog.
/var/log/Bigdata/yarn	Registro de Yarn.
/var/log/Bigdata/zookeeper	Registro de ZooKeeper.
/var/log/Bigdata/oozie	Registro de Oozie.
/var/log/Bigdata/kafka	Registro de Kafka.
/var/log/Bigdata/storm	Registro de Storm.
/var/log/Bigdata/upgrade	Registro de actualización de OMS.
/var/log/Bigdata/update-service	Registro de servicio de actualización.

NOTA

Después de habilitar la función de instancia múltiple, si el administrador del sistema agrega varias instancias de servicio HBase, Hive y Spark, la descripción del registro, el nivel de registro y el formato de registro de las instancias de servicio recién agregadas son los mismos que los de los registros de servicio originales. Los registros de instancia de servicio se almacenan por separado en el directorio **/var/log/Bigdata/***servicenameN*. Los registros de auditoría de las instancias de servicio HBase y Hive se almacenan en el directorio **/var/log/Bigdata/audit/***servicenameN*. Por ejemplo, los registros de HBase1 se almacenan en los directorios **/var/log/Bigdata/hbase1** y **/var/log/Bigdata/audit/hbase1**.

Registros de instalación

Tabla 7-60 Registros de instalación

Registro de instalación	Descripción
Registro de configuración	Registra información sobre el proceso de configuración antes de la instalación.

Registro de instalación	Descripción
Registro de instalación de FusionInsight Manager	Registra información sobre la instalación de FusionInsight Manager de dos nodos.
Registro de instalación del clúster	Registra información sobre la instalación del clúster.

Registros de ejecución

Tabla 7-61 describe la información de ejecución registrada en los registros de ejecución.

Tabla 7-61 Información de ejecución

Registro de ejecución	Descripción
Registro de preparación de la instalación	Registra información sobre los preparativos para la instalación, como la información de operación de detección, configuración y retroalimentación.
Registro de inicio de proceso	Registra información sobre los comandos ejecutados durante el inicio del proceso.
Registro de excepciones de inicio de proceso	Registra información sobre excepciones durante el inicio del proceso, como errores de servicio dependientes y recursos insuficientes.
Registro de ejecución del proceso	Registra información sobre el proceso que ejecuta información de pista e información de depuración, como entradas y salidas de funciones, así como mensajes de interfaz de módulo cruzado.
Registro de excepción de ejecución de proceso	Registra los errores que causan errores de ejecución del proceso, por ejemplo, los objetos de entrada vacíos o errores de codificación o decodificación.
Registro de entorno en ejecución del proceso	Registra información sobre el entorno en ejecución del proceso, como el estado de los recursos y las variables de entorno.
Registro de script	Registra información sobre el proceso de ejecución del script.
Registro de recuperación de recursos	Registra información sobre el proceso de recuperación de recursos.
Registros de borrado de desinstalación	Registra información sobre las operaciones realizadas durante la desinstalación del servicio, como la eliminación de directorios y tiempo de ejecución.

Registros de auditoría

La información de auditoría registrada en los registros de auditoría incluye la información de auditoría de FusionInsight Manager y la información de auditoría de componentes.

Tabla 7-62 Información de auditoría de FusionInsight Manager

Tipo de operación	Operación
Gestión de usuarios	Crear un usuario. Modificar un usuario. Eliminar un usuario. Crear un grupo de usuarios. Modificar un grupo de usuarios. Eliminar un grupo. Agregar un rol. Cambiar los roles del usuario. Eliminar un rol. Cambiar una política de contraseñas. Cambiar una contraseña. Restablecer una contraseña. Iniciar sesión. Cerrar sesión. Desbloquear la pantalla. Descargar la credencial de autenticación. Operación no autorizada. Desbloquear una cuenta de usuario. Bloquear una cuenta de usuario. Bloquear la pantalla. Exportar un usuario. Exportar un grupo de usuarios. Exportar un rol.

Tipo de operación	Operación
Gestión de clúster	Iniciar un clúster. Detener un clúster. Reiniciar un clúster. Realizar un reinicio continuo de un clúster. Reiniciar todas las instancias caducadas. Guardar configuraciones. Sincronizar configuraciones de clúster. Personalizar las métricas de monitoreo de clústeres. Configurar volcado de monitoreo. Guardar umbrales de monitoreo. Descargar un archivo de configuración de cliente. Configurar interfaz de Syslog en dirección norte. Configurar interfaz de SNMP en dirección norte. Borrar alarmas mediante SNMP. Agregar un destino de trap mediante SNMP. Eliminar un destino de trap mediante SNMP. Comprobar alarmas mediante SNMP. Sincronizar alarmas mediante SNMP. Crear una plantilla de umbral. Eliminar una plantilla de umbral. Aplicar una plantilla de umbral. Guardar configuraciones de monitoreo de clústeres. Exportar configuraciones. Importar configuraciones de clúster. Exportar una plantilla de instalación. Modificar una plantilla de umbral. Cancelar la aplicación de una plantilla de umbral. Enmascarar una alarma. Enviar una alarma. Cambiar la contraseña de la base de datos de OMS. Restablecer la contraseña de la base de datos de componentes. Reiniciar OMM y Controller. Iniciar la comprobación de estado de un clúster. Importar un archivo de certificado. Configurar información de SSO. Eliminar informes históricos de comprobación de estado. Modificar propiedades del clúster.

Tipo de operación	Operación
	Ejecutar comandos de mantenimiento en modo síncrono. Ejecutar comandos de mantenimiento en modo asíncrono. Personalizar métricas de monitoreo de informes. Exportar datos de monitoreo de informes. Ejecutar un comando en modo asincrónico mediante SNMP. Reiniciar el servicio Web. Personalizar métricas de monitoreo para grupos de recursos estáticos. Exportar datos de monitoreo de un grupo de recursos estático. Personalizar métricas de monitoreo del panel de control. Detener una tarea. Restaurar configuraciones. Modificar configuraciones de dominio y confianza mutua. Modificar parámetros del sistema. Hacer que un clúster entre en el modo de mantenimiento. Hacer que un clúster salga del modo de mantenimiento. Hacer que OMS entre en el modo de mantenimiento. Hacer que OMS salga del modo de mantenimiento. Hacer que los servicios en un clúster salgan del modo de mantenimiento en lotes. Modificación de configuraciones de OMS. Habilitación de alarmas de umbral. Sincronización de todas las configuraciones de clúster.

Tipo de operación	Operación
Gestión de servicio	Iniciar un servicio. Detener un servicio. Sincronizar configuraciones de servicio. Refrescar una cola de servicio. Personalizar métricas de monitoreo de servicio. Reiniciar un servicio. Realizar un reinicio de servicio continuo. Exportar datos de monitoreo de servicio. Importar datos de configuración del servicio. Iniciar la comprobación de estado de un servicio. Configurar un servicio. Cargar un archivo de configuración. Descargar un archivo de configuración. Sincronizar configuraciones de instancia. Poner en marcha de una instancia. Desmantelar una instancia. Iniciar una instancia. Detener una instancia. Personalizar métricas de monitoreo de instancia. Reiniciar una instancia. Realizar un reinicio continuo de una instancia. Exportar datos de monitoreo de instancia. Importar datos de configuración de instancia. Crear un grupo de instancias. Modificar un grupo de instancias. Eliminar un grupo de instancias. Mover una instancia a otro grupo de instancias. Hacer que un servicio entre en el modo de mantenimiento. Hacer que un servicio salga del modo de mantenimiento. Cambiar el nombre de un servicio. Modificar la asociación de servicios. Descargar datos de monitoreo. Enmascarar alarmas. Desenmascarar alarmas. Exportar datos de informe de un servicio. Agregar parámetros personalizados para un informe. Modificar parámetros personalizados de un informe.

Tipo de operación	Operación
	Eliminar parámetros personalizados de un informe. Conmutar nodos de control. Agregar una tabla de montaje. Modificar una tabla de montaje.
Gestión de hosts	Configurar un rack de nodos. Comenzar todos los roles. Detener todos los roles. Aislar un host. Cancelar el aislamiento de un host. Personalizar las métricas de monitoreo de host. Exportar datos de monitoreo de host. Hacer que un host entre en el modo de mantenimiento. Hacer que un host salga del modo de mantenimiento. Exportar información básica del host. Exportar datos de informes de distribución de host. Exportar datos del informe de tendencias del host. Exportar datos de informes de clúster de host. Exportar datos de informe de un servicio. Personalizar las métricas de monitoreo de clústeres de host. Personalizar las métricas de monitoreo de tendencias de clústeres de host.
Gestión de alarmas	Exportar alarmas. Borrar alarmas. Exportar eventos. Borrar alarmas por lotes.
Recolección de registros	Recolección de archivos de registro. Descarga de archivos de registro. Recolección de información de pila de servicio. Recolección de información de pila de instancia. Preparación de la información de la pila de servicio. Preparación de la información de la pila de instancias. Borrar la información de la pila de servicio. Borrar la información de la pila de instancias.
Gestión de registros de auditoría	Modificar configuraciones de volcado de auditoría. Exportar registros de auditoría.

Tipo de operación	Operación
Copia de respaldo y restauración de datos	Creación de una tarea de copia de respaldo. Ejecución de una tarea de copia de respaldo. Ejecución de tareas de copia de respaldo en lotes. Detener una tarea de copia de respaldo. Eliminar una tarea de copia de respaldo. Modificación de una tarea de copia de respaldo. Bloquear una tarea de copia de respaldo. Desbloquear una tarea de copia de respaldo. Crear una tarea de restauración. Ejecución de una tarea de restauración. Detener una tarea de restauración. Reintentar una tarea de restauración. Eliminar una tarea de restauración.

Tipo de operación	Operación
Gestión de multitenant	Guardar configuraciones estáticas. Agregar un tenant. Eliminar un tenant. Asociar un servicio con un tenant. Eliminar un servicio de un tenant. Configurar recursos. Crear un recurso. Eliminar un recurso. Agregar un grupo de recurso. Modificar un grupo de recurso. Eliminar un grupo de recurso. Restaurar datos de tenant. Modificar configuraciones globales de un tenant. Modificación de las configuraciones de cola de un programador de capacidad. Modificación de las configuraciones de cola de un súper programador. Modificación de la distribución de recursos de un programador de capacidad. Borrar la distribución de recursos de un programador de capacidad. Modificación de la distribución de recursos de un súper programador. Borrar la distribución de recursos de un súper programador. Adición de un catálogo de recurso. Modificación de un catálogo de recursos. Eliminación de un catálogo de recursos. Personalización de las métricas de monitoreo de tenant.

Tipo de operación	Operación
Comprobación de estado	Iniciar la comprobación de estado de un clúster. Iniciar la comprobación de estado de un servicio. Iniciar la comprobación de estado de un host. Iniciar la comprobación de estado de OMS. Iniciar la comprobación de estado del sistema. Actualización de las configuraciones de comprobación de estado. Exportación de informes de comprobación de estado. Exportación de resultados de comprobación de estado de un clúster. Exportación de resultados de comprobación de estado de un servicio. Exportación de resultados de comprobación de estado de un host. Eliminación de informes históricos de comprobación de estado. Exportación de informes históricos de comprobación de estado. Descargar un informe de comprobación de estado.

Tabla 7-63 Información de auditoría de componentes

Registro de auditoría	Tipo de operación	Operación
Registro de auditoría de ClickHouse	Gestión de mantenimiento	Concesión de permisos. Revocación de permisos. Registro de autenticación e información de inicio de sesión.
	Operaciones del servicio	Creación de bases de datos o tablas. Insertar, eliminar, consultar y migrar datos.
Registro de auditoría de DBService	Gestión de mantenimiento	Realización de operaciones de restauración de copia de respaldo.

Registro de auditoría	Tipo de operación	Operación
Registro de auditoría de HBase	Sentencias del lenguaje de definición de datos (DDL)	Creación de una tabla. Eliminación de una tabla. Modificación de una tabla. Adición de una familia de columnas. Modificación de una familia de columnas. Eliminación de una familia de columnas. Habilitación de una tabla. Deshabilitación de una tabla. Modificación de la información del usuario. Cambio de una contraseña. Iniciar sesión.
	Sentencias de lenguaje de manipulación de datos (DML)	Poner datos (en las tablas **hbase:meta**, **_ctmeta_** y **hbase:acl**). Eliminar datos (de las tablas **hbase:meta**, **_ctmeta_** y **hbase:acl**). Comprobar y poner datos (en las tablas **hbase:meta**, **_ctmeta_** y **hbase:acl**). Comprobar y eliminar datos (de las tablas **hbase:meta**, **_ctmeta_** y **hbase:acl**).
	Control de permisos	Asignar permisos a un usuario. Cancelar la asignación de permisos.
Registro de auditoría de HDFS	Gestión de permisos	Gestión de permisos de acceso en archivos o carpetas. Gestión de información de propietario de archivos o carpetas.
	Operaciones de archivos	Crear una carpeta. Crear un archivo. Abrir un archivo. Adjuntar contenido del archivo. Cambiar el nombre de un archivo. Eliminar un archivo o carpeta. Configuración de la propiedad de tiempo de un archivo. Configuración del número de copias de archivos. Fusionar archivos. Comprobación del sistema de archivos. Vinculación a un archivo.

Registro de auditoría	Tipo de operación	Operación
Registro de auditoría de Hive	Operaciones de metadatos	Definición de metadatos, como la creación de bases de datos y tablas. Eliminar metadatos, como eliminar bases de datos y tablas. Modificar metadatos, como agregar columnas y cambiar el nombre de tablas. Importación y exportación de metadatos.
	Mantenimiento de datos	Cargar datos en una tabla. Inserción de datos en una tabla.
	Gestión de permisos	Crear o eliminar un rol. Otorgar/Recuperar roles. Conceder/Recuperar permisos.
Registro de auditoría de Hue	Iniciar servicio	Iniciar Hue.
	Operaciones del usuario	Iniciar sesión. Cerrar sesión.
	Operaciones de tareas	Crear una tarea. Modificar una tarea. Eliminar una tarea. Enviar una tarea. Guardar una tarea. Actualizar el estado de una tarea.
Registro de auditoría de KrbServer	Gestión de mantenimiento	Cambiar la contraseña de una cuenta de Kerberos. Adición de una cuenta de Kerberos. Eliminar una cuenta de Kerberos. Autenticación de usuarios.
Registro de auditoría de LdapServer	Gestión de mantenimiento	Agregar un usuario del sistema operativo. Agregar un grupo de usuarios. Incorporación de un usuario a un grupo de usuarios. Eliminar un usuario. Eliminar un grupo.
Registro de auditoría de Loader	Gestión de la seguridad	Iniciar sesión.
	Gestión de metadatos	Consultar información del conector. Consultar un marco de trabajo. Consultar información de paso.

Registro de auditoría	Tipo de operación	Operación
	Gestión de conexiones de origen de datos	Consulta de una conexión de origen de datos. Adición de una conexión de origen de datos. Actualización de una conexión de origen de datos. Eliminación de una conexión de origen de datos. Activación de una conexión de origen de datos. Deshabilitación de una conexión de origen de datos.
	Gestión de trabajo	Consultar un trabajo. Crear un trabajo. Actualizar un trabajo. Eliminar un trabajo. Activar un trabajo. Deshabilitar un trabajo. Consultar todos los registros de ejecución de un trabajo. Consultar el último registro de ejecución de un trabajo. Enviar un trabajo. Detener un trabajo.
Registro de auditoría de MapReduce	Ejecución de aplicación	Iniciar una solicitud de container. Detener una solicitud de container. Una vez completada una solicitud de container, el estado de la solicitud pasa a ser correcto. Una vez que se completa una solicitud de container, el estado de la solicitud pasa a ser fallido. Una vez completada una solicitud de container, el estado de la solicitud se suspende. Enviar una tarea. Finalizar una tarea.
Registro de auditoría de Oozie	Gestión de tareas	Enviar una tarea. Iniciar una tarea. Eliminar una tarea. Suspender una tarea. Reanudar una tarea. Ejecutar una tarea de nuevo.

Registro de auditoría	Tipo de operación	Operación
Registro de auditoría de Spark2x	Operaciones de metadatos	Definición de metadatos, como la creación de bases de datos y tablas. Eliminar metadatos, como eliminar bases de datos y tablas. Modificar metadatos, como agregar columnas y cambiar el nombre de tablas. Importación y exportación de metadatos.
	Mantenimiento de datos	Cargar datos en una tabla. Inserción de datos en una tabla.
Registro de auditoría de Storm	Operaciones de Nimbus	Enviar una topología. Detener una topología. Reasignar una topología. Desactivar una topología. Activar una topología.
	Operaciones de UI	Detener una topología. Reasignar una topología. Desactivar una topología. Activar una topología.
Registro de auditoría de Yarn	Envío de trabajos	Enviar un trabajo a una cola.
Registro de auditoría de ZooKeeper	Gestión de permisos	Establecer permisos de acceso a Znode.
	Operaciones de Znode	Creación de Znodes. Eliminación de Znodes. Configuración de los datos de Znode.
Registro de auditoría de HetuEngine	Gestión de trabajo	Adición de un origen de datos externo. Eliminación de un origen de datos externo. Modificación de un origen de datos externo. Creación de una instancia de cómputo. Iniciar una instancia de cómputo. Detener una instancia de cómputo. Eliminación de una instancia de cómputo. Consultar una instancia de cómputo. Modificación de configuraciones de instancia de cómputo.

Los registros de auditoría de FusionInsight Manager se almacenan en la base de datos. Puede ver y exportar los registros de auditoría en la página **Audit**.

En la siguiente tabla se enumeran los directorios para almacenar los registros de auditoría de componentes. Los archivos de registro de auditoría de algunos componentes se almacenan en **/var/log/Bigdata/audit**, como HDFS, HBase, MapReduce, Hive, Hue, Yarn, Storm, y ZooKeeper. Los registros de auditoría de componentes se comprimen y se copian automáticamente a **/var/log/Bigdata/audit/bk** a las 03:00 todos los días. Se conserva un máximo de 90 archivos de copia de respaldo comprimidos más recientes y no se puede cambiar el tiempo de copia de respaldo. Para obtener más información acerca de cómo configurar el número de archivos de registro de auditoría reservados, consulte **Configuración del número de copias de respaldo del registro de auditoría local**.

Los archivos de registro de auditoría de otros componentes se almacenan en el directorio de registro de componentes.

Tabla 7-64 Directorios para almacenar registros de auditoría de componentes

Componente	Directorio de registro de auditoría
DBService	/var/log/Bigdata/audit/dbservice/dbservice_audit.log
HBase	/var/log/Bigdata/audit/hbase/hm/hbase-audit-hmaster.log /var/log/Bigdata/audit/hbase/hm/hbase-ranger-audit-hmaster.log /var/log/Bigdata/audit/hbase/rs/hbase-audit-regionserver.log /var/log/Bigdata/audit/hbase/rs/hbase-ranger-audit-regionserver.log /var/log/Bigdata/audit/hbase/rt/hbase-audit-restserver.log /var/log/Bigdata/audit/hbase/ts/hbase-audit-thriftserver.log
HDFS	/var/log/Bigdata/audit/hdfs/nn/hdfs-audit-namenode.log /var/log/Bigdata/audit/hdfs/nn/ranger-plugin-audit.log /var/log/Bigdata/audit/hdfs/dn/hdfs-audit-datanode.log /var/log/Bigdata/audit/hdfs/jn/hdfs-audit-journalnode.log /var/log/Bigdata/audit/hdfs/zkfc/hdfs-audit-zkfc.log /var/log/Bigdata/audit/hdfs/httpfs/hdfs-audit-httpfs.log /var/log/Bigdata/audit/hdfs/router/hdfs-audit-router.log
HetuEngine	/var/log/Bigdata/audit/hetuengine/hsbroker/hsbroker-audit.log.0 /var/log/Bigdata/audit/hetuengine/hsconsole/hsconsole-audit.log.0 /var/log/Bigdata/audit/hetuengine/hsfabric/hsfabric-audit.log.0 hdfs://hacluster/hetuserverhistory/*Tenant name*/coordinator/application_*ID*/container_*ID*/*yyyyMMdd*/hetuserver-engine-audit.log hdfs://hacluster/hetuserverhistory/*Tenant name*/coordinator or worker/application_*ID*/container_*ID*/*yyyyMMdd*/server.log
Hive	/var/log/Bigdata/audit/hive/hiveserver/hive-audit.log /var/log/Bigdata/audit/hive/hiveserver/hive-rangeraudit.log /var/log/Bigdata/audit/hive/metastore/metastore-audit.log /var/log/Bigdata/audit/hive/webhcat/webhcat-audit.log

Componente	Directorio de registro de auditoría
Hue	/var/log/Bigdata/audit/hue/hue-audits.log
Kafka	/var/log/Bigdata/audit/kafka/audit.log
Loader	/var/log/Bigdata/loader/audit/default.audit
MapReduce	/var/log/Bigdata/audit/mapreduce/jobhistory/mapred-audit-jobhistory.log
Oozie	/var/log/Bigdata/audit/oozie/oozie-audit.log
Spark2x	/var/log/Bigdata/audit/spark2x/jdbcserver/jdbcserver-audit.log /var/log/Bigdata/audit/spark2x/jdbcserver/ranger-audit.log /var/log/Bigdata/audit/spark2x/jobhistory/jobhistory-audit.log
Storm	/var/log/Bigdata/audit/storm/logviewer/audit.log /var/log/Bigdata/audit/storm/nimbus/audit.log /var/log/Bigdata/audit/storm/supervisor/audit.log /var/log/Bigdata/audit/storm/ui/audit.log
Yarn	/var/log/Bigdata/audit/yarn/rm/yarn-audit-resourcemanager.log /var/log/Bigdata/audit/yarn/rm/ranger-plugin-audit.log /var/log/Bigdata/audit/yarn/nm/yarn-audit-nodemanager.log
ZooKeeper	/var/log/Bigdata/audit/zookeeper/quorumpeer/zk-audit-quorumpeer.log

7.9.2 Lista de registros de Manager

Descripción del registro

Log path: La ruta de almacenamiento predeterminada de los archivos de registro de Manager es **/var/log/Bigdata/***Manager component*.

- ControllerService: **/var/log/Bigdata/controller/** (registros de instalación y ejecución de OMS)
- HTTPd: **/var/log/Bigdata/httpd** (registros de instalación y ejecución de HTTPd)
- Logman: **/var/log/Bigdata/logman** (registros de la herramienta de empaquetado de registros)
- NodeAgent: **/var/log/Bigdata/NodeAgent** (registros de instalación y ejecución de NodeAgent)
- okerberos: **/var/log/Bigdata/okerberos** (registros de instalación y ejecución de okerberos)
- oldapserver: **/var/log/Bigdata/oldapserver** (registros de instalación y ejecución de oldapserver)
- MetricAgent: **/var/log/Bigdata/metric_agent** (registros de ejecución de MetricAgent)
- OMM: **/var/log/Bigdata/omm** (registros de ejecución de OMM)

- Timestamp: **/var/log/Bigdata/timestamp** (registros de tiempo de inicio de NodeAgent)
- Tomcat: **/var/log/Bigdata/tomcat** (registros de procesos de web)
- Watchdog: **/var/log/Bigdata/watchdog** (registros de watchdog)
- Upgrade: **/var/log/Bigdata/upgrade** (registros de actualización de OMS)
- UpdateService: **/var/log/Bigdata/update-service** (registros de servicio de actualización)
- Sudo: **/var/log/Bigdata/sudo** (registros de ejecución de script de sudo)
- OS: **/var/log/***message file* (registros de sistema de OS)
- OS performance: **/var/log/osperf** (registros de estadísticas de rendimiento de OS)
- OS statistics: **/var/log/osinfo/statistics** (registros de configuración de parámetro de OS)

Regla de archivado de registro:

La función de compresión y archivado automáticos está habilitada para los registros de Manager. De forma predeterminada, cuando el tamaño de un archivo de registro supera los 10 MB, el archivo de registro se comprime automáticamente. La regla de denominación de un archivo de registro comprimido es la siguiente: <*Original log name*>-<*yyyy-mm-dd_hh-mm-ss*>.[*ID*].**log.zip** Un máximo de 20 más recientes se conservan los archivos comprimidos.

Tabla 7-65 Registros de Manager

Tipo de registro	Nombre de archivo de registro	Descripción
Registros de ejecución de Controller	controller.log	Archivo de registro que registra la instalación de componentes, la actualización, la configuración, el monitoreo, los informes de alarmas y las operaciones de O&M rutinaria
	controller_client.log	Archivo de registro de ejecución de API de Transferencia de Estado Representacional (REST)
	acs.log	Archivo de registro de ejecución de ACS
	acs_spnego.log	Registros de usuario de spnego en ACS
	aos.log	Archivo de registro de ejecución de AOS
	plugin.log	Registros de complemento de AOS
	backupplugin.log	Archivo de registro de ejecución que registra las operaciones de copia de respaldo y restauración

Tipo de registro	Nombre de archivo de registro	Descripción
	controller_config.log	Archivo de registro de ejecución de configuración
	controller_nodesetup.log	Archivo de registro de tarea de carga de Controller
	controller_root.log	Archivo de registro del sistema del proceso Controller
	controller_trace.log	Archivo de registro que registra la comunicación de llamada a procedimiento remoto (RPC) entre el Controller y NodeAgent
	controller_monitor.log	Archivo de registro de monitoreo
	controller_fsm.log	Archivo de registro de máquina de estado
	controller_alarm.log	Archivo de registro de alarma de Controller
	controller_backup.log	Copia de respaldo del Controller y archivo de registro de recuperación
	install.log, restore_package.log, installPack.log, distributeAdapterFiles.log, and install_os_optimization.log	Archivo de registro de instalación de OMS
	oms_ctl.log	Archivo de registro de inicio y detención de OMS
	preInstall_client.log	Preprocesamiento del archivo de registro antes de la instalación del cliente
	installntp.log	Archivo de registro de instalación de NTP
	modify_manager_param.log	Archivo de registro de modificación de parámetros de Manager
	backup.log	Archivo de registro de ejecución del script de copia de respaldo de OMS

Tipo de registro	Nombre de archivo de registro	Descripción
	supressionAlarm.log	Archivo de registro de ejecución de script de alarma
	om.log	Archivo de registro de generación de certificados de OM
	backupplugin_ctl.log	Archivo de registro de inicio del proceso de complemento de copia de respaldo y restauración
	getLogs.log	Registro de ejecución de script de recolección de registro
	backupAuditLogs.log	Registro de ejecución de script de copia de respaldo de registro de auditoría
	certStatus.log	Archivo de registro que registra comprobaciones de certificados regulares
	distribute.log	Registro de distribución de certificados
	ficertgenetrate.log	Archivo de registro de reemplazo de certificados, que cubre certificados de nivel 2, certificados CAS y certificados HTTPd
	genPwFile.log	Archivo de registro que registra la generación de archivos de contraseña de certificado
	modifyproxyconf.log	Archivo de registro que registra la modificación de la configuración de proxy de HTTPd
	importTar.log	Archivo de registro que registra el proceso de importación de certificados en el almacén de confianza.
HTTPd	install.log	Archivo de registro de instalación de HTTPd

Tipo de registro	Nombre de archivo de registro	Descripción
	access_log, error_log	Archivo de registro de ejecución de HTTPd
Logman	logman.log	Archivo de registro de la herramienta de empaquetado de registros
NodeAgent	install.log and install_os_optimization.log	Archivo de registro de instalación de NodeAgent
	installntp.log	Archivo de registro de instalación de NTP
	start_ntp.log	Archivo de registro de inicio de NTP
	ntpChecker.log	Archivo de registro de comprobación de NTP
	ntpMonitor.log	Archivo de registro de monitoreo de NTP
	heartbeat_trace.log	Archivo de registro que registra los latidos entre NodeAgent y Controller
	alarm.log	Archivo de registro de alarma
	monitor.log	Archivo de registro de monitoreo
	nodeagent_ctl.log and start-agent.log	Archivo de registro de inicio de NodeAgent
	agent.log	Archivo de registro de ejecución de NodeAgent
	cert.log	Archivo de registro de certificados
	agentplugin.log	Archivo de registro que registra el estado de ejecución del complemento del agente
	omaplugin.log	Archivo de registro de ejecución del complemento OMA
	diskhealth.log	Archivo de registro de comprobación de estado del disco

Tipo de registro	Nombre de archivo de registro	Descripción
	supressionAlarm.log	Archivo de registro de ejecución de script de alarma
	updateHostFile.log	Archivo de registro de actualización de lista de hosts
	collectLog.log	Archivo de registro de ejecución de script de recolección de registro de nodo
	host_metric_collect.log	Archivo de registro de ejecución de recolección de métrica de host
	checkfileconfig.log	Archivo de registro de ejecución de comprobación de permiso de archivo
	entropycheck.log	Archivo de registro de ejecución de comprobación de entropía
	timer.log	Archivo de registro de programación de nodos programados
	pluginmonitor.log	Archivo de registro de complemento de monitoreo de componentes
	agent_alarm_py.log	Archivo de registro que registra alarmas si el permiso de archivo NodeAgent no es suficiente
oKerberos	addRealm.log and modifyKerberosRealm.log	Archivo de registro de traspaso de dominio kerberos
	checkservice_detail.log	Archivo de registro de comprobación de salud de Okerberos
	genKeytab.log	Archivo de registro de generación de keytab
	KerberosAdmin_genConfigDetail.log	Archivo de registro de ejecución de **kadmin.conf** generado durante el inicio del proceso kadmin

Tipo de registro	Nombre de archivo de registro	Descripción
	KerberosServer_genConfigDetail.log	Archivo de registro de ejecución de **krb5kdc.conf** generado durante el inicio del proceso krb5kdc
	oms-kadmind.log	Archivo de registro de ejecución del proceso kadmin
	oms_kerberos_install.log and postinstall_detail.log	Archivo de registro de instalación de Okerberos
	oms-krb5kdc.log	Archivo de registro de ejecución del proceso krbkdc
	start_detail.log	Archivo de registro de inicio de Okerberos
	realmDataConfigProcess.log	Archivo de registro que registra la reversión tras un error de traspaso de dominio kerberos
	stop_detail.log	Archivo de registro de detención de Okerberos
oldapserver	ldapserver_backup.log	Archivo de registro de copia de respaldo de Oldapserver
	ldapserver_chk_service.log	Archivo de registro de comprobación de estado de Oldapserver
	ldapserver_install.log	Archivo de registro de instalación de Oldapserver
	ldapserver_start.log	Archivo de registro de inicio de Oldapserver
	ldapserver_status.log	Archivo de registro que registra el estado del proceso Oldapserver
	ldapserver_stop.log	Archivo de registro de detención de Oldapserver
	ldapserver_wrap.log	Archivo de registro de gestión de servicio Oldapserver

Tipo de registro	Nombre de archivo de registro	Descripción
	ldapserver_uninstall.log	Archivo de registro de desinstalación de Oldapserver
	restart_service.log	Archivo de registro de reinicio de Oldapserver
	ldapserver_unlockUser.log	Archivo de registro que registra información sobre el desbloqueo de usuarios de LDAP y la gestión de cuentas
metric_agent	gc.log	Archivo de registro de JVM GC de MetricAgent
	metric_agent.log	Archivo de registro de ejecución de MetricAgent
	metric_agent_qps.log	Archivo de registro que registra longitud de la cola interna de MetricAgent e información de QPS
	metric_agent_root.log	Todos los archivos de registro de ejecución de MetricAgent
	start.log	Archivo de registro que registra información sobre el inicio y la detención de MetricAgent
OMM	omsconfig.log	Archivo de registro de configuración de OMS
	check_oms_heartbeat.log	Archivo de registro de latidos de OMS
	monitor.log	Archivo de registro de monitoreo de OMS
	ha_monitor.log	Archivo de registro de operaciones de HA_Monitor
	ha.log	Archivo de registro de operación HA
	fms.log	Archivo de registro de alarma
	fms_ha.log	Archivo de registro de monitoreo de alarma HA

Tipo de registro	Nombre de archivo de registro	Descripción
	fms_script.log	Archivo de registro de control de alarma
	config.log	Archivo de registro de configuración de alarma
	iam.log	Archivo de registro de IAM
	iam_script.log	Archivo de registro de control de IAM
	iam_ha.log	Archivo de registro de monitoreo de IAM HA
	config.log	Archivo de registro de configuración de IAM
	operatelog.log	Archivo de registro de operaciones de IAM
	heartbeatcheck_ha.log	Archivo de registro de monitoreo de HA de latidos del corazón de OMS
	install_oms.log	Archivo de registro de instalación de OMS
	pms_ha.log	Archivo de registro de monitoreo de HA
	pms_script.log	Archivo de registro de control de monitoreo
	config.log	Archivo de registro de configuración de monitoreo
	plugin.log	Archivo de registro de ejecución del complemento de monitoreo
	pms.log	Archivo de registro de monitoreo
	ha.log	Archivo de registro de ejecución de HA
	cep_ha.log	Archivo de registro de monitoreo CEP HA
	cep_script.log	Archivo de registro de control CEP
	cep.log	Archivo de registro CEP

Tipo de registro	Nombre de archivo de registro	Descripción
	config.log	Archivo de registro de configuración CEP
	omm_gaussdba.log	Archivo de registro de monitoreo de GaussDB HA
	gaussdb-<SERIAL>.log	Archivo de registro de ejecución de GaussDB
	gs_ctl-<DATE>.log	Archivo de registro de archivos de registros de control de GaussDB
	gs_ctl-current.log	Archivo de registro de control de GaussDB
	gs_guc-current.log	Archivo de registro de operaciones de GaussDB
	encrypt.log	Archivo de registro de encriptación de OMM
	omm_agent_ctl.log	Archivo de registro de control de OMA
	oma_monitor.log	Archivo de registro de monitoreo de OMA
	install_oma.log	Archivo de registro de instalación de OMA
	config_oma.log	Archivo de registro de configuración de OMA
	omm_agent.log	Archivo de registro de ejecución de OMA
	acs.log	Archivo de registro de recursos ACS
	aos.log	Archivo de registro de recursos AOS
	controller.log	Archivo de registro de recursos del Controller
	floatip.log	Archivo de registro de recursos de dirección IP flotante
	ha_ntp.log	Archivo de registro de recursos NTP
	httpd.log	Archivo de registro de recursos HTTPd

Tipo de registro	Nombre de archivo de registro	Descripción
	okerberos.log	Archivo de registro de recursos de Okerberos
	oldap.log	Archivo de registro de recursos de OLdap
	tomcat.log	Archivo de registro de recursos de Tomcat
	send_alarm.log	Archivo de registro de ejecución del script de envío de alarma HA de nodo de gestión
	feed_watchdog.log	registro de recurso de feed_watchdog
Timestamp	restart_stamp	Archivo de registro de tiempo de inicio de NodeAgent
Tomcat	cas.log and localhost_access_cas_log.log	Archivo de registro de ejecución de CAS
	catalina.log, catalina.out, host-manager.log, localhost.log, and manager.log	Archivo de registro de ejecución de Tomcat
	localhost_access_web_log.log	Archivo de registro que registra el acceso a las API de REST de FusionInsight Manager
	web.log	Archivo de registro de ejecución de proceso Web
	northbound_ftp_sftp.log and snmp.log	Archivo de registro en dirección norte
	perfStats.log	Archivo de registro de estadísticas de rendimiento
Watchdog	watchdog.log and feed_watchdog.log	Archivo de registro de ejecución de watchdog.log
update-service	omm_upd_server.log	Archivo de registro de ejecución de UPDServer
	omm_upd_agent.log	Archivo de registro de ejecución de UPDAgent
	update-manager.log	Archivo de registro de ejecución de UPDManager

Tipo de registro	Nombre de archivo de registro	Descripción
	install.log	Archivo de registro de instalación del servicio de actualización
	uninstall.log	Archivo de registro de desinstalación del servicio de actualización
	catalina.<*Time*>.log, catalina.out, host-manager.<*Time*>.log, localhost.<*Time*>.log, manager.<*Time*>.log, manager_access_log.<*Time*>.txt, web_service_access_log.<*Time*>.txt, catalina.log, gc-update-service.log.0.current, update-manager.controller, update-web-service.controller, update-web-service.log, commit_rm_distributed.log, commit_rm_upload_package.log, common_omagent_operator.log, forbid_monitor.log, initialize_package_atoms.log, initialize_unzip_pack.log, omm-upd.log, register_patch_pack.log, resume_monitor.logrollback_clear_patch.log, unregister_patch_pack.log, update-rcommupd.log, update-rcupdatemanager.log, and update-service.log	Archivo de registro de ejecución del servicio de actualización
Upgrade	upgrade.log_<*Time*>	Archivo de registro de actualización de OMS
	rollback.log_<*Time*>	Archivo de registro de rollback de OMS
sudo	sudo.log	Archivo de registro de ejecución de script Sudo

Niveles de registro

Tabla 7-66 describe los niveles de registro proporcionados por Manager. Los niveles de registro son FATAL, ERROR, WARN, INFO y DEBUG en orden descendente. Los registros

cuyos niveles son superiores o iguales al nivel establecido son impresos por el programa. El número de registros impresos disminuye a medida que aumenta el nivel de registro establecido.

Tabla 7-66 Niveles de registro

Nivel	Descripción
FATAL	Los registros de este nivel registran información de error fatal sobre el procesamiento de eventos actuales que puede provocar un bloqueo del sistema.
ERROR	Los registros de este nivel registran información de error sobre el procesamiento de eventos actual, lo que indica que el funcionamiento del sistema es anormal.
WARN	Los registros de este nivel registran información anormal sobre el procesamiento del evento actual. Estas anomalías no darán lugar a fallas del sistema.
INFO	Los registros de este nivel registran información de estado de ejecución normal sobre el sistema y los eventos.
DEBUG	Los registros de este nivel registran la información del sistema y la información de depuración.

Formatos de registro

En la siguiente tabla se muestran los formatos de registro de Manager.

Tabla 7-67 Formatos de registro

Tipo de registro	Componente	Formato	Ejemplo
Controller, HTTPd, Logman, NodeAgent, oKerberos, oldapserver, OMM, Tomcat, and upgrade	Controller, HTTPd, Logman, NodeAgent, oKerberos, oldapserver, OMM, Tomcat, and upgrade	<yyyy-MM-dd HH:mm:ss, SSS>|<Log Level>|<*Name of the thread for which the log is generated*>|<*Log message*>|<*Location where the log event occurs*>	2020-06-30 00:37:09,067 INFO [pool-1-thread-1] Completed Discovering Node. com.xxx.hadoop.om .controller.tasks.nod esetup.DiscoverNod eTask.execute(Disco verNodeTask.java:2 99)

7.9.3 Configuración del nivel de registro y el tamaño del archivo de registro

Escenario

Puede cambiar los niveles de registro del FusionInsight Manager. Para un servicio específico, puede cambiar el nivel de registro y el tamaño del archivo de registro para evitar que se produzca un error al guardar registros debido a la falta de espacio en disco.

Impacto en el sistema

Es necesario reiniciar los servicios para que la nueva configuración entre en vigor. Durante el reinicio, los servicios no están disponibles.

Cambio del nivel de registro del FusionInsight Manager

1. Inicie sesión en el nodo de gestión activo como usuario **omm**.
2. Ejecute el siguiente comando para cambiar al directorio requerido:

   cd ${BIGDATA_HOME}/om-server/om/sbin
3. Ejecute el siguiente comando para cambiar el nivel de registro:

   ./setLogLevel.sh*Log level parameters*

   Las prioridades de los niveles de registro son FATAL, ERROR, WARN, INFO y DEBUG en orden descendente. Se imprimen los registros cuyos niveles sean superiores o iguales al nivel establecido. El número de registros impresos disminuye a medida que aumenta el nivel de registro configurado.

   - **DEFAULT**: Después de establecer este parámetro, se utiliza el nivel de registro predeterminado.
   - **FATAL**: Nivel de registro de errores críticos. Después de establecer este parámetro, sólo se imprimen registros del nivel **FATAL**.
   - **ERROR**: Nivel de registro de errores. Después de establecer este parámetro, se imprimen registros de los niveles **ERROR** y **FATAL**.
   - **WARN**: Nivel de registro de advertencias. Después de establecer este parámetro, se imprimen los registros de los niveles **WARN**, **ERROR** y **FATAL**.
   - **INFO** (predeterminado): Nivel de registro informativo. Después de establecer este parámetro, se imprimen los registros de los niveles **INFO**, **WARN**, **ERROR** y **FATAL**.
   - **DEBUG**: nivel de registro de depuración. Después de establecer este parámetro, se imprimen los registros de los niveles **DEBUG**, **INFO**, **WARN**, **ERROR** y **FATAL**.
   - **TRACE**: Nivel de registro de seguimiento. Después de establecer este parámetro, se imprimen los registros de los niveles **TRACE**, **DEBUG**, **INFO**, **WARN**, **ERROR** y **FATAL**.

   NOTA

   Los niveles de registro de los componentes son diferentes de los definidos en el código de código abierto.
4. Descargue y vea registros para verificar que la configuración del nivel de registro haya tenido efecto. Para obtener más información, consulte **Registro**.

Cambio del nivel de registro de servicio y del tamaño del archivo de registro

NOTA

KrbServer, LdapServer y DBService no admiten el cambio de niveles de registro de servicio y tamaños de archivo de registro.

Paso 1 Inicie sesión en FusionInsight Manager.

Paso 2 Elija **Cluster** >*Name of the desired cluster* >**Services**.

Paso 3 Haga clic en un servicio en la lista de servicios. En la página mostrada, haga clic en la página **Configuration**.

Paso 4 En la página mostrada, haga clic en la pestaña **All Configuration**. Expanda la instancia de rol que se muestra a la izquierda de la página. Haga clic en **Log** del rol que se va a modificar.

Paso 5 Busque cada parámetro y obtenga la descripción del parámetro. En la página de configuración de parámetros, seleccione el nivel de registro requerido o cambie el tamaño del archivo de registro. La unidad del tamaño del archivo de registro es MB.

AVISO

- El sistema elimina automáticamente los registros según el tamaño de registro configurado. Para guardar más información, establezca el tamaño del archivo de registro en un valor mayor. Para garantizar la integridad de los archivos de registro, se recomienda realizar una copia de respaldo manual de los archivos de registro en otro directorio basado en el volumen de servicio real antes de que los archivos de registro se borren de acuerdo con las reglas de autorización.
- Algunos servicios no admiten el cambio del nivel de registro en la interfaz de usuario.

Paso 6 Haga clic en **Save**. En el cuadro de diálogo **Save Configuration**, haga clic en **OK**.

Paso 7 Descargue y vea registros para verificar que la configuración del nivel de registro haya tenido efecto.

----Fin

7.9.4 Configuración del número de copias de respaldo del registro de auditoría local

Escenario

Los registros de auditoría de los componentes del clúster se clasifican por nombre y se almacenan en el directorio **/var/log/Bigdata/audit** de cada nodo del clúster. El OMS realiza automáticamente una copia de respaldo de los directorios del registro de auditoría a las 03:00 todos los días.

El directorio de registro de auditoría en cada nodo se comprime y se nombra en el formato *<Node IP address>***.tar.gz**. Todos los archivos comprimidos se comprimen y nombran en el formato *<yyyy-MM-dd_HH-mm-ss>***.tar.gz** y se guardan en el directorio **/var/log/Bigdata/audit/bk/** en el nodo de gestión activa. Además, el nodo de gestión en espera guarda una copia del archivo.

De forma predeterminada, se puede conservar un máximo de 90 archivos de copia de respaldo de OMS. Esta sección describe cómo configurar el número máximo.

Procedimiento

Paso 1 Inicie sesión en el nodo de gestión activo como usuario **omm**.

NOTA

Realice esta operación sólo en el nodo de gestión activo. Esta operación no se admite en los nodos de gestión en espera; de lo contrario, el clúster no puede funcionar correctamente.

Paso 2 Ejecute el siguiente comando para cambiar al directorio requerido:

cd ${BIGDATA_HOME}/om-server/om/sbin

Paso 3 Ejecute el siguiente comando para cambiar el número máximo de archivos de copia de respaldo del registro de auditoría que se conservarán:

./modifyLogConfig.sh -m ***Maximum number of backup files that can be retained***

El valor predeterminado es **90**. El valor oscila entre **0** y **365**. Un valor mayor significa consumir más espacio en disco.

Si se muestra la siguiente información, la operación se realiza correctamente:

```
Modify log config successfully
```

----Fin

7.9.5 Consulta de registros de instancias de rol

Escenario

FusionInsight Manager permite a los usuarios ver los registros de cada instancia de rol.

Procedimiento

Paso 1 Inicie sesión en FusionInsight Manager.

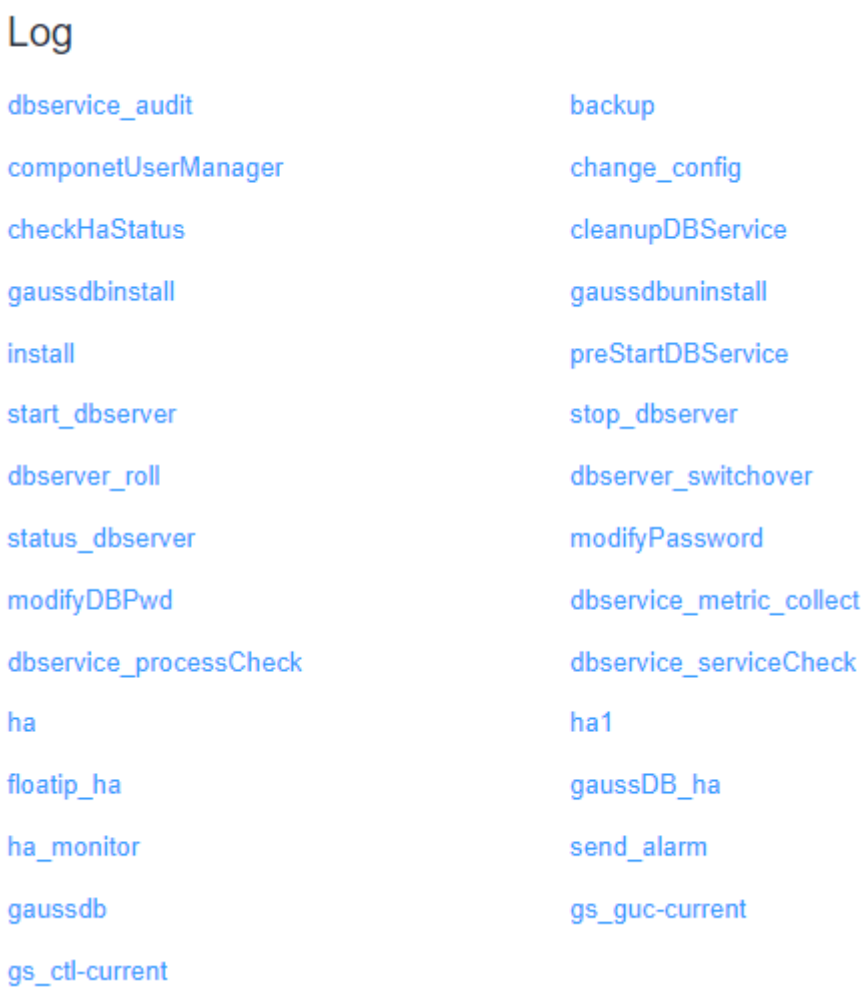
Paso 2 Elija **Cluster**, haga clic en el nombre del clúster deseado, elija **Services** y haga clic en un nombre de servicio. A continuación, haga clic en la pestaña **Instance** del servicio y haga clic en el nombre de la instancia de destino para acceder a la página de estado de la instancia.

Paso 3 En el área **Log**, haga clic en el nombre de un archivo de registro para obtener una vista previa de su contenido en línea.

NOTA

- En la página **Hosts**, haga clic en un nombre de host. En la lista de instancias del host, puede ver los archivos de registro de todas las instancias de rol del host.
- Por defecto, se puede mostrar un máximo de 100 líneas de registros. Puede hacer clic en **Load More** para ver más registros. Haga clic en **Download** para descargar el archivo de registro en el PC local. Para obtener más información acerca de cómo descargar los registros de servicio en lotes, consulte **Descarga de registro**.

Figura 7-57 Consulta de registros de instancia



----Fin

7.10 Copia de respaldo y gestión de recuperación

7.10.1 Introducción

Descripción

FusionInsight Manager proporciona la copia de respaldo y la restauración de los datos del sistema y de los datos del usuario por componente. El sistema puede hacer copias de respaldo de los datos de Manager, los metadatos de los componentes y los datos de servicio.

Los datos se pueden hacer copias de respaldo en discos locales (LocalDir), HDFS locales (LocalHDFS), HDFS remotos (RemoteHDFS), NAS (NFS/CIFS), Object Storage Service (OBS), y SFTP server (SFTP). Para obtener más información, consulte **Copia de respaldo de datos**.

Para un componente que admite varios servicios, se pueden realizar copias de respaldo y restaurar varias instancias de un servicio. Las operaciones de copia de respaldo y restauración son coherentes con las de una instancia de servicio.

NOTA

Solo MRS 3.1.0 o posterior admite la copia de respaldo de datos en OBS.

Las tareas de copia de respaldo y restauración se realizan en los siguientes escenarios:

- La copia de respaldo de rutina se realiza para garantizar la seguridad de los datos del sistema y los componentes.
- Si el sistema está defectuoso, la copia de respaldo de datos se puede utilizar para recuperar el sistema.
- Si el clúster activo es completamente defectuoso, es necesario crear un clúster reflejado idéntico al clúster activo. Puede utilizar los datos de copia de respaldo para restaurar el clúster activo.

Tabla 7-68 Datos de configuración del Manager que se van a realizar copias de respaldo

Tipo de copia de respaldo	Contenido de la copia de respaldo	Tipo de directorio de copia de respaldo
OMS	Datos de base de datos (excluidos los datos de alarma) y datos de configuración en el sistema de gestión de clústeres de forma predeterminada	● LocalDir ● LocalHDFS ● RemoteHDFS ● NFS ● CIFS ● SFTP ● OBS

Tabla 7-69 Metadatos de componentes u otros datos que se van a realizar copias de respaldo

Tipo de copia de respaldo	Contenido de la copia de respaldo	Tipo de directorio de copia de respaldo
DBService	Metadatos de los componentes (incluidos Loader, Hive, Spark, Oozie, y Hue) gestionado por DBService. Para un clúster con varios servicios instalados, realice una copia de respaldo de los metadatos de varias instancias de servicio de Hive y Spark.	● LocalDir ● LocalHDFS ● RemoteHDFS ● NFS ● CIFS ● SFTP ● OBS

Tipo de copia de respaldo	Contenido de la copia de respaldo	Tipo de directorio de copia de respaldo
Flink (Aplicable a MRS 3.2.0 y versiones posteriores)	Metadatos de Flink.	● LocalDir ● LocalHDFS ● RemoteHDFS
Kafka	Metadatos de Kafka.	● LocalDir ● LocalHDFS ● RemoteHDFS ● NFS ● CIFS ● OBS
NameNode	Metadatos de HDFS. Después de agregar múltiples NameServices, se admiten copias de respaldo y restauración para todos ellos y las operaciones son consistentes con las de la instancia de hacluster predeterminada.	● LocalDir ● RemoteHDFS ● NFS ● CIFS ● SFTP ● OBS
Yarn	Información sobre el grupo de recursos del servicio Yarn.	
HBase	Archivos **tableinfo** y archivos de datos de tablas del sistema HBase.	
ClickHouse	Metadatos de ClickHouse.	● LocalDir ● RemoteHDFS

Tabla 7-70 Datos de servicio de componentes específicos que se van a realizar copias de respaldo

Tipo de copia de respaldo	Contenido de la copia de respaldo	Tipo de directorio de copia de respaldo
HBase	Datos de usuario a nivel de tabla. Para un clúster con varios servicios instalados, la copia de respaldo y la restauración son compatibles con varias instancias de servicio de HBase y las operaciones de copia de respaldo y restauración son consistentes con las de una sola instancia de servicio de HBase.	● RemoteHDFS ● NFS ● CIFS ● SFTP

Tipo de copia de respaldo	Contenido de la copia de respaldo	Tipo de directorio de copia de respaldo
HDFS	Directorios o archivos de servicios de usuario. **NOTA** Los directorios cifrados no se pueden hacer copias de respaldo ni restaurar.	
Hive	Datos de usuario a nivel de tabla. Para un clúster con varios servicios instalados, se admiten copias de respaldo y restauración para varias instancias de servicio de Hive y las operaciones de copia de respaldo y restauración son coherentes con las de una sola instancia de servicio de Hive.	
ClickHouse	Datos de usuario a nivel de tabla.	● RemoteHDFS

Tenga en cuenta que algunos componentes no proporcionan copia de respaldo o restauración de datos:

- Kafka admite réplicas y permite especificar varias réplicas cuando se crea un tema.
- Los datos de MapReduce y Yarn se almacenan en HDFS. Por lo tanto, se basan en la copia de respaldo y restauración proporcionada por HDFS.
- Las copias de respaldo y la restauración de los datos de servicio de ZooKeeper se realizan mediante sus propios componentes de capa superior.

Principios

Tarea

Antes de realizar una copia de respaldo o restauración, debe crear una tarea de copia de respaldo o restauración y establecer parámetros de tarea, como el nombre de la tarea, el origen de datos de copia de respaldo y el tipo del directorio para almacenar los archivos de copia de respaldo. A continuación, puede ejecutar las tareas para realizar una copia de respaldo o restaurar los datos. Cuando se utiliza Manager para restaurar los datos de HDFS, HBase, Hive y NameNode, no se puede acceder al clúster.

Cada tarea de copia de respaldo puede realizar copias de respaldo de datos de diferentes orígenes de datos y generar un archivo de copia de respaldo independiente para cada origen de datos. Todos los archivos de copia de respaldo generados en una tarea de copia de respaldo forman un conjunto de archivos de copia de respaldo, que se pueden utilizar en tareas de restauración. Los datos de copia de respaldo se pueden almacenar en discos locales de Linux, HDFS de clúster local y HDFS de clúster en espera.

Las tareas de copia de respaldo admiten políticas de copia de respaldo completas e incrementales. Las tareas de copia de respaldo de datos en la nube no admiten copias de respaldo incrementales. Si el tipo de directorio de copia de respaldo es NFS o CIFS, no se recomienda realizar una copia de respaldo incremental. Cuando se utiliza la copia de respaldo

incremental para la copia de respaldo de NFS o CIFS, los datos de copia de respaldo completa más recientes se actualizan cada vez que se realiza la copia de respaldo incremental. Por lo tanto, no se genera ningún nuevo punto de recuperación.

> **NOTA**
>
> Reglas de ejecución de tareas:
>
> - Si se está ejecutando una tarea, la tarea no se puede ejecutar repetidamente y otras tareas no se pueden iniciar al mismo tiempo.
> - El intervalo en el que se ejecuta automáticamente una tarea periódica debe ser superior a 120 segundos. De lo contrario, la tarea se pospone y se ejecutará en el próximo período. Las tareas manuales se pueden ejecutar en cualquier intervalo.
> - Cuando se va a ejecutar automáticamente una tarea periódica, la hora actual no puede ser 120 segundos más tarde que la hora de inicio de la tarea. De lo contrario, la tarea se pospone y se ejecuta en el siguiente período.
> - Cuando se bloquea una tarea periódica, no se puede ejecutar automáticamente y es necesario desbloquearla manualmente.
> - Antes de que se inicie una tarea de copia de respaldo de OMS, DBService, Kafka o NameNode, asegúrese de que la partición LocalBackup del nodo de gestión activo no tenga menos de 20 GB de espacio disponible. De lo contrario, no se puede iniciar la tarea de copia de respaldo.

Cuando planifique las tareas de copia de respaldo y restauración, seleccione los datos que se van a hacer copia de respaldo o restaurar estrictamente en función de la lógica del servicio, la estructura del almacén de datos y la asociación de bases de datos o tablas. De forma predeterminada, el sistema crea tareas de copia de respaldo periódicas **default-oms** y **default-*cluster ID*** en un intervalo de una hora. Los metadatos de OMS y los metadatos de clúster, como DBService y NameNode, se pueden realizar copias de respaldo completas en discos locales.

Instantánea

El sistema utiliza la tecnología de instantáneas para realizar rápidamente copias de respaldo de los datos. Las instantáneas incluyen instantáneas de HBase y HDFS.

- Instantáneas de HBase

  Una instantánea de HBase es un archivo de copia de respaldo de tablas de HBase en un punto de tiempo especificado. Este archivo de copia de respaldo no replica datos de servicio ni afecta al RegionServer. La instantánea de HBase replica metadatos de tabla, incluidos descriptor de tabla, información de región e información de referencia de HFile. Los metadatos se pueden utilizar para restaurar datos antes del tiempo de creación de instantáneas.

- Instantáneas de HDFS

  Una instantánea HDFS es una copia de respaldo de solo lectura de HDFS en un punto de tiempo especificado. La instantánea se utiliza en copia de respaldo de datos, protección de mal funcionamiento y escenarios de recuperación ante desastres.

  La función de instantánea se puede habilitar para que cualquier directorio de HDFS cree el archivo de instantánea relacionado. Antes de crear una instantánea para un directorio, el sistema activa automáticamente la función de instantánea para el directorio. La creación de una instantánea no afecta a ninguna operación de HDFS. Se puede crear un máximo de 65,536 instantáneas para cada directorio de HDFS.

  Cuando se crea una instantánea para un directorio de HDFS, el directorio no se puede eliminar ni modificar antes de crear la instantánea. No se pueden crear instantáneas para los directorios o subdirectorios de capa superior del directorio.

DistCp

Distributed copy (DistCp) es una herramienta utilizada para replicar una gran cantidad de datos en HDFS en un clúster o entre los HDFS de diferentes clústeres. En una tarea de copia de respaldo o restauración de HBase, HDFS, o Hive, si realiza una copia de respaldo de los datos en HDFS del clúster en espera, el sistema invoca a DistCp para realizar la operación. Instale el software de de la misma versión para los clústeres activo y en espera e instale el clúster.

DistCp utiliza MapReduce para implementar la distribución de datos, la solución de problemas, la restauración y el informe. DistCp especifica diferentes trabajos de Map para varios archivos y directorios de origen en la lista especificada. Cada trabajo de Map copia los datos de la partición que corresponde al archivo especificado en la lista.

Si utiliza DistCp para replicar datos entre HDFS de dos clústeres, configure la confianza mutua entre clústeres (no es necesario configurar la confianza mutua para clústeres gestionados por el mismo FusionInsight Manager) y replicación entre clústeres para ambos clústeres. Cuando realice una copia de respaldo de los datos del clúster en HDFS en otro clúster, debe instalar el componente Yarn. De hacerlo, no se realizará la copia de respaldo.

Restauración rápida local

Después de utilizar DistCp para realizar una copia de respaldo de los datos HBase, HDFS y Hive del clúster local en el HDFS del clúster en espera, el HDFS del clúster local conserva las instantáneas de datos de copia de respaldo. Puede crear tareas de restauración rápida locales para restaurar datos mediante los archivos de instantáneas en el HDFS del clúster local.

NAS

El almacenamiento conectado a la red (NAS) es un servidor de almacenamiento de datos dedicado que incluye los componentes de almacenamiento y el software del sistema integrado. Proporciona la función de intercambio de archivos entre plataformas. Mediante el uso de NFS (que admite NFSv3 y NFSv4) y CIFS (que admite SMBv2 y SMBv3), puede conectar el plano de servicio de al servidor NAS para realizar copias de respaldo de los datos en el NAS o restaurar los datos desde el NAS.

NOTA

- Antes de realizar una copia de respaldo de los datos en el NAS, el sistema monta automáticamente la dirección compartida del NAS en una partición local del nodo de ejecución de tareas de copia de respaldo. Una vez completada la copia de respaldo, el sistema desmonta la partición compartida del NAS del nodo de ejecución de tareas de copia de respaldo.
- Para evitar fallas de copia de respaldo y restauración, no acceda a la dirección compartida donde se ha montado el servidor NAS, por ejemplo, **/srv/BigData/LocalBackup/nas** durante la copia de respaldo y restauración de datos.
- Cuando se realiza una copia de respaldo de los datos de servicio en el NAS, se utiliza DistCp.

Especificaciones

Tabla 7-71 Especificaciones de la función de copia de respaldo y restauración

Concepto	Especificación
Número máximo de tareas de copia de respaldo o restauración	100
Número de tareas simultáneas en un clúster	1

Concepto	Especificación
Número máximo de tareas en espera	199
Tamaño máximo (GB) de los archivos de copia de respaldo en un disco local de Linux	600

NOTA

Si los datos de servicio se almacenan en los componentes de capa superior de ZooKeeper, asegúrese de que el número de znodes en una sola tarea de copia de respaldo o restauración no sea demasiado grande. De lo contrario, la tarea fallará y el rendimiento del servicio ZooKeeper se verá afectado. Para comprobar el número de znodes en una sola tarea de copia de respaldo o restauración, realice las siguientes operaciones:

- Asegúrese de que el número de znodes en una sola tarea de copia de respaldo o restauración sea menor que el límite superior de los controladores de archivos del sistema operativo. Específicamente:
  1. Para comprobar el límite superior en el nivel del sistema, ejecute el comando **cat /proc/sys/fs/file-max**.
  2. Para comprobar el límite superior a nivel de usuario, ejecute el comando **ulimit -n**.
- Si el número de znodes en el directorio principal excede el límite superior, realice una copia de respaldo y restaure los datos en sus subdirectorios en lotes. Para comprobar el número de znodes que utilizan scripts de cliente ZooKeeper, realice las siguientes operaciones:
  1. En FusionInsight Manager, elija **Cluster**, haga clic en el nombre del clúster deseado, elija **Services** > **ZooKeeper** > **Instance**, y vea la dirección IP de gestión de cada rol de ZooKeeper.
  2. Inicie sesión en el nodo donde se encuentra el cliente y ejecute el siguiente comando:

     zkCli.sh -server *ip*:*port*, donde, *ip* puede ser cualquier dirección IP de gestión, y el número de puerto predeterminado es 2181.
  3. Si se muestra la siguiente información, el inicio de sesión en el servidor ZooKeeper se realiza correctamente:

     ```
     WatchedEvent state:SyncConnected type:None path:null
     [zk: ip:port(CONNECIED) 0]
     ```
  4. Ejecute el comando **getusage** para verificar el número de znodes en el directorio que se va a realizar la copia de respaldo.

     Por ejemplo, **getusage /hbase/region**. En la salida del comando, **Node count=xxxxxx** indica el número de znodes almacenados en el directorio **region**.

Tabla 7-72 Especificaciones de la tarea default

Concepto	OMS	HBase	Kafka	DBService	NameNode
Período de copia de respaldo	1 hora				
Número máximo de copias de respaldo	168 (datos históricos de 7 días)				24 (datos históricos de un día)

Concepto	OMS	HBase	Kafka	DBService	NameNode
Tamaño máximo de un archivo de copia de respaldo	10 MB	10 MB	512 MB	100 MB	20 GB
Tamaño máximo del espacio en disco utilizado	1.64 GB	1.64 GB	84 GB	16.41 GB	480 GB
Ruta de almacenamiento de datos de copia de respaldo	*Data storage path*/**LocalBackup/** de los nodos de gestión activo y en espera				

NOTA

- Los datos de copia de respaldo de la tarea de copia de respaldo predeterminada deben transferirse y guardarse periódicamente fuera del clúster según los requisitos de O&M de la empresa.
- Los administradores pueden crear tareas de copia de respaldo de DistCp para guardar datos de OMS, DBService y NameNode en clústeres externos.
- El tiempo de ejecución de una tarea de copia de respaldo de datos del clúster se puede calcular utilizando la siguiente fórmula: Tiempo de ejecución de la tarea = Volumen de datos que se van a hacer copias de respaldo/Ancho de banda de red entre el clúster y el dispositivo de copia de respaldo. En la práctica, se recomienda multiplicar el tiempo calculado por 1.5 para obtener el valor de referencia del tiempo de ejecución de la tarea.
- La ejecución de una tarea de copia de respaldo de datos afecta al rendimiento máximo de E/S del clúster. Por lo tanto, se recomienda ejecutar una tarea de copia de respaldo durante las horas no pico.

7.10.2 Copia de respaldo de datos

7.10.2.1 Copia de respaldo de los datos del Manager

Escenario

Para garantizar la seguridad de los datos de FusionInsight Manager de forma rutinaria o antes y después de una operación crítica (como la ampliación y la reducción de capacidad) en FusionInsight Manager, debe realizar una copia de respaldo de los datos de FusionInsight Manager. Los datos de copia de respaldo se pueden utilizar para recuperar el sistema si se produce una excepción o la operación no ha logrado el resultado esperado, minimizando los impactos adversos en los servicios.

Puede crear una tarea de copia de respaldo en el FusionInsight Manager para realizar una copia de respaldo de los datos del Manager. Se admiten tareas de copia de respaldo tanto automáticas como manuales.

Prerrequisitos

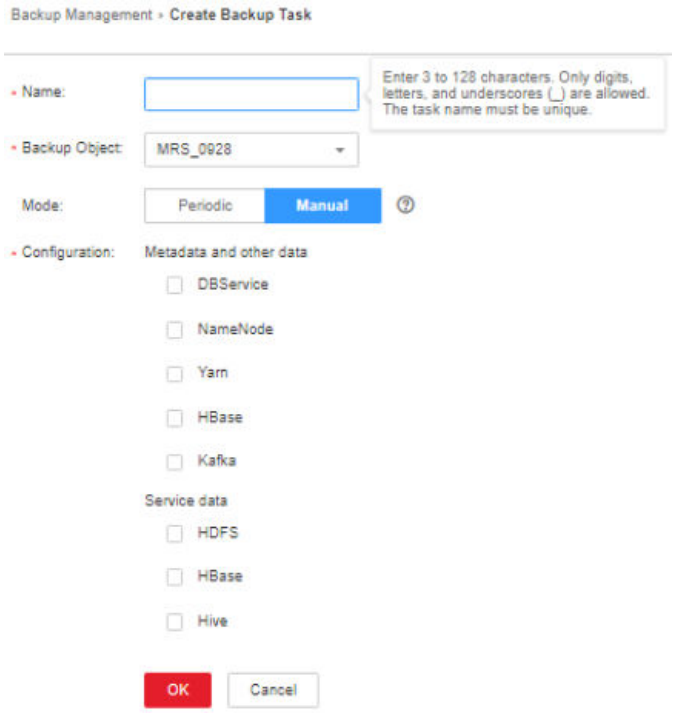
- Si es necesario realizar una copia de respaldo de los datos en el HDFS remoto, ha preparado un clúster en espera para la copia de respaldo de los datos. El modo de autenticación del clúster en espera es el mismo que el del clúster activo. Para otros modos de copia de respaldo, no es necesario preparar el clúster en espera.
- Si el clúster activo se despliega en modo de seguridad y los clústeres activo y en espera no son gestionados por el mismo FusionInsight Manager, se ha configurado la confianza mutua. Para obtener más información, consulte **Configuración de la confianza mutua Cross-Manager entre clústeres**. Si el clúster activo se despliega en modo normal, no se requiere confianza mutua.
- Se ha configurado la replicación entre clústeres para los clústeres activo y en espera. Para obtener más información, consulte **Habilitación de la replicación entre clústeres**.
- El tiempo es consistente entre los clústeres activos y en espera y los servicios NTP en los clústeres activos y en espera utilizan la misma fuente de tiempo.
- El tipo de copia de respaldo, el período, la política y otras especificaciones se han planificado en función de los requisitos de servicio y se ha comprobado si *Data storage path*/**LocalBackup/** tiene suficiente espacio en los nodos de gestión activo y en espera.
- Si desea realizar una copia de respaldo de los datos en el NAS, ha desplegado el servidor NAS por adelantado.
- Si desea realizar una copia de respaldo de los datos en OBS, ha conectado el clúster actual a OBS y tiene el permiso para acceder a OBS.

Procedimiento

Paso 1 En FusionInsight Manager, seleccione **O&M** > **Backup and Restoration** > **Backup Management**.

Paso 2 Haga clic en **Create**.

Figura 7-58 Creación de una tarea de copia de respaldo.



Paso 3 Establezca **Name** en el nombre de la tarea de copia de respaldo.

Paso 4 Ajusta **Backup Object** a **OMS**.

Paso 5 Establezca **Mode** en el tipo de tarea de copia de respaldo.

Periodic indica que la tarea de copia de respaldo es ejecutada por el sistema periódicamente. **Manual** indica que la tarea de copia de respaldo se ejecuta manualmente.

Tabla 7-73 Parámetros de copia de respaldo periódico

Parámetro	Descripción
Started	Indica la hora a la que se inicia la tarea por primera vez.
Period	Indica el intervalo de ejecución de la tarea. Las opciones incluyen **Hours** y **Days**.
Backup Policy	● **Copia de respaldo completa la primera vez y copia de respaldo incremental posteriormente** ● **Copia de respaldo completa cada vez** ● **Copia de respaldo completa una vez cada n veces** **NOTA** ● No se admite la copia de respaldo incremental cuando se realizan copias de respaldo de los datos de Manager y los metadatos de los componentes. Solo se admite **Copia de respaldo completa cada vez**. ● Si **Path Type** se establece en **NFS** o **CIFS**, no se puede utilizar la copia de respaldo incremental. Cuando se utiliza la copia de respaldo incremental para la copia de respaldo de NFS o CIFS, los datos de copia de respaldo completa más recientes se actualizan cada vez que se realiza la copia de respaldo incremental. Por lo tanto, no se genera ningún nuevo punto de recuperación.

Paso 6 En **Configuration**, seleccione **OMS**.

Paso 7 Establecer **Path Type** de **OMS** en un tipo de directorio de copia de respaldo.

Se admiten los siguientes tipos de directorio de copia de respaldo:

- **LocalDir**: indica que los archivos de copia de respaldo se almacenan en el disco local del nodo de gestión activo y el nodo de gestión en espera sincroniza automáticamente los archivos de copia de respaldo.

  El directorio de almacenamiento predeterminado es *Data storage path*/**LocalBackup/**, por ejemplo, **/srv/BigData/LocalBackup**.

  Si selecciona esta opción, debe establecer el número máximo de réplicas para especificar el número de conjuntos de archivos de copia de respaldo que se pueden conservar en el directorio de copia de respaldo.

- **LocalHDFS**: indica que los archivos de copia de respaldo se almacenan en el directorio de HDFS del clúster actual.

  Si selecciona esta opción, establezca los siguientes parámetros:

  – **Target Path**: indica el directorio de HDFS para almacenar los archivos de copia de respaldo. La ruta de almacenamiento no puede ser un directorio oculto de HDFS, como un directorio de instantáneas o papelera de reciclaje, o un directorio de sistema predeterminado, como **/hbase** o **/user/hbase/backup**.

  - **Maximum Number of Backup Copies**: indica el número de conjuntos de archivos de copia de respaldo que se pueden retener en el directorio de copia de respaldo.
  - **Cluster for Backup**: Introduzca el nombre del clúster asignado al directorio de copia de respaldo.
  - **Target NameService Name**: indica el nombre de NameService del directorio de copia de respaldo. El valor predeterminado es **hacluster**.

- **RemoteHDFS**: indica que los archivos de copia de respaldo se almacenan en el directorio de HDFS del clúster en espera.

  Si selecciona esta opción, establezca los siguientes parámetros:

  - **Destination NameService Name**: indica el nombre de NameService del clúster en espera. Puede establecerlo en el nombre de NameService (**haclusterX**, **haclusterX1**, **haclusterX2**, **haclusterX3**, o **haclusterX4**) del clúster remoto integrado del clúster, o el nombre de NameService de un clúster remoto configurado.
  - **IP Mode**: indica el modo de la dirección IP de destino. El sistema selecciona automáticamente el modo de dirección IP en función del tipo de red del clúster, por ejemplo **IPv4** o **IPv6**.
  - **Target NameNode IP Address**: indica la dirección IP del plano de servicio NameNode en el clúster en espera. Puede ser de un nodo activo o en espera.
  - **Target Path**: indica el directorio HDFS para almacenar los datos de copia de respaldo del clúster en espera. La ruta de almacenamiento no puede ser un directorio oculto de HDFS, como un directorio de instantáneas o papelera de reciclaje, o un directorio de sistema predeterminado, como **/hbase** o **/user/hbase/backup**.
  - **Maximum Number of Backup Copies**: indica el número de conjuntos de archivos de copia de respaldo que se pueden retener en el directorio de copia de respaldo.
  - **Source Cluster**: Seleccione el clúster de la cola de Yarn utilizada por los datos de copia de respaldo.
  - **Queue Name**: indica el nombre de la cola de Yarn utilizada para la ejecución de tareas de copia de respaldo. El nombre debe ser el mismo que el nombre de la cola que se está ejecutando correctamente en el clúster de origen.

- **NFS**: indica que los archivos de copia de respaldo se almacenan en el NAS mediante el protocolo NFS.

  Si selecciona esta opción, establezca los siguientes parámetros:

  - **IP Mode**: indica el modo de la dirección IP de destino. El sistema selecciona automáticamente el modo de dirección IP en función del tipo de red del clúster, por ejemplo **IPv4** o **IPv6**.
  - **Server IP Address**: indica la dirección IP del servidor NAS.
  - **Server Shared Path**: indica el directorio compartido configurado del servidor NAS. (La ruta de acceso compartida del servidor no se puede establecer en el directorio raíz, y el grupo de usuarios y el grupo de propietarios de la ruta de acceso compartida deben ser **nobody:nobody**.)
  - **Maximum Number of Backup Copies**: indica el número de conjuntos de archivos de copia de respaldo que se pueden retener en el directorio de copia de respaldo.

- **CIFS**: indica que los archivos de copia de respaldo se almacenan en el NAS mediante el protocolo CIFS.

  Si selecciona esta opción, establezca los siguientes parámetros:

  - **IP Mode**: indica el modo de la dirección IP de destino. El sistema selecciona automáticamente el modo de dirección IP en función del tipo de red del clúster, por ejemplo **IPv4** o **IPv6**.
  - **Server IP Address**: indica la dirección IP del servidor NAS.
  - **Port**: indica el número de puerto utilizado para conectarse al servidor NAS a través del protocolo CIFS. El valor predeterminado es **445**.
  - **Username**: indica el nombre de usuario establecido cuando se configura el protocolo CIFS.
  - **Password**: indica la contraseña establecida cuando se configura el protocolo CIFS.
  - **Server Shared Path**: indica el directorio compartido configurado del servidor NAS. (La ruta de acceso compartida del servidor no se puede establecer en el directorio raíz, y el grupo de usuarios y el grupo de propietarios de la ruta de acceso compartida deben ser **nobody:nobody**.)
  - **Maximum Number of Backup Copies**: indica el número de conjuntos de archivos de copia de respaldo que se pueden retener en el directorio de copia de respaldo.
- **SFTP**: indica que los archivos de copia de respaldo se almacenan en el servidor mediante el protocolo SFTP.

  Si selecciona esta opción, establezca los siguientes parámetros:
  - **IP Mode**: indica el modo de la dirección IP de destino. El sistema selecciona automáticamente el modo de dirección IP en función del tipo de red del clúster, por ejemplo **IPv4** o **IPv6**.
  - **Server IP Address**: indica la dirección IP del servidor donde se almacenan los datos de copia de respaldo.
  - **Port**: indica el número de puerto utilizado para conectarse al servidor de copia de respaldo a través del protocolo SFTP. El valor predeterminado es **22**.
  - **Username**: indica el nombre de usuario para conectarse al servidor mediante el protocolo SFTP.
  - **Password**: indica la contraseña para conectarse al servidor mediante el protocolo SFTP.
  - **Server Shared Path**: indica la ruta de copia de respaldo en el servidor SFTP.
  - **Maximum Number of Backup Copies**: indica el número de conjuntos de archivos de copia de respaldo que se pueden retener en el directorio de copia de respaldo.
- **OBS**: indica que los archivos de copia de respaldo se almacenan en OBS.

  Si selecciona esta opción, establezca los siguientes parámetros:
  - **Target Path**: indica el directorio OBS para almacenar los datos de copia de respaldo.
  - **Maximum Number of Backup Copies**: indica el número de conjuntos de archivos de copia de respaldo que se pueden retener en el directorio de copia de respaldo.

    NOTA

    Solo MRS 3.1.0 o posterior admite la copia de respaldo de datos en OBS.

Paso 8 Haga clic en **OK**.

Paso 9 En la columna **Operation** de la tarea creada en la lista de tareas de copia de respaldo, haga clic en **More** y seleccione **Back Up Now** para ejecutar la tarea de copia de respaldo.

Después de ejecutar la tarea de copia de respaldo, el sistema crea automáticamente un subdirectorio para cada tarea de copia de respaldo en el directorio de copia de respaldo. El

formato del nombre del subdirectorio es de *Backup task name_Task creation time* y el subdirectorio se utiliza para guardar los archivos de copia de respaldo de origen de datos.

El formato del nombre del archivo de copia de respaldo es *Version_Data source_Task execution time***.tar.gz**.

----Fin

7.10.2.2 Copia de respaldo de metadatos de ClickHouse

Escenario

Para garantizar la seguridad de los metadatos de ClickHouse o antes de una operación importante (como la actualización o la migración), debe realizar una copia de respaldo de los metadatos de ClickHouse. Los datos de copia de respaldo se pueden utilizar para recuperar el sistema si se produce una excepción o la operación no ha logrado el resultado esperado, minimizando los impactos adversos en los servicios.

Puede crear una tarea de copia de respaldo en FusionInsight Manager para realizar una copia de respaldo de los metadatos de ClickHouse. Se admiten tareas de copia de respaldo tanto automáticas como manuales.

AVISO

Esta función solo es compatible con MRS 3.1.0 o posterior.

Prerrequisitos

- Si es necesario realizar una copia de respaldo de los datos en el HDFS remoto, ha preparado un clúster en espera para la copia de respaldo de los datos. El modo de autenticación del clúster en espera es el mismo que el del clúster activo. Para otros modos de copia de respaldo, no es necesario preparar el clúster en espera.
- El tipo de copia de respaldo, el período, la política y otras especificaciones se han planificado en función de los requisitos de servicio y se ha comprobado si *Data storage path*/**LocalBackup/** tiene suficiente espacio en los nodos de gestión activo y en espera.
- Si los clústeres activos y en espera se despliegan en modo de seguridad y no son gestionados por el mismo FusionInsight Manager, se debe configurar la confianza mutua. Para obtener más información, consulte **Configuración de la confianza mutua Cross-Manager entre clústeres**. Si los clústeres activos y en espera se despliegan en modo normal, no se requiere confianza mutua.
- El tiempo es consistente entre los clústeres activos y en espera y los servicios NTP en los clústeres activos y en espera utilizan la misma fuente de tiempo.
- En el clúster activo/en espera, si se hace una copia de respaldo remota de los datos en HDFS, asegúrese de que el valor de **HADOOP_RPC_PROTECTION** de ClickHouse es el mismo que el de **hadoop.rpc.protection** de HDFS.

Procedimiento

Paso 1 En FusionInsight Manager, seleccione **O&M** > **Backup and Restoration** > **Backup Management**.

Paso 2 Haga clic en **Create**.

Paso 3 Establezca **Name** en el nombre de la tarea de copia de respaldo.

Paso 4 Seleccione el clúster que se va a operar desde **Backup Object**.

Paso 5 Establezca **Mode** en el tipo de tarea de copia de respaldo. **Periodic** indica que la tarea de copia de respaldo se ejecuta periódicamente. **Manual** indica que la tarea de copia de respaldo se ejecuta manualmente.

Para crear una tarea de copia de respaldo periódica, establezca los siguientes parámetros:

- **Started**: indica la hora en la que se inicia la tarea por primera vez.
- **Period**: indica el intervalo de ejecución de la tarea. Las opciones incluyen **Hours** y **Days**.
- **Backup Policy**: Solo se admite el uso de **Full backup every time**.

Paso 6 En **Configuration**, seleccione **ClickHouse** en **Metadata and other data**.

Paso 7 Establezca **Path Type** de **ClickHouse** en un tipo de directorio de copia de respaldo.

Se admiten los siguientes tipos de directorio de copia de respaldo:

- **LocalDir**: indica que los archivos de copia de respaldo se almacenan en el disco local del nodo de gestión activo y el nodo de gestión en espera sincroniza automáticamente los archivos de copia de respaldo.

  El directorio de almacenamiento predeterminado es *Data storage path*/**LocalBackup/**, por ejemplo, **/srv/BigData/LocalBackup**.

  Si selecciona esta opción, debe establecer el número máximo de réplicas para especificar el número de conjuntos de archivos de copia de respaldo que se pueden conservar en el directorio de copia de respaldo.

- **RemoteHDFS**: indica que los archivos de copia de respaldo se almacenan en el directorio de HDFS del clúster en espera.

  Esta opción de valor está disponible solo después de configurar el entorno haciendo referencia a **¿Cómo configuro el entorno al crear una tarea de copia de respaldo de ClickHouse en el FusionInsight Manager y establecer el tipo de ruta en RemoteHDFS?**.

  También debe configurar los siguientes parámetros:

  – **Destination NameService Name**: indica el nombre de NameService del clúster en espera, por ejemplo, **hacluster**. Puede obtenerlo en la página **NameService Management** de HDFS del clúster en espera.

  – **IP Mode**: indica el modo de la dirección IP de destino. El sistema selecciona automáticamente el modo de dirección IP en función del tipo de red del clúster, por ejemplo **IPv4** o **IPv6**.

  – **Target NameNode IP Address**: indica la dirección IP del plano de servicio NameNode en el clúster en espera. Puede ser de un nodo activo o en espera.

  – **Target Path**: indica el directorio HDFS para almacenar los datos de copia de respaldo del clúster en espera. La ruta de almacenamiento no puede ser un directorio oculto de HDFS, como un directorio de instantáneas o papelera de reciclaje, o un directorio de sistema predeterminado, como **/hbase** o **/user/hbase/backup**.

  – **Maximum Number of Backup Copies**: indica el número de conjuntos de archivos de copia de respaldo que se pueden retener en el directorio de copia de respaldo.

Paso 8 Haga clic en **OK**.

Paso 9 En la columna **Operation** de la tarea creada en la lista de tareas de copia de respaldo, haga clic en **More** y seleccione **Back Up Now** para ejecutar la tarea de copia de respaldo.

Después de ejecutar la tarea de copia de respaldo, el sistema crea automáticamente un subdirectorio para cada tarea de copia de respaldo en el directorio de copia de respaldo. El formato del nombre del subdirectorio es de *Backup task name*_*Task creation time* y el subdirectorio se utiliza para guardar los archivos de copia de respaldo de origen de datos. El formato del nombre del archivo de copia de respaldo es *Data source*_*Task execution time*.**tar.gz**.

----Fin

7.10.2.3 Copia de respaldo de datos del servicio ClickHouse

Escenario

Para garantizar la seguridad de los datos de servicio de ClickHouse rutinariamente o antes de una operación importante en ClickHouse (como actualización o migración), necesita hacer una copia de respaldo de los datos de servicio de ClickHouse. Los datos de copia de respaldo se pueden utilizar para recuperar el sistema si se produce una excepción o la operación no ha logrado el resultado esperado, minimizando los impactos adversos en los servicios.

Puede crear una tarea de copia de respaldo en FusionInsight Manager para realizar una copia de respaldo de los datos del servicio de ClickHouse. Se admiten tareas de copia de respaldo tanto automáticas como manuales.

AVISO

Esta función solo es compatible con MRS 3.1.0 o posterior.

Prerrequisitos

- Si es necesario realizar una copia de respaldo de los datos en el HDFS remoto, ha preparado un clúster en espera para la copia de respaldo de los datos. El modo de autenticación del clúster en espera es el mismo que el del clúster activo. Para otros modos de copia de respaldo, no es necesario preparar el clúster en espera.
- Si los clústeres activos y en espera se despliegan en modo de seguridad y no son gestionados por el mismo FusionInsight Manager, se debe configurar la confianza mutua. Para obtener más información, consulte **Configuración de la confianza mutua Cross-Manager entre clústeres**. Si los clústeres activos y en espera se despliegan en modo normal, no se requiere confianza mutua.
- El tiempo es consistente entre los clústeres activos y en espera y los servicios NTP en los clústeres activos y en espera utilizan la misma fuente de tiempo.
- Ha planificado el tipo de copia de respaldo, el período, el objeto y el directorio según los requisitos del servicio.
- El HDFS del clúster en espera tiene suficiente espacio. Se recomienda guardar los archivos de copia de respaldo en un directorio personalizado.

- En el clúster activo/en espera, si se hace una copia de respaldo remota de los datos en HDFS, asegúrese de que el valor de **HADOOP_RPC_PROTECTION** de ClickHouse es el mismo que el de **hadoop.rpc.protection** de HDFS.

Procedimiento

Paso 1 En FusionInsight Manager, seleccione **O&M** > **Backup and Restoration** > **Backup Management**.

Paso 2 Haga clic en **Create**.

Paso 3 Establezca **Name** en el nombre de la tarea de copia de respaldo.

Paso 4 Seleccione el clúster que se va a operar desde **Backup Object**.

Paso 5 Establezca **Mode** en el tipo de tarea de copia de respaldo.

Periodic indica que la tarea de copia de respaldo es ejecutada por el sistema periódicamente. **Manual** indica que la tarea de copia de respaldo se ejecuta manualmente.

Tabla 7-74 Parámetros de copia de respaldo periódico

Parámetro	Descripción
Started	Indica la hora a la que se inicia la tarea por primera vez.
Period	Indica el intervalo de ejecución de la tarea. Las opciones incluyen **Hours** y **Days**.
Backup Policy	● **Copia de respaldo completa la primera vez y copia de respaldo incremental posteriormente** ● **Copia de respaldo completa cada vez** ● **Copia de respaldo completa una vez cada n veces** **NOTA** ● No se admite la copia de respaldo incremental cuando se realizan copias de respaldo de los datos de Manager y los metadatos de los componentes. Solo se admite **Copia de respaldo completa cada vez**.

Paso 6 En **Configuration**, seleccione **ClickHouse** en **Service Data**.

Paso 7 Establezca **Path Type** de **ClickHouse** en un tipo de directorio de copia de respaldo.

Actualmente, solo está disponible el tipo **RemoteHDFS**.

RemoteHDFS: indica que los archivos de copia de respaldo se almacenan en HDFS del clúster en espera.

Esta opción de valor está disponible solo después de configurar el entorno haciendo referencia a **¿Cómo configuro el entorno al crear una tarea de copia de respaldo de ClickHouse en el FusionInsight Manager y establecer el tipo de ruta en RemoteHDFS?**.

También debe configurar los siguientes parámetros:

- **Destination NameService Name**: indica el nombre de NameService del clúster en espera, por ejemplo, **hacluster**. Puede obtenerlo en la página **NameService Management** de HDFS del clúster en espera.

- **IP Mode**: indica el modo de la dirección IP de destino. El sistema selecciona automáticamente el modo de dirección IP en función del tipo de red del clúster, por ejemplo **IPv4** o **IPv6**.
- **Target NameNode IP Address**: indica la dirección IP del plano de servicio NameNode en el clúster en espera. Puede ser de un nodo activo o en espera.
- **Target Path**: indica el directorio HDFS para almacenar los datos de copia de respaldo del clúster en espera. La ruta de almacenamiento no puede ser un directorio oculto de HDFS, como un directorio de instantáneas o papelera de reciclaje, o un directorio de sistema predeterminado, como **/hbase** o **/user/hbase/backup**.
- **Maximum Number of Backup Copies**: indica el número de conjuntos de archivos de copia de respaldo que se pueden retener en el directorio de copia de respaldo.
- **Maximum Number of Maps**: indica el número máximo de map en una tarea de MapReduce. El valor predeterminado es **20**.
- **Maximum Bandwidth of a Map (MB/s)**: indica el ancho de banda máximo de un map. El valor predeterminado es **100**.

Paso 8 Establezca **Maximum Number of Recovery Points** en el número de instantáneas que se pueden retener en el clúster.

Paso 9 Establezca **Backup Content** en una o varias tablas de ClickHouse para realizar una copia de respaldo.

Puede seleccionar los datos de copia de respaldo utilizando cualquiera de los siguientes métodos:

- Adición de un archivo de datos de copia de respaldo

  Haga clic en el nombre de una base de datos en el árbol de navegación para mostrar todas las tablas de la base de datos y seleccione las tablas especificadas.

- Filtrado de expresiones regulares

  a. Haga clic en **Query Regular Expression**.

  b. Introduzca la base de datos donde se encuentran las tablas ClickHouse en el primer cuadro de texto según se le solicite. La base de datos debe ser la misma que la base de datos existente, por ejemplo, **default**.

  c. Escriba una expresión regular en el segundo cuadro de texto. Se admiten expresiones regulares estándares. Por ejemplo, para obtener todas las tablas de la base de datos, escriba **([\s\S]*?)**. Para obtener el nombre de las tablas en el formato de letras y dígitos, por ejemplo, **tb1**, escriba **tb\d***.

  d. Haga clic en **Refresh** para ver las tablas mostradas en **Directory Name**.

  e. Haga clic en **Synchronize** para guardar el resultado.

  NOTA

  - Cuando escriba expresiones regulares, haga clic en + o − para agregar o eliminar una expresión.
  - Si la tabla o el directorio seleccionado no es correcto, haga clic en **Clear Selected Node** para anular la selección.

Paso 10 Haga clic en **Verify** para comprobar si la tarea de copia de respaldo está configurada correctamente.

Las posibles causas de la falla de verificación son las siguientes:

- La dirección IP del NameNode de destino es incorrecta.
- El directorio o la tabla que se va a hacer una copia de respaldo no existe.
- El nombre del NameService es incorrecto.

Paso 11 Haga clic en **OK**.

Paso 12 En la columna **Operation** de la tarea creada en la lista de tareas de copia de respaldo, haga clic en **More** y seleccione **Back Up Now** para ejecutar la tarea de copia de respaldo.

Después de ejecutar la tarea de copia de respaldo, el sistema crea automáticamente un subdirectorio para cada tarea de copia de respaldo en el directorio de copia de respaldo. El formato del nombre del subdirectorio es *Data source_Task creation time* y el subdirectorio se utiliza para guardar los últimos archivos de copia de respaldo de origen de datos.

----Fin

7.10.2.4 Copia de respaldo de datos de DBService

Escenario

Para garantizar la seguridad de los datos del servicio DBService de forma rutinaria o antes de una operación importante en DBService (como la actualización o la migración), debe realizar una copia de respaldo de los datos de DBService. Los datos de copia de respaldo se pueden utilizar para recuperar el sistema si se produce una excepción o la operación no ha logrado el resultado esperado, minimizando los impactos adversos en los servicios.

Puede crear una tarea de copia de respaldo en FusionInsight Manager para realizar una copia de respaldo de los datos de DBService. Se admiten tareas de copia de respaldo tanto automáticas como manuales.

Prerrequisitos

- Si es necesario realizar una copia de respaldo de los datos en el HDFS remoto, ha preparado un clúster en espera para la copia de respaldo de los datos. El modo de autenticación del clúster en espera es el mismo que el del clúster activo. Para otros modos de copia de respaldo, no es necesario preparar el clúster en espera.
- Si el clúster activo se despliega en modo de seguridad y los clústeres activo y en espera no son gestionados por el mismo FusionInsight Manager, se ha configurado la confianza mutua. Para obtener más información, consulte **Configuración de la confianza mutua Cross-Manager entre clústeres**. Si el clúster activo se despliega en modo normal, no se requiere confianza mutua.
- Se ha configurado la replicación entre clústeres para los clústeres activos y en espera. Para obtener más información, consulte **Habilitación de la replicación entre clústeres**.
- El tiempo es consistente entre los clústeres activos y en espera y los servicios NTP en los clústeres activos y en espera utilizan la misma fuente de tiempo.
- El tipo de copia de respaldo, el período, la política y otras especificaciones se han planificado en función de los requisitos de servicio y se ha comprobado si *Data storage path*/**LocalBackup/** tiene suficiente espacio en los nodos de gestión activo y en espera.
- Si desea realizar una copia de respaldo de los datos en el NAS, ha desplegado el servidor NAS por adelantado.
- Si desea realizar una copia de respaldo de los datos en OBS, ha conectado el clúster actual a OBS y tiene el permiso para acceder a OBS.

Procedimiento

Paso 1 En FusionInsight Manager, seleccione **O&M** > **Backup and Restoration** > **Backup Management**.

Paso 2 Haga clic en **Create**.

Paso 3 Establezca **Name** en el nombre de la tarea de copia de respaldo.

Paso 4 Seleccione el clúster que se va a operar desde **Backup Object**.

Paso 5 Establezca **Mode** en el tipo de tarea de copia de respaldo.

Periodic indica que la tarea de copia de respaldo es ejecutada por el sistema periódicamente. **Manual** indica que la tarea de copia de respaldo se ejecuta manualmente.

Tabla 7-75 Parámetros de copia de respaldo periódico

Parámetro	Descripción
Comenzado	Indica la hora a la que se inicia la tarea por primera vez.
Period	Indica el intervalo de ejecución de la tarea. Las opciones incluyen **Hours** y **Days**.
Backup Policy	● **Copia de respaldo completa la primera vez y copia de respaldo incremental posteriormente** ● **Copia de respaldo completa cada vez** ● **Copia de respaldo completa una vez cada n veces** **NOTA** ● No se admite la copia de respaldo incremental cuando se realizan copias de respaldo de los datos de Manager y los metadatos de los componentes. Solo se admite **Copia de respaldo completa cada vez**. ● Si **Path Type** se establece en **NFS** o **CIFS**, no se puede utilizar la copia de respaldo incremental. Cuando se utiliza la copia de respaldo incremental para la copia de respaldo de NFS o CIFS, los datos de copia de respaldo completa más recientes se actualizan cada vez que se realiza la copia de respaldo incremental. Por lo tanto, no se genera ningún nuevo punto de recuperación.

Paso 6 En **Configuration**, seleccione **DBService**.

NOTA

Si hay varios servicios de DBService, se realiza una copia de respaldo de todos los servicios de DBService de forma predeterminada. Puede hacer clic en **Assign Service** para especificar los servicios que se van a realizar una copia de respaldo.

Paso 7 Establecer **Path Type** de **DBService** en un tipo de directorio de copia de respaldo.

Se admiten los siguientes tipos de directorio de copia de respaldo:

- **LocalDir**: indica que los archivos de copia de respaldo se almacenan en el disco local del nodo de gestión activo y el nodo de gestión en espera sincroniza automáticamente los archivos de copia de respaldo.

  El directorio de almacenamiento predeterminado es *Data storage path*/**LocalBackup/**, por ejemplo, **/srv/BigData/LocalBackup**.

Si selecciona esta opción, debe establecer el número máximo de réplicas para especificar el número de conjuntos de archivos de copia de respaldo que se pueden conservar en el directorio de copia de respaldo.

- **LocalHDFS**: indica que los archivos de copia de respaldo se almacenan en el directorio de HDFS del clúster actual.

  Si selecciona esta opción, establezca los siguientes parámetros:

  – **Target Path**: indica el directorio de HDFS para almacenar los archivos de copia de respaldo. La ruta de almacenamiento no puede ser un directorio oculto de HDFS, como un directorio de instantáneas o papelera de reciclaje, o un directorio de sistema predeterminado, como **/hbase** o **/user/hbase/backup**.

  – **Maximum Number of Backup Copies**: indica el número de conjuntos de archivos de copia de respaldo que se pueden retener en el directorio de copia de respaldo.

  – **Target NameService Name**: indica el nombre de NameService del directorio de copia de respaldo. El valor predeterminado es **hacluster**.

- **RemoteHDFS**: indica que los archivos de copia de respaldo se almacenan en el directorio de HDFS del clúster en espera.

  Si selecciona esta opción, establezca los siguientes parámetros:

  – **Destination NameService Name**: indica el nombre de NameService del clúster en espera. Puede establecerlo en el nombre de NameService (**haclusterX**, **haclusterX1**, **haclusterX2**, **haclusterX3**, o **haclusterX4**) del clúster remoto integrado del clúster, o el nombre de NameService de un clúster remoto configurado.

  – **IP Mode**: indica el modo de la dirección IP de destino. El sistema selecciona automáticamente el modo de dirección IP en función del tipo de red del clúster, por ejemplo **IPv4** o **IPv6**.

  – **Target NameNode IP Address**: indica la dirección IP del plano de servicio NameNode en el clúster en espera. Puede ser de un nodo activo o en espera.

  – **Target Path**: indica el directorio HDFS para almacenar los datos de copia de respaldo del clúster en espera. La ruta de almacenamiento no puede ser un directorio oculto de HDFS, como un directorio de instantáneas o papelera de reciclaje, o un directorio de sistema predeterminado, como **/hbase** o **/user/hbase/backup**.

  – **Maximum Number of Backup Copies**: indica el número de conjuntos de archivos de copia de respaldo que se pueden retener en el directorio de copia de respaldo.

  – **Queue Name**: indica el nombre de la cola de Yarn utilizada para la ejecución de tareas de copia de respaldo. El nombre debe ser el mismo que el nombre de la cola que se está ejecutando correctamente en el clúster de origen.

- **NFS**: indica que los archivos de copia de respaldo se almacenan en el NAS mediante el protocolo NFS.

  Si selecciona esta opción, establezca los siguientes parámetros:

  – **IP Mode**: indica el modo de la dirección IP de destino. El sistema selecciona automáticamente el modo de dirección IP en función del tipo de red del clúster, por ejemplo **IPv4** o **IPv6**.

  – **Server IP Address**: indica la dirección IP del servidor NAS.

  – **Server Shared Path**: indica el directorio compartido configurado del servidor NAS. (La ruta de acceso compartida del servidor no se puede establecer en el directorio raíz, y el grupo de usuarios y el grupo de propietarios de la ruta de acceso compartida deben ser **nobody:nobody**.)

  - **Maximum Number of Backup Copies**: indica el número de conjuntos de archivos de copia de respaldo que se pueden retener en el directorio de copia de respaldo.

- **CIFS**: indica que los archivos de copia de respaldo se almacenan en el NAS mediante el protocolo CIFS.

  Si selecciona esta opción, establezca los siguientes parámetros:

  - **IP Mode**: indica el modo de la dirección IP de destino. El sistema selecciona automáticamente el modo de dirección IP en función del tipo de red del clúster, por ejemplo **IPv4** o **IPv6**.
  - **Server IP Address**: indica la dirección IP del servidor NAS.
  - **Port**: indica el número de puerto utilizado para conectarse al servidor NAS a través del protocolo CIFS. El valor predeterminado es **445**.
  - **Username**: indica el nombre de usuario establecido cuando se configura el protocolo CIFS.
  - **Password**: indica la contraseña establecida cuando se configura el protocolo CIFS.
  - **Server Shared Path**: indica el directorio compartido configurado del servidor NAS. (La ruta de acceso compartida del servidor no se puede establecer en el directorio raíz, y el grupo de usuarios y el grupo de propietarios de la ruta de acceso compartida deben ser **nobody:nobody**.)
  - **Maximum Number of Backup Copies**: indica el número de conjuntos de archivos de copia de respaldo que se pueden retener en el directorio de copia de respaldo.

- **SFTP**: indica que los archivos de copia de respaldo se almacenan en el servidor mediante el protocolo SFTP.

  Si selecciona esta opción, establezca los siguientes parámetros:

  - **IP Mode**: indica el modo de la dirección IP de destino. El sistema selecciona automáticamente el modo de dirección IP en función del tipo de red del clúster, por ejemplo **IPv4** o **IPv6**.
  - **Server IP Address**: indica la dirección IP del servidor donde se almacenan los datos de copia de respaldo.
  - **Port**: indica el número de puerto utilizado para conectarse al servidor de copia de respaldo a través del protocolo SFTP. El valor predeterminado es **22**.
  - **Username**: indica el nombre de usuario para conectarse al servidor mediante el protocolo SFTP.
  - **Password**: indica la contraseña para conectarse al servidor mediante el protocolo SFTP.
  - **Server Shared Path**: indica la ruta de copia de respaldo en el servidor SFTP.
  - **Maximum Number of Backup Copies**: indica el número de conjuntos de archivos de copia de respaldo que se pueden retener en el directorio de copia de respaldo.

- **OBS**: indica que los archivos de copia de respaldo se almacenan en OBS.

  Si selecciona esta opción, establezca los siguientes parámetros:

  - **Target Path**: indica el directorio OBS para almacenar los datos de copia de respaldo.
  - **Maximum Number of Backup Copies**: indica el número de conjuntos de archivos de copia de respaldo que se pueden retener en el directorio de copia de respaldo.

    NOTA

    Solo MRS 3.1.0 o posterior admite la copia de respaldo de datos en OBS.

Paso 8 Haga clic en **OK**.

Paso 9 En la columna **Operation** de la tarea creada en la lista de tareas de copia de respaldo, haga clic en **More** y seleccione **Back Up Now** para ejecutar la tarea de copia de respaldo.

Después de ejecutar la tarea de copia de respaldo, el sistema crea automáticamente un subdirectorio para cada tarea de copia de respaldo en el directorio de copia de respaldo. El formato del nombre del subdirectorio es de *Backup task name_Task creation time* y el subdirectorio se utiliza para guardar los archivos de copia de respaldo de origen de datos.

El formato del nombre del archivo de copia de respaldo es *Version_Data source_Task execution time***.tar.gz**.

----Fin

7.10.2.5 Copia de respaldo de metadatos de Flink

Escenario

Para garantizar la seguridad de los metadatos de Flink o antes de una operación importante en Flink (como la actualización o la migración), debe realizar una copia de respaldo de los metadatos de Flink. Los datos de copia de respaldo se pueden utilizar para recuperar el sistema si se produce una excepción o la operación no ha logrado el resultado esperado, minimizando los impactos adversos en los servicios.

Puede crear una tarea de copia de respaldo en FusionInsight Manager para hacer una copia de respaldo de los metadatos de Flink. Se admiten tareas de copia de respaldo tanto automáticas como manuales.

Prerrequisitos

- Si es necesario realizar una copia de respaldo de los datos en el HDFS remoto, ha preparado un clúster en espera para la copia de respaldo de los datos. El modo de autenticación del clúster en espera es el mismo que el del clúster activo. Para otros modos de copia de respaldo, no es necesario preparar el clúster en espera.
- Los servicios HDFS y Yarn se han instalado si es necesario realizar una copia de respaldo de los datos en HDFS.
- El tipo de copia de respaldo, el período, la política y otras especificaciones se han planificado en función de los requisitos de servicio y se ha comprobado si *Data storage path*/**LocalBackup/** tiene suficiente espacio en los nodos de gestión activo y en espera.
- Si el clúster activo se despliega en modo de seguridad y los clústeres activo y en espera no son gestionados por el mismo FusionInsight Manager, se ha configurado la confianza mutua. Para obtener más información, consulte **Configuración de la confianza mutua Cross-Manager entre clústeres**. Si el clúster activo se despliega en modo normal, no se requiere confianza mutua.
- Se ha configurado la replicación entre clústeres para los clústeres activos y en espera. Para obtener más información, consulte **Habilitación de la replicación entre clústeres**.
- El tiempo es consistente entre los clústeres activos y en espera y los servicios NTP en los clústeres activos y en espera utilizan la misma fuente de tiempo.

Procedimiento

Paso 1 En FusionInsight Manager, seleccione **O&M** > **Backup and Restoration** > **Backup Management**.

Paso 2 Haga clic en **Create**.

Paso 3 Establezca **Name** en el nombre de la tarea de copia de respaldo.

Paso 4 Seleccione el clúster que se va a operar desde **Backup Object**.

Paso 5 Establezca **Mode** en el tipo de tarea de copia de respaldo. **Periodic** indica que la tarea de copia de respaldo se ejecuta periódicamente. **Manual** indica que la tarea de copia de respaldo se ejecuta manualmente.

Para crear una tarea de copia de respaldo periódica, establezca los siguientes parámetros:

- **Started**: indica la hora en la que se inicia la tarea por primera vez.
- **Period**: indica el intervalo de ejecución de la tarea. Las opciones incluyen **Hours** y **Days**.
- **Backup Policy**: Solo se admite el uso de **Full backup every time**.

Paso 6 En **Configuration**, seleccione **Flink** en **Metadata and other data**.

Paso 7 Establezca **Path Type** de **Flink** en un tipo de directorio de copia de respaldo.

Se admiten los siguientes tipos de directorio de copia de respaldo:

- **LocalDir**: indica que los archivos de copia de respaldo se almacenan en el disco local del nodo de gestión activo y el nodo de gestión en espera sincroniza automáticamente los archivos de copia de respaldo.

  El directorio de almacenamiento predeterminado es *Data storage path*/**LocalBackup/**, por ejemplo, **/srv/BigData/LocalBackup**.

  Si selecciona esta opción, debe establecer el número máximo de réplicas para especificar el número de conjuntos de archivos de copia de respaldo que se pueden conservar en el directorio de copia de respaldo.

- **LocalHDFS**: indica que los archivos de copia de respaldo se almacenan en el directorio de HDFS del clúster actual.

  Si selecciona esta opción, establezca los siguientes parámetros:

  – **Target Path**: indica el directorio de HDFS para almacenar los archivos de copia de respaldo. La ruta de almacenamiento no puede ser un directorio oculto de HDFS, como un directorio de instantáneas o papelera de reciclaje, o un directorio de sistema predeterminado, como **/hbase** o **/user/hbase/backup**.

  – **Maximum Number of Backup Copies**: indica el número de conjuntos de archivos de copia de respaldo que se pueden retener en el directorio de copia de respaldo.

  – **Target NameService Name**: indica el nombre de NameService del directorio de copia de respaldo. El valor predeterminado es **hacluster**.

- **RemoteHDFS**: indica que los archivos de copia de respaldo se almacenan en el directorio de HDFS del clúster en espera.

  Si selecciona esta opción, establezca los siguientes parámetros:

  – **Destination NameService Name**: indica el nombre de NameService del clúster en espera. Puede establecerlo en el nombre de NameService (**haclusterX**, **haclusterX1**, **haclusterX2**, **haclusterX3**, o **haclusterX4**) del clúster remoto

integrado del clúster, o el nombre de NameService de un clúster remoto configurado.

- **IP Mode**: indica el modo de la dirección IP de destino. El sistema selecciona automáticamente el modo de dirección IP en función del tipo de red del clúster, por ejemplo **IPv4** o **IPv6**.
- **Target NameNode IP Address**: indica la dirección IP del plano de servicio NameNode en el clúster en espera. Puede ser de un nodo activo o en espera.
- **Target Path**: indica el directorio HDFS para almacenar los datos de copia de respaldo del clúster en espera. La ruta de almacenamiento no puede ser un directorio oculto de HDFS, como un directorio de instantáneas o papelera de reciclaje, o un directorio de sistema predeterminado, como **/hbase** o **/user/hbase/backup**.
- **Maximum Number of Backup Copies**: indica el número de conjuntos de archivos de copia de respaldo que se pueden retener en el directorio de copia de respaldo.
- **Queue Name**: indica el nombre de la cola de Yarn utilizada para la ejecución de tareas de copia de respaldo. El nombre debe ser el mismo que el nombre de la cola que se está ejecutando correctamente en el clúster de origen.

Paso 8 Haga clic en **OK**.

Paso 9 En la columna **Operation** de la tarea creada en la lista de tareas de copia de respaldo, haga clic en **More** y seleccione **Back Up Now** para ejecutar la tarea de copia de respaldo.

Después de ejecutar la tarea de copia de respaldo, el sistema crea automáticamente un subdirectorio para cada tarea de copia de respaldo en el directorio de copia de respaldo. El formato del nombre del subdirectorio es de *Backup task name_Task creation time* y el subdirectorio se utiliza para guardar los archivos de copia de respaldo de origen de datos. El formato del nombre del archivo de copia de respaldo es *Data source_Task execution time***.tar.gz**.

----Fin

7.10.2.6 Copia de respaldo de metadatos de HBase

Escenario

Para garantizar la seguridad de los metadatos de HBase (incluidos los archivos tableinfo y HFiles) o antes de una operación importante en las tablas del sistema HBase (como la actualización o la migración), debe realizar una copia de respaldo de los metadatos de HBase para evitar la indisponibilidad del servicio HBase causada por el directorio de tablas del sistema HBase o los daños en los archivos. Los datos de copia de respaldo se pueden utilizar para recuperar el sistema si se produce una excepción o la operación no ha logrado el resultado esperado, minimizando los impactos adversos en los servicios.

Puede crear una tarea de copia de respaldo en FusionInsight Manager para hacer una copia de respaldo de los metadatos de HBase. Se admiten tareas de copia de respaldo tanto automáticas como manuales.

Prerrequisitos

- Si es necesario realizar una copia de respaldo de los datos en el HDFS remoto, ha preparado un clúster en espera para la copia de respaldo de los datos. El modo de autenticación del clúster en espera es el mismo que el del clúster activo. Para otros modos de copia de respaldo, no es necesario preparar el clúster en espera.

- Si el clúster activo se despliega en modo de seguridad y los clústeres activo y en espera no son gestionados por el mismo FusionInsight Manager, se ha configurado la confianza mutua. Para obtener más información, consulte **Configuración de la confianza mutua Cross-Manager entre clústeres**. Si el clúster activo se despliega en modo normal, no se requiere confianza mutua.
- Se ha configurado la replicación entre clústeres para los clústeres activos y en espera. Para obtener más información, consulte **Habilitación de la replicación entre clústeres**.
- El tiempo es consistente entre los clústeres activos y en espera y los servicios NTP en los clústeres activos y en espera utilizan la misma fuente de tiempo.
- El tipo de copia de respaldo, el período, la política y otras especificaciones se han planificado en función de los requisitos de servicio y se ha comprobado si *Data storage path*/**LocalBackup/** tiene suficiente espacio en los nodos de gestión activo y en espera.
- Si desea realizar una copia de respaldo de los datos en el NAS, ha desplegado el servidor NAS por adelantado.
- Los parámetros **fs.defaultFS** de HBase son los mismos que los de Yarn y HDFS.
- Si los datos de HBase se almacenan en el HDFS local, los metadatos de HBase se pueden hacer copias de respaldo en OBS. Si los datos de HBase se almacenan en OBS, no se admite la copia de respaldo de datos.
- Si desea realizar una copia de respaldo de los datos en OBS, ha conectado el clúster actual a OBS y tiene el permiso para acceder a OBS.

Procedimiento

Paso 1 En FusionInsight Manager, seleccione **O&M** > **Backup and Restoration** > **Backup Management**.

Paso 2 Haga clic en **Create**.

Paso 3 Establezca **Name** en el nombre de la tarea de copia de respaldo.

Paso 4 Seleccione el clúster que se va a operar desde **Backup Object**.

Paso 5 Establezca **Mode** en el tipo de tarea de copia de respaldo.

Periodic indica que la tarea de copia de respaldo es ejecutada por el sistema periódicamente. **Manual** indica que la tarea de copia de respaldo se ejecuta manualmente.

Tabla 7-76 Parámetros de copia de respaldo periódico

Parámetro	Descripción
Started	Indica la hora a la que se inicia la tarea por primera vez.
Period	Indica el intervalo de ejecución de la tarea. Las opciones incluyen **Hours** y **Days**.

Parámetro	Descripción
Backup Policy	● **Copia de respaldo completa la primera vez y copia de respaldo incremental posteriormente** ● **Copia de respaldo completa cada vez** ● **Copia de respaldo completa una vez cada n veces** **NOTA** ● No se admite la copia de respaldo incremental cuando se realizan copias de respaldo de los datos de Manager y los metadatos de los componentes. Solo se admite **Copia de respaldo completa cada vez**. ● Si **Path Type** se establece en **NFS** o **CIFS**, no se puede utilizar la copia de respaldo incremental. Cuando se utiliza la copia de respaldo incremental para la copia de respaldo de NFS o CIFS, los datos de copia de respaldo completa más recientes se actualizan cada vez que se realiza la copia de respaldo incremental. Por lo tanto, no se genera ningún nuevo punto de recuperación.

Paso 6 En **Configuration**, seleccione **HBase** en **Metadata and other data**.

NOTA

Si hay varios servicios HBase, todos los servicios HBase están respaldados de forma predeterminada. Puede hacer clic en **Assign Service** para especificar los servicios que se van a realizar una copia de respaldo.

Paso 7 Establezca **Path Type** de **HBase** en un tipo de directorio de copia de respaldo.

Se admiten los siguientes tipos de directorio de copia de respaldo:

- **LocalDir**: indica que los archivos de copia de respaldo se almacenan en el disco local del nodo de gestión activo y el nodo de gestión en espera sincroniza automáticamente los archivos de copia de respaldo.

  El directorio de almacenamiento predeterminado es *Data storage path*/**LocalBackup/**, por ejemplo, **/srv/BigData/LocalBackup**.

  Si selecciona esta opción, debe establecer el número máximo de réplicas para especificar el número de conjuntos de archivos de copia de respaldo que se pueden conservar en el directorio de copia de respaldo.

- **RemoteHDFS**: indica que los archivos de copia de respaldo se almacenan en el directorio de HDFS del clúster en espera.

  Si selecciona esta opción, establezca los siguientes parámetros:

  – **Destination NameService Name**: indica el nombre de NameService del clúster en espera. Puede establecerlo en el nombre de NameService (**haclusterX**, **haclusterX1**, **haclusterX2**, **haclusterX3**, o **haclusterX4**) del clúster remoto integrado del clúster, o el nombre de NameService de un clúster remoto configurado.

  – **IP Mode**: indica el modo de la dirección IP de destino. El sistema selecciona automáticamente el modo de dirección IP en función del tipo de red del clúster, por ejemplo **IPv4** o **IPv6**.

  – **Target NameNode IP Address**: indica la dirección IP del plano de servicio NameNode en el clúster en espera. Puede ser de un nodo activo o en espera.

  – **Target Path**: indica el directorio HDFS para almacenar los datos de copia de respaldo del clúster en espera. La ruta de almacenamiento no puede ser un

directorio oculto de HDFS, como un directorio de instantáneas o papelera de reciclaje, o un directorio de sistema predeterminado, como **/hbase** o **/user/hbase/backup**.

- **Maximum Number of Backup Copies**: indica el número de conjuntos de archivos de copia de respaldo que se pueden retener en el directorio de copia de respaldo.
- **Queue Name**: indica el nombre de la cola de Yarn utilizada para la ejecución de tareas de copia de respaldo. El nombre debe ser el mismo que el nombre de la cola que se está ejecutando correctamente en el clúster de origen.

- **NFS**: indica que los archivos de copia de respaldo se almacenan en el NAS mediante el protocolo NFS.

  Si selecciona esta opción, establezca los siguientes parámetros:

  - **IP Mode**: indica el modo de la dirección IP de destino. El sistema selecciona automáticamente el modo de dirección IP en función del tipo de red del clúster, por ejemplo **IPv4** o **IPv6**.
  - **Server IP Address**: indica la dirección IP del servidor NAS.
  - **Server Shared Path**: indica el directorio compartido configurado del servidor NAS. (La ruta de acceso compartida del servidor no se puede establecer en el directorio raíz, y el grupo de usuarios y el grupo de propietarios de la ruta de acceso compartida deben ser **nobody:nobody**.)
  - **Maximum Number of Backup Copies**: indica el número de conjuntos de archivos de copia de respaldo que se pueden retener en el directorio de copia de respaldo.

- **CIFS**: indica que los archivos de copia de respaldo se almacenan en el NAS mediante el protocolo CIFS.

  Si selecciona esta opción, establezca los siguientes parámetros:

  - **IP Mode**: indica el modo de la dirección IP de destino. El sistema selecciona automáticamente el modo de dirección IP en función del tipo de red del clúster, por ejemplo **IPv4** o **IPv6**.
  - **Server IP Address**: indica la dirección IP del servidor NAS.
  - **Port**: indica el número de puerto utilizado para conectarse al servidor NAS a través del protocolo CIFS. El valor predeterminado es **445**.
  - **Username**: indica el nombre de usuario establecido cuando se configura el protocolo CIFS.
  - **Password**: indica la contraseña establecida cuando se configura el protocolo CIFS.
  - **Server Shared Path**: indica el directorio compartido configurado del servidor NAS. (La ruta de acceso compartida del servidor no se puede establecer en el directorio raíz, y el grupo de usuarios y el grupo de propietarios de la ruta de acceso compartida deben ser **nobody:nobody**.)
  - **Maximum Number of Backup Copies**: indica el número de conjuntos de archivos de copia de respaldo que se pueden retener en el directorio de copia de respaldo.

- **SFTP**: indica que los archivos de copia de respaldo se almacenan en el servidor mediante el protocolo SFTP.

  Si selecciona esta opción, establezca los siguientes parámetros:

  - **IP Mode**: indica el modo de la dirección IP de destino. El sistema selecciona automáticamente el modo de dirección IP en función del tipo de red del clúster, por ejemplo **IPv4** o **IPv6**.
  - **Server IP Address**: indica la dirección IP del servidor donde se almacenan los datos de copia de respaldo.

- **Port**: indica el número de puerto utilizado para conectarse al servidor de copia de respaldo a través del protocolo SFTP. El valor predeterminado es **22**.
- **Username**: indica el nombre de usuario para conectarse al servidor mediante el protocolo SFTP.
- **Password**: indica la contraseña para conectarse al servidor mediante el protocolo SFTP.
- **Server Shared Path**: indica la ruta de copia de respaldo en el servidor SFTP.
- **Maximum Number of Backup Copies**: indica el número de conjuntos de archivos de copia de respaldo que se pueden retener en el directorio de copia de respaldo.

- **OBS**: indica que los archivos de copia de respaldo se almacenan en OBS.

  Si selecciona esta opción, establezca los siguientes parámetros:

  - **Target Path**: indica el directorio OBS para almacenar los datos de copia de respaldo.
  - **Maximum Number of Backup Copies**: indica el número de conjuntos de archivos de copia de respaldo que se pueden retener en el directorio de copia de respaldo.

  NOTA

  Solo MRS 3.1.0 o posterior admite la copia de respaldo de datos en OBS.

Paso 8 Haga clic en **OK**.

Paso 9 En la columna **Operation** de la tarea creada en la lista de tareas de copia de respaldo, haga clic en **More** y seleccione **Back Up Now** para ejecutar la tarea de copia de respaldo.

Después de ejecutar la tarea de copia de respaldo, el sistema crea automáticamente un subdirectorio para cada tarea de copia de respaldo en el directorio de copia de respaldo. El formato del nombre del subdirectorio es de *Backup task name_Task creation time* y el subdirectorio se utiliza para guardar los archivos de copia de respaldo de origen de datos. El formato del nombre del archivo de copia de respaldo es *Version_Data source_Task execution time***.tar.gz**.

----Fin

7.10.2.7 Copia de respaldo de datos de servicio de HBase

Escenario

Para garantizar la seguridad de los datos de servicio de HBase de forma rutinaria o antes de una operación importante en HBase (como la actualización o la migración), debe realizar una copia de respaldo de los datos de servicio de HBase. Los datos de copia de respaldo se pueden utilizar para recuperar el sistema si se produce una excepción o la operación no ha logrado el resultado esperado, minimizando los impactos adversos en los servicios.

Puede crear una tarea de copia de respaldo en FusionInsight Manager para hacer una copia de respaldo de los datos del servicio de HBase. Se admiten tareas de copia de respaldo tanto automáticas como manuales.

Las siguientes situaciones pueden ocurrir durante la copia de respaldo de datos del servicio HBase:

- Cuando un usuario crea una tabla HBase, **KEEP_DELETED_CELLS** se establece en **false** de forma predeterminada. Cuando el usuario hace una copia de respaldo de esta

tabla de HBase, los datos eliminados se respaldarán y los datos basura pueden existir después de la restauración de los datos. Este parámetro se puede establecer en **true** manualmente cuando se crea una tabla HBase en función de los requisitos de servicio.

- Cuando un usuario especifica manualmente la marca de tiempo al escribir datos en una tabla HBase y la hora especificada es anterior a la última hora de copia de respaldo de la tabla HBase, es posible que no se realice una copia de respaldo de los datos nuevos en tareas de copia de respaldo incrementales.
- La función de copia de respaldo de HBase no puede realizar copias de respaldo de las listas de control de acceso (ACL) para leer, escribir, ejecutar, crear y administrar espacios de nombres o globales de HBase. Después de restaurar los datos de HBase, debe restablecer los permisos de rol en el FusionInsight Manager.
- Si los datos de copia de respaldo del clúster en espera se pierden en una tarea de copia de respaldo de HBase existente, la siguiente copia de respaldo incremental fallará y deberá crear una tarea de copia de respaldo de HBase de nuevo. Sin embargo, la siguiente tarea de copia de respaldo completa será normal.

Prerrequisitos

- Si es necesario realizar una copia de respaldo de los datos en el HDFS remoto, ha preparado un clúster en espera para la copia de respaldo de los datos. El modo de autenticación del clúster en espera es el mismo que el del clúster activo. Para otros modos de copia de respaldo, no es necesario preparar el clúster en espera.
- Si el clúster activo se despliega en modo de seguridad y los clústeres activo y en espera no son gestionados por el mismo FusionInsight Manager, se ha configurado la confianza mutua. Para obtener más información, consulte **Configuración de la confianza mutua Cross-Manager entre clústeres**. Si el clúster activo se despliega en modo normal, no se requiere confianza mutua.
- Se ha configurado la replicación entre clústeres para los clústeres activo y en espera. Para obtener más información, consulte **Habilitación de la replicación entre clústeres**.
- El tiempo es consistente entre los clústeres activos y en espera y los servicios NTP en los clústeres activos y en espera utilizan la misma fuente de tiempo.
- Las políticas de copia de respaldo, incluido el tipo de tarea de copia de respaldo, el período, el objeto de copia de respaldo, el directorio de copia de respaldo y la cola de Yarn que requiere la tarea de copia de respaldo, se planifican según los requisitos de servicio.
- El HDFS del clúster en espera tiene suficiente espacio. Se recomienda guardar los archivos de copia de respaldo en un directorio personalizado.
- En el cliente HDFS, ha ejecutado el comando **hdfs lsSnapshottableDir** como usuario **hdfs** para comprobar la lista de directorios para los que se han creado instantáneas HDFS en el clúster actual y asegurarse de que el directorio o subdirectorio principal HDFS donde se almacenan los archivos de datos que se van a hacer una copia de respaldo no tiene Instantáneas de HDFS. De lo contrario, no se puede crear la tarea de copia de respaldo.
- Si desea realizar una copia de respaldo de los datos en el NAS, ha desplegado el servidor NAS por adelantado.
- Los parámetros **fs.defaultFS** de HBase son los mismos que los de Yarn y HDFS.

Procedimiento

Paso 1 En FusionInsight Manager, seleccione **O&M** > **Backup and Restoration** > **Backup Management**.

Paso 2 Haga clic en **Create**.

Paso 3 Establezca **Name** en el nombre de la tarea de copia de respaldo.

Paso 4 Seleccione el clúster que se va a operar desde **Backup Object**.

Paso 5 Establezca **Mode** en el tipo de tarea de copia de respaldo.

Periodic indica que la tarea de copia de respaldo es ejecutada por el sistema periódicamente. **Manual** indica que la tarea de copia de respaldo se ejecuta manualmente.

Tabla 7-77 Parámetros de copia de respaldo periódico

Parámetro	Descripción
Started	Indica la hora a la que se inicia la tarea por primera vez.
Period	Indica el intervalo de ejecución de la tarea. Las opciones incluyen **Hours** y **Days**.
Backup Policy	● **Copia de respaldo completa la primera vez y copia de respaldo incremental posteriormente** ● **Copia de respaldo completa cada vez** ● **Copia de respaldo completa una vez cada n veces** **NOTA** ● No se admite la copia de respaldo incremental cuando se realizan copias de respaldo de los datos de Manager y los metadatos de los componentes. Solo se admite **Copia de respaldo completa cada vez**. ● Si **Path Type** se establece en **NFS** o **CIFS**, no se puede utilizar la copia de respaldo incremental. Cuando se utiliza la copia de respaldo incremental para la copia de respaldo de NFS o CIFS, los datos de copia de respaldo completa más recientes se actualizan cada vez que se realiza la copia de respaldo incremental. Por lo tanto, no se genera ningún nuevo punto de recuperación.

Paso 6 En **Configuration**, elija **HBase** > **HBase** bajo **Service data**.

Paso 7 Establezca **Path Type** de **HBase** en un tipo de directorio de copia de respaldo.

Se admiten los siguientes tipos de directorio de copia de respaldo:

- **RemoteHDFS**: indica que los archivos de copia de respaldo se almacenan en el directorio de HDFS del clúster en espera.

  Si selecciona esta opción, establezca los siguientes parámetros:

  – **Destination NameService Name**: indica el nombre de NameService del clúster en espera. Puede establecerlo en el nombre de NameService (**haclusterX**, **haclusterX1**, **haclusterX2**, **haclusterX3**, o **haclusterX4**) del clúster remoto integrado del clúster, o el nombre de NameService de un clúster remoto configurado.

- **IP Mode**: indica el modo de la dirección IP de destino. El sistema selecciona automáticamente el modo de dirección IP en función del tipo de red del clúster, por ejemplo **IPv4** o **IPv6**.
- **Target NameNode IP Address**: indica la dirección IP del plano de servicio NameNode en el clúster en espera. Puede ser de un nodo activo o en espera.
- **Target Path**: indica el directorio HDFS para almacenar los datos de copia de respaldo del clúster en espera. La ruta de almacenamiento no puede ser un directorio oculto de HDFS, como un directorio de instantáneas o papelera de reciclaje, o un directorio de sistema predeterminado, como **/hbase** o **/user/hbase/backup**.
- **Maximum Number of Backup Copies**: indica el número de conjuntos de archivos de copia de respaldo que se pueden retener en el directorio de copia de respaldo.
- **Queue Name**: indica el nombre de la cola de Yarn utilizada para la ejecución de tareas de copia de respaldo. El nombre debe ser el mismo que el nombre de la cola que se está ejecutando correctamente en el clúster.
- **Maximum Number of Maps**: indica el número máximo de map en una tarea de MapReduce. El valor predeterminado es **20**.
- **Maximum Bandwidth of a Map (MB/s)**: indica el ancho de banda máximo de un map. El valor predeterminado es **100**.

- **NFS**: indica que los archivos de copia de respaldo se almacenan en el NAS mediante el protocolo NFS.

  Si selecciona esta opción, establezca los siguientes parámetros:

  - **IP Mode**: indica el modo de la dirección IP de destino. El sistema selecciona automáticamente el modo de dirección IP en función del tipo de red del clúster, por ejemplo **IPv4** o **IPv6**.
  - **Server IP Address**: indica la dirección IP del servidor NAS.
  - **Server Shared Path**: indica el directorio compartido configurado del servidor NAS. (La ruta de acceso compartida del servidor no se puede establecer en el directorio raíz, y el grupo de usuarios y el grupo de propietarios de la ruta de acceso compartida deben ser **nobody:nobody**.)
  - **Maximum Number of Backup Copies**: indica el número de conjuntos de archivos de copia de respaldo que se pueden retener en el directorio de copia de respaldo.
  - **Queue Name**: indica el nombre de la cola de Yarn utilizada para la ejecución de tareas de copia de respaldo. El nombre debe ser el mismo que el nombre de la cola que se está ejecutando correctamente en el clúster.
  - **Maximum Number of Maps**: indica el número máximo de map en una tarea de MapReduce. El valor predeterminado es **20**.
  - **Maximum Bandwidth of a Map (MB/s)**: indica el ancho de banda máximo de un map. El valor predeterminado es **100**.

- **CIFS**: indica que los archivos de copia de respaldo se almacenan en el NAS mediante el protocolo CIFS.

  Si selecciona esta opción, establezca los siguientes parámetros:

  - **IP Mode**: indica el modo de la dirección IP de destino. El sistema selecciona automáticamente el modo de dirección IP en función del tipo de red del clúster, por ejemplo **IPv4** o **IPv6**.
  - **Server IP Address**: indica la dirección IP del servidor NAS.

- **Port**: indica el número de puerto utilizado para conectarse al servidor NAS a través del protocolo CIFS. El valor predeterminado es **445**.
- **Username**: indica el nombre de usuario establecido cuando se configura el protocolo CIFS.
- **Password**: indica la contraseña establecida cuando se configura el protocolo CIFS.
- **Server Shared Path**: indica el directorio compartido configurado del servidor NAS. (La ruta de acceso compartida del servidor no se puede establecer en el directorio raíz, y el grupo de usuarios y el grupo de propietarios de la ruta de acceso compartida deben ser **nobody:nobody**.)
- **Maximum Number of Backup Copies**: indica el número de conjuntos de archivos de copia de respaldo que se pueden retener en el directorio de copia de respaldo.
- **Queue Name**: indica el nombre de la cola de Yarn utilizada para la ejecución de tareas de copia de respaldo. El nombre debe ser el mismo que el nombre de la cola que se está ejecutando correctamente en el clúster.
- **Maximum Number of Maps**: indica el número máximo de map en una tarea de MapReduce. El valor predeterminado es **20**.
- **Maximum Bandwidth of a Map (MB/s)**: indica el ancho de banda máximo de un map. El valor predeterminado es **100**.

- **SFTP**: indica que los archivos de copia de respaldo se almacenan en el servidor mediante el protocolo SFTP.

  Si selecciona esta opción, establezca los siguientes parámetros:

  - **IP Mode**: indica el modo de la dirección IP de destino. El sistema selecciona automáticamente el modo de dirección IP en función del tipo de red del clúster, por ejemplo **IPv4** o **IPv6**.
  - **Server IP Address**: indica la dirección IP del servidor donde se almacenan los datos de copia de respaldo.
  - **Port**: indica el número de puerto utilizado para conectarse al servidor de copia de respaldo a través del protocolo SFTP. El valor predeterminado es **22**.
  - **Username**: indica el nombre de usuario para conectarse al servidor mediante el protocolo SFTP.
  - **Password**: indica la contraseña para conectarse al servidor mediante el protocolo SFTP.
  - **Server Shared Path**: indica la ruta de copia de respaldo en el servidor SFTP.
  - **Maximum Number of Backup Copies**: indica el número de conjuntos de archivos de copia de respaldo que se pueden retener en el directorio de copia de respaldo.
  - **Queue Name**: indica el nombre de la cola de Yarn utilizada para la ejecución de tareas de copia de respaldo. El nombre debe ser el mismo que el nombre de la cola que se está ejecutando correctamente en el clúster.
  - **Maximum Number of Maps**: indica el número máximo de map en una tarea de MapReduce. El valor predeterminado es **20**.
  - **Maximum Bandwidth of a Map (MB/s)**: indica el ancho de banda máximo de un map. El valor predeterminado es **100**.

Paso 8 Establezca **Maximum Number of Recovery Points** en el número de instantáneas que se pueden retener en el clúster.

Paso 9 Establezca **Backup Content** en una o varias tablas de HBase para realizar una copia de respaldo.

Puede seleccionar los datos de copia de respaldo utilizando cualquiera de los siguientes métodos:

- Adición de un archivo de datos de copia de respaldo

  Haga clic en el nombre de una base de datos en el árbol de navegación para mostrar todas las tablas de la base de datos y seleccione las tablas especificadas.

- Selección del uso de expresiones regulares

  a. Haga clic en **Query Regular Expression**.

  b. Introduzca el espacio de nombres donde se encuentran las tablas HBase en el primer cuadro de texto según se le solicite. El espacio de nombres debe ser el mismo que el espacio de nombres existente, por ejemplo, **default**.

  c. Escriba una expresión regular en el segundo cuadro de texto. Se admiten expresiones regulares estándar. Por ejemplo, para obtener todas las tablas del espacio de nombres, escriba **([\s\S]*?)**. Para obtener tablas cuyos nombres consisten en letras y dígitos, por ejemplo, **tb1**, escriba **tb\d***.

  d. Haga clic en **Refresh** para ver las tablas mostradas en **Directory Name**.

  e. Haga clic en **Synchronize** para guardar el resultado.

  NOTA

  – Cuando escriba expresiones regulares, haga clic en + o − para agregar o eliminar una expresión.

  – Si la tabla o el directorio seleccionado no es correcto, haga clic en **Clear Selected Node** para anular la selección.

Paso 10 Haga clic en **Verify** para comprobar si la tarea de copia de respaldo está configurada correctamente.

Las posibles causas de falla de verificación son las siguientes:

- La dirección IP del NameNode de destino es incorrecta.
- El nombre de la cola es incorrecto.
- El directorio primario o subdirectorio del directorio HDFS donde se almacenan los archivos de datos de la tabla HBase que se van a realizar una copia de respaldo tiene instantáneas HDFS.
- El directorio o la tabla que se va a hacer una copia de respaldo no existe.

Paso 11 Haga clic en **OK**.

Paso 12 En la columna **Operation** de la tarea creada en la lista de tareas de copia de respaldo, haga clic en **More** y seleccione **Back Up Now** para ejecutar la tarea de copia de respaldo.

Después de ejecutar la tarea de copia de respaldo, el sistema crea automáticamente un subdirectorio para cada tarea de copia de respaldo en el directorio de copia de respaldo. El formato del nombre del subdirectorio es *Backup task name_Data source_Task creation time* y el subdirectorio se utiliza para guardar los últimos archivos de copia de respaldo de origen de datos. Todos los conjuntos de archivos de copia de respaldo se almacenan en los directorios de instantáneas relacionados.

----Fin

7.10.2.8 Copia de respaldo de los datos de NameNode

Escenario

Para garantizar la seguridad de los datos del servicio NameNode de forma rutinaria o antes de una operación importante en NameNode (como la actualización o la migración), debe realizar una copia de respaldo de los datos de NameNode. Los datos de copia de respaldo se pueden utilizar para recuperar el sistema si se produce una excepción o la operación no ha logrado el resultado esperado, minimizando los impactos adversos en los servicios.

Puede crear una tarea de copia de respaldo en FusionInsight Manager para realizar una copia de respaldo de los datos de NameNode. Se admiten tareas de copia de respaldo tanto automáticas como manuales.

Prerrequisitos

- Si es necesario realizar una copia de respaldo de los datos en el HDFS remoto, ha preparado un clúster en espera para la copia de respaldo de los datos. El modo de autenticación del clúster en espera es el mismo que el del clúster activo. Para otros modos de copia de respaldo, no es necesario preparar el clúster en espera.
- Si el clúster activo se despliega en modo de seguridad y los clústeres activo y en espera no son gestionados por el mismo FusionInsight Manager, se ha configurado la confianza mutua. Para obtener más información, consulte **Configuración de la confianza mutua Cross-Manager entre clústeres**. Si el clúster activo se despliega en modo normal, no se requiere confianza mutua.
- Se ha configurado la replicación entre clústeres para los clústeres activo y en espera. Para obtener más información, consulte **Habilitación de la replicación entre clústeres**.
- El tiempo es consistente entre los clústeres activos y en espera y los servicios NTP en los clústeres activos y en espera utilizan la misma fuente de tiempo.
- El tipo de copia de respaldo, el período, la política y otras especificaciones se han planificado en función de los requisitos de servicio y se ha comprobado si *Data storage path*/**LocalBackup/** tiene suficiente espacio en los nodos de gestión activo y en espera.
- Si desea realizar una copia de respaldo de los datos en el NAS, ha desplegado el servidor NAS por adelantado.
- Si desea realizar una copia de respaldo de los datos en OBS, ha conectado el clúster actual a OBS y tiene el permiso para acceder a OBS.

Procedimiento

Paso 1 En FusionInsight Manager, seleccione **O&M** > **Backup and Restoration** > **Backup Management**.

Paso 2 Haga clic en **Create**.

Paso 3 Establezca **Name** en el nombre de la tarea de copia de respaldo.

Paso 4 Seleccione el clúster que se va a operar desde **Backup Object**.

Paso 5 Establezca **Mode** en el tipo de tarea de copia de respaldo.

Periodic indica que la tarea de copia de respaldo es ejecutada por el sistema periódicamente. **Manual** indica que la tarea de copia de respaldo se ejecuta manualmente.

Tabla 7-78 Parámetros de copia de respaldo periódico

Parámetro	Descripción
Started	Indica la hora a la que se inicia la tarea por primera vez.
Period	Indica el intervalo de ejecución de la tarea. Las opciones incluyen **Hours** y **Days**.
Backup Policy	Solo se admite **Copia de respaldo completa cada vez**. **NOTA** ● No se admite la copia de respaldo incremental cuando se realizan copias de respaldo de los datos de Manager y los metadatos de los componentes. Solo se admite **Copia de respaldo completa cada vez**. ● Si **Path Type** se establece en **NFS** o **CIFS**, no se puede utilizar la copia de respaldo incremental. Cuando se utiliza la copia de respaldo incremental para la copia de respaldo de NFS o CIFS, los datos de copia de respaldo completa más recientes se actualizan cada vez que se realiza la copia de respaldo incremental. Por lo tanto, no se genera ningún nuevo punto de recuperación.

Paso 6 En **Configuration**, seleccione **NameNode**.

Paso 7 Establezca **Path Type** de **NameNode** en un tipo de directorio de copia de respaldo.

Se admiten los siguientes tipos de directorio de copia de respaldo:

- **LocalDir**: indica que los archivos de copia de respaldo se almacenan en el disco local del nodo de gestión activo y el nodo de gestión en espera sincroniza automáticamente los archivos de copia de respaldo. De forma predeterminada, los archivos de copia de respaldo se almacenan en *Data storage path*/**LocalBackup/**.
  - **Maximum Number of Backup Copies**: indica el número de conjuntos de archivos de copia de respaldo que se pueden retener en el directorio de copia de respaldo.
  - **NameService Name**: indica el nombre NameService del directorio de copia de respaldo. El valor predeterminado es **hacluster**.
- **RemoteHDFS**: indica que los archivos de copia de respaldo se almacenan en el directorio de HDFS del clúster en espera. Si selecciona esta opción, establezca los siguientes parámetros:
  - **Destination NameService Name**: indica el nombre de NameService del clúster en espera. Puede establecerlo en el nombre de NameService (**haclusterX**, **haclusterX1**, **haclusterX2**, **haclusterX3**, o **haclusterX4**) del clúster remoto integrado del clúster, o el nombre de NameService de un clúster remoto configurado.
  - **IP Mode**: indica el modo de la dirección IP de destino. El sistema selecciona automáticamente el modo de dirección IP en función del tipo de red del clúster, por ejemplo **IPv4** o **IPv6**.
  - **Target NameNode IP Address**: indica la dirección IP del plano de servicio del NameNode en el clúster en espera.
  - **Target Path** indica la ruta para almacenar los archivos de copia de respaldo.
  - **Maximum Number of Backup Copies**: indica el número de conjuntos de archivos de copia de respaldo que se pueden retener en el directorio de copia de respaldo.

  - **NameService Name**: indica el nombre NameService del directorio de copia de respaldo. El valor predeterminado es **hacluster**.
  - **Queue Name**: indica el nombre de la cola de Yarn utilizada para la ejecución de tareas de copia de respaldo. El nombre debe ser el mismo que el nombre de la cola que se está ejecutando correctamente en el clúster.
- **NFS**: indica que los archivos de copia de respaldo se almacenan en el NAS mediante el protocolo NFS. Si selecciona esta opción, establezca los siguientes parámetros:
  - **IP Mode**: indica el modo de la dirección IP de destino. El sistema selecciona automáticamente el modo de dirección IP en función del tipo de red del clúster, por ejemplo **IPv4** o **IPv6**.
  - **Server IP Address**: indica la dirección IP del servidor NAS.
  - **Server Shared Path**: indica el directorio compartido configurado del servidor NAS. (La ruta de acceso compartida del servidor no se puede establecer en el directorio raíz, y el grupo de usuarios y el grupo de propietarios de la ruta de acceso compartida deben ser **nobody:nobody**.)
  - **Maximum Number of Backup Copies**: indica el número de conjuntos de archivos de copia de respaldo que se pueden retener en el directorio de copia de respaldo.
  - **NameService Name**: indica el nombre NameService del directorio de copia de respaldo. El valor predeterminado es **hacluster**.
- **CIFS**: indica que los archivos de copia de respaldo se almacenan en el NAS mediante el protocolo CIFS. Si selecciona esta opción, establezca los siguientes parámetros:
  - **IP Mode**: indica el modo de la dirección IP de destino. El sistema selecciona automáticamente el modo de dirección IP en función del tipo de red del clúster, por ejemplo **IPv4** o **IPv6**.
  - **Server IP Address**: indica la dirección IP del servidor NAS.
  - **Port**: indica el número de puerto utilizado para conectarse al servidor NAS a través del protocolo CIFS. El valor predeterminado es **445**.
  - **Username**: indica el nombre de usuario establecido cuando se configura el protocolo CIFS.
  - **Password**: indica la contraseña establecida cuando se configura el protocolo CIFS.
  - **Server Shared Path**: indica el directorio compartido configurado del servidor NAS. (La ruta de acceso compartida del servidor no se puede establecer en el directorio raíz, y el grupo de usuarios y el grupo de propietarios de la ruta de acceso compartida deben ser **nobody:nobody**.)
  - **Maximum Number of Backup Copies**: indica el número de conjuntos de archivos de copia de respaldo que se pueden retener en el directorio de copia de respaldo.
  - **NameService Name**: indica el nombre NameService del directorio de copia de respaldo. El valor predeterminado es **hacluster**.
- **SFTP**: indica que los archivos de copia de respaldo se almacenan en el servidor mediante el protocolo SFTP.

  Si selecciona esta opción, establezca los siguientes parámetros:
  - **IP Mode**: indica el modo de la dirección IP de destino. El sistema selecciona automáticamente el modo de dirección IP en función del tipo de red del clúster, por ejemplo **IPv4** o **IPv6**.
  - **Server IP Address**: indica la dirección IP del servidor donde se almacenan los datos de copia de respaldo.

- **Port**: indica el número de puerto utilizado para conectarse al servidor de copia de respaldo a través del protocolo SFTP. El valor predeterminado es **22**.
- **Username**: indica el nombre de usuario para conectarse al servidor mediante el protocolo SFTP.
- **Password**: indica la contraseña para conectarse al servidor mediante el protocolo SFTP.
- **Server Shared Path**: indica la ruta de copia de respaldo en el servidor SFTP.
- **Maximum Number of Backup Copies**: indica el número de conjuntos de archivos de copia de respaldo que se pueden retener en el directorio de copia de respaldo.
- **NameService Name**: indica el nombre NameService del directorio de copia de respaldo. El valor predeterminado es **hacluster**.

- **OBS**: indica que los archivos de copia de respaldo se almacenan en OBS.

  Si selecciona esta opción, establezca los siguientes parámetros:

  - **Target Path**: indica el directorio OBS para almacenar los datos de copia de respaldo.
  - **Maximum Number of Backup Copies**: indica el número de conjuntos de archivos de copia de respaldo que se pueden retener en el directorio de copia de respaldo.
  - **NameService Name**: indica el nombre NameService del directorio de copia de respaldo. El valor predeterminado es **hacluster**.

    NOTA

    Solo MRS 3.1.0 o posterior admite la copia de respaldo de datos en OBS.

Paso 8 Haga clic en **OK**.

Paso 9 En la columna **Operation** de la tarea creada en la lista de tareas de copia de respaldo, haga clic en **More** y seleccione **Back Up Now** para ejecutar la tarea de copia de respaldo.

Después de ejecutar la tarea de copia de respaldo, el sistema crea automáticamente un subdirectorio para cada tarea de copia de respaldo en el directorio de copia de respaldo. El formato del nombre del subdirectorio es de *Backup task name_Task creation time* y el subdirectorio se utiliza para guardar los archivos de copia de respaldo de origen de datos.

El formato del nombre del archivo de copia de respaldo es *Version_Data source_Task execution time***.tar.gz**.

----Fin

7.10.2.9 Copia de respaldo de datos de servicio de HDFS

Escenario

Para garantizar la seguridad de los datos de servicio HDFS de forma rutinaria o antes de una operación importante en HDFS (como la actualización o la migración), debe realizar una copia de respaldo de los datos de servicio HDFS. Los datos de copia de respaldo se pueden utilizar para recuperar el sistema si se produce una excepción o la operación no ha logrado el resultado esperado, minimizando los impactos adversos en los servicios.

Puede crear una tarea de copia de respaldo en FusionInsight Manager para realizar una copia de respaldo de los datos de servicio HDFS. Se admiten tareas de copia de respaldo tanto automáticas como manuales.

NOTA

Los directorios cifrados no se pueden hacer copias de respaldo ni restaurar.

Prerrequisitos

- Si es necesario realizar una copia de respaldo de los datos en el HDFS remoto, ha preparado un clúster en espera para la copia de respaldo de los datos. El modo de autenticación del clúster en espera es el mismo que el del clúster activo. Para otros modos de copia de respaldo, no es necesario preparar el clúster en espera.
- Si el clúster activo se despliega en modo de seguridad y los clústeres activo y en espera no son gestionados por el mismo FusionInsight Manager, se ha configurado la confianza mutua. Para obtener más información, consulte **Configuración de la confianza mutua Cross-Manager entre clústeres**. Si el clúster activo se despliega en modo normal, no se requiere confianza mutua.
- Se ha configurado la replicación entre clústeres para los clústeres activos y en espera. Para obtener más información, consulte **Habilitación de la replicación entre clústeres**.
- El tiempo es consistente entre los clústeres activos y en espera y los servicios NTP en los clústeres activos y en espera utilizan la misma fuente de tiempo.
- Las políticas de copia de respaldo, incluido el tipo de tarea de copia de respaldo, el período, el objeto de copia de respaldo, el directorio de copia de respaldo y la cola de Yarn que requiere la tarea de copia de respaldo, se planifican según los requisitos de servicio.
- El HDFS del clúster en espera tiene suficiente espacio. Se recomienda guardar los archivos de copia de respaldo en un directorio personalizado.
- En el cliente HDFS, ha ejecutado el comando **hdfs lsSnapshottableDir** como usuario **hdfs** para comprobar la lista de directorios para los que se han creado instantáneas HDFS en el clúster actual y asegurarse de que el directorio o subdirectorio principal HDFS donde se almacenan los archivos de datos que se van a hacer una copia de respaldo no tiene instantáneas de HDFS. De lo contrario, no se puede crear la tarea de copia de respaldo.
- Si desea realizar una copia de respaldo de los datos en el NAS, ha desplegado el servidor NAS por adelantado.

Procedimiento

Paso 1 En FusionInsight Manager, seleccione **O&M** > **Backup and Restoration** > **Backup Management**.

Paso 2 Haga clic en **Create**.

Paso 3 Establezca **Name** en el nombre de la tarea de copia de respaldo.

Paso 4 Seleccione el clúster que se va a operar desde **Backup Object**.

Paso 5 Establezca **Mode** en el tipo de tarea de copia de respaldo.

Periodic indica que la tarea de copia de respaldo es ejecutada por el sistema periódicamente. **Manual** indica que la tarea de copia de respaldo se ejecuta manualmente.

Tabla 7-79 Parámetros de copia de respaldo periódico

Parámetro	Descripción
Started	Indica la hora a la que se inicia la tarea por primera vez.
Period	Indica el intervalo de ejecución de la tarea. Las opciones incluyen **Hours** y **Days**.
Backup Policy	● **Copia de respaldo completa la primera vez y copia de respaldo incremental posteriormente** ● **Copia de respaldo completa cada vez** ● **Copia de respaldo completa una vez cada n veces** **NOTA** ● No se admite la copia de respaldo incremental cuando se realizan copias de respaldo de los datos de Manager y los metadatos de los componentes. Solo se admite **Copia de respaldo completa cada vez**. ● Si **Path Type** se establece en **NFS** o **CIFS**, no se puede utilizar la copia de respaldo incremental. Cuando se utiliza la copia de respaldo incremental para la copia de respaldo de NFS o CIFS, los datos de copia de respaldo completa más recientes se actualizan cada vez que se realiza la copia de respaldo incremental. Por lo tanto, no se genera ningún nuevo punto de recuperación.

Paso 6 En **Configuration**, seleccione **HDFS**.

Paso 7 Establezca **Path Type** de **HDFS** en un tipo de directorio de copia de respaldo.

Se admiten los siguientes tipos de directorio de copia de respaldo:

- **RemoteHDFS**: indica que los archivos de copia de respaldo se almacenan en el directorio de HDFS del clúster en espera.

  Si selecciona esta opción, establezca los siguientes parámetros:

  – **Destination NameService Name**: indica el nombre de NameService del clúster en espera. Puede establecerlo en el nombre de NameService (**haclusterX**, **haclusterX1**, **haclusterX2**, **haclusterX3**, o **haclusterX4**) del clúster remoto integrado del clúster, o el nombre de NameService de un clúster remoto configurado.

  – **IP Mode**: indica el modo de la dirección IP de destino. El sistema selecciona automáticamente el modo de dirección IP en función del tipo de red del clúster, por ejemplo **IPv4** o **IPv6**.

  – **Target NameNode IP Address**: indica la dirección IP del plano de servicio NameNode en el clúster en espera. Puede ser de un nodo activo o en espera.

  – **Target Path**: indica el directorio HDFS para almacenar los datos de copia de respaldo del clúster en espera. La ruta de almacenamiento no puede ser un directorio oculto de HDFS, como un directorio de instantáneas o papelera de reciclaje, o un directorio de sistema predeterminado, como **/hbase** o **/user/hbase/backup**.

  – **Maximum Number of Backup Copies**: indica el número de conjuntos de archivos de copia de respaldo que se pueden retener en el directorio de copia de respaldo.

- **Queue Name**: indica el nombre de la cola de Yarn utilizada para la ejecución de tareas de copia de respaldo. El nombre debe ser el mismo que el nombre de la cola que se está ejecutando correctamente en el clúster.
- **Maximum Number of Maps**: indica el número máximo de map en una tarea de MapReduce. El valor predeterminado es **20**.
- **Maximum Bandwidth of a Map (MB/s)**: indica el ancho de banda máximo de un map. El valor predeterminado es **100**.
- **NameService Name**: indica el nombre NameService del directorio de copia de respaldo. El valor predeterminado es **hacluster**.

- **NFS**: indica que los archivos de copia de respaldo se almacenan en el NAS mediante el protocolo NFS.

  Si selecciona esta opción, establezca los siguientes parámetros:

  - **IP Mode**: indica el modo de la dirección IP de destino. El sistema selecciona automáticamente el modo de dirección IP en función del tipo de red del clúster, por ejemplo **IPv4** o **IPv6**.
  - **Server IP Address**: indica la dirección IP del servidor NAS.
  - **Maximum Number of Backup Copies**: indica el número de conjuntos de archivos de copia de respaldo que se pueden retener en el directorio de copia de respaldo.
  - **Server Shared Path**: indica el directorio compartido configurado del servidor NAS. (La ruta de acceso compartida del servidor no se puede establecer en el directorio raíz, y el grupo de usuarios y el grupo de propietarios de la ruta de acceso compartida deben ser **nobody:nobody**.)
  - **Queue Name**: indica el nombre de la cola de Yarn utilizada para la ejecución de tareas de copia de respaldo. El nombre debe ser el mismo que el nombre de la cola que se está ejecutando correctamente en el clúster.
  - **Maximum Number of Maps**: indica el número máximo de map en una tarea de MapReduce. El valor predeterminado es **20**.
  - **Maximum Bandwidth of a Map (MB/s)**: indica el ancho de banda máximo de un map. El valor predeterminado es **100**.
  - **NameService Name**: indica el nombre NameService del directorio de copia de respaldo. El valor predeterminado es **hacluster**.

- **CIFS**: indica que los archivos de copia de respaldo se almacenan en el NAS mediante el protocolo CIFS. Si selecciona esta opción, establezca los siguientes parámetros:
  - **IP Mode**: indica el modo de la dirección IP de destino. El sistema selecciona automáticamente el modo de dirección IP en función del tipo de red del clúster, por ejemplo **IPv4** o **IPv6**.
  - **Server IP Address**: indica la dirección IP del servidor NAS.
  - **Port**: indica el número de puerto utilizado para conectarse al servidor NAS a través del protocolo CIFS. El valor predeterminado es **445**.
  - **Username**: indica el nombre de usuario establecido cuando se configura el protocolo CIFS.
  - **Password**: indica la contraseña establecida cuando se configura el protocolo CIFS.
  - **Maximum Number of Backup Copies**: indica el número de conjuntos de archivos de copia de respaldo que se pueden retener en el directorio de copia de respaldo.
  - **Server Shared Path**: indica el directorio compartido configurado del servidor NAS. (La ruta de acceso compartida del servidor no se puede establecer en el

directorio raíz, y el grupo de usuarios y el grupo de propietarios de la ruta de acceso compartida deben ser **nobody:nobody**.)

- **Queue Name**: indica el nombre de la cola de Yarn utilizada para la ejecución de tareas de copia de respaldo. El nombre debe ser el mismo que el nombre de la cola que se está ejecutando correctamente en el clúster.
- **Maximum Number of Maps**: indica el número máximo de map en una tarea de MapReduce. El valor predeterminado es **20**.
- **Maximum Bandwidth of a Map (MB/s)**: indica el ancho de banda máximo de un map. El valor predeterminado es **100**.
- **NameService Name**: indica el nombre NameService del directorio de copia de respaldo. El valor predeterminado es **hacluster**.

- **SFTP**: indica que los archivos de copia de respaldo se almacenan en el servidor mediante el protocolo SFTP.

  Si selecciona esta opción, establezca los siguientes parámetros:

  - **IP Mode**: indica el modo de la dirección IP de destino. El sistema selecciona automáticamente el modo de dirección IP en función del tipo de red del clúster, por ejemplo **IPv4** o **IPv6**.
  - **Server IP Address**: indica la dirección IP del servidor donde se almacenan los datos de copia de respaldo.
  - **Port**: indica el número de puerto utilizado para conectarse al servidor de copia de respaldo a través del protocolo SFTP. El valor predeterminado es **22**.
  - **Username**: indica el nombre de usuario para conectarse al servidor mediante el protocolo SFTP.
  - **Password**: indica la contraseña para conectarse al servidor mediante el protocolo SFTP.
  - **Server Shared Path**: indica la ruta de copia de respaldo en el servidor SFTP.
  - **Maximum Number of Backup Copies**: indica el número de conjuntos de archivos de copia de respaldo que se pueden retener en el directorio de copia de respaldo.
  - **Queue Name**: indica el nombre de la cola de Yarn utilizada para la ejecución de tareas de copia de respaldo. El nombre debe ser el mismo que el nombre de la cola que se está ejecutando correctamente en el clúster.
  - **Maximum Number of Maps**: indica el número máximo de map en una tarea de MapReduce. El valor predeterminado es **20**.
  - **Maximum Bandwidth of a Map (MB/s)**: indica el ancho de banda máximo de un map. El valor predeterminado es **100**.
  - **NameService Name**: indica el nombre NameService del directorio de copia de respaldo. El valor predeterminado es **hacluster**.

Paso 8 Establezca **Maximum Number of Recovery Points** en el número de instantáneas que se pueden retener en el clúster.

Paso 9 Establezca **Backup Content** en uno o varios directorios HDFS para realizar copias de respaldo según los requisitos de servicio.

Puede seleccionar los datos de copia de respaldo utilizando cualquiera de los siguientes métodos:

- Adición de un archivo de datos de copia de respaldo

  Haga clic en el nombre de una base de datos en el árbol de navegación para mostrar todas las tablas de la base de datos y seleccione las tablas especificadas.

- Selección del uso de expresiones regulares
  a. Haga clic en **Query Regular Expression**.
  b. Introduzca la ruta completa del directorio principal del directorio en el primer cuadro de texto según se le solicite. El directorio debe ser el mismo que el directorio existente, por ejemplo, **/tmp**.
  c. Escriba una expresión regular en el segundo cuadro de texto. Se admiten expresiones regulares estándares. Por ejemplo, para obtener todos los archivos o subdirectorios en el directorio principal, escriba **([\s\S]*?)**. Para obtener archivos cuyos nombres consisten en letras y dígitos, por ejemplo, **file*1***, escriba **file\d***.
  d. Haga clic en **Refresh** para ver los directorios mostrados en **Directory Name**.
  e. Haga clic en **Synchronize** para guardar el resultado.

  NOTA

  - Cuando escriba expresiones regulares, haga clic en + o − para agregar o eliminar una expresión.
  - Si la tabla o el directorio seleccionado no es correcto, haga clic en **Clear Selected Node** para anular la selección.
  - El directorio de copia de respaldo no puede contener archivos que se hayan escrito durante mucho tiempo. De lo contrario, la tarea de copia de respaldo fallará. Por lo tanto, no se recomienda realizar operaciones en el directorio de nivel superior, como **/user**, **/tmp** y **/mr-history**.

Paso 10 Haga clic en **Verify** para comprobar si la tarea de copia de respaldo está configurada correctamente.

Las posibles causas de la falla de verificación son las siguientes:

- La dirección IP del NameNode de destino es incorrecta.
- El nombre de la cola es incorrecto.
- El directorio primario o subdirectorio del directorio HDFS donde se almacenan los archivos de datos que se van a realizar una copia de respaldo tiene instantáneas HDFS.
- El directorio o la tabla que se va a hacer una copia de respaldo no existe.
- El nombre del NameService es incorrecto.

Paso 11 Haga clic en **OK**.

Paso 12 En la columna **Operation** de la tarea creada en la lista de tareas de copia de respaldo, haga clic en **More** y seleccione **Back Up Now** para ejecutar la tarea de copia de respaldo.

Después de ejecutar la tarea de copia de respaldo, el sistema crea automáticamente un subdirectorio para cada tarea de copia de respaldo en el directorio de copia de respaldo. El formato del nombre del subdirectorio es *Backup task name_Data source_Task creation time* y el subdirectorio se utiliza para guardar los últimos archivos de copia de respaldo de origen de datos. Todos los conjuntos de archivos de copia de respaldo se almacenan en los directorios de instantáneas relacionados.

----Fin

7.10.2.10 Copia de respaldo de los datos del servicio Hive

Escenario

Para garantizar la seguridad de los datos del servicio Hive de forma rutinaria o antes de una operación importante en Hive (como la actualización o la migración), debe realizar una copia de respaldo de los datos del servicio Hive. Los datos de copia de respaldo se pueden utilizar para recuperar el sistema si se produce una excepción o la operación no ha logrado el resultado esperado, minimizando los impactos adversos en los servicios.

Puede crear una tarea de copia de respaldo en FusionInsight Manager para realizar una copia de respaldo de los datos del servicio de Hive. Se admiten tareas de copia de respaldo tanto automáticas como manuales.

- La copia de respaldo y restauración de Hive no pueden identificar las relaciones de servicio y estructura de objetos como tablas, índices y vistas de Hive. Al ejecutar tareas de copia de respaldo y restauración, debe gestionar puntos de restauración unificados basados en escenarios de servicio para garantizar la ejecución adecuada del servicio.
- La copia de respaldo y restauración de Hive no admiten Hive en tablas de datos RDB. Es necesario realizar copias de respaldo y restaurar tablas de datos originales en bases de datos externas de forma independiente.
- Si los datos de copia de respaldo del clúster en espera se pierden en una tarea de copia de respaldo de Hive existente que contiene tablas de Hive en HBase, la siguiente copia de respaldo incremental fallará y deberá crear una tarea de copia de respaldo de Hive de nuevo. Sin embargo, la siguiente tarea de copia de respaldo completa será normal.
- Después de utilizar la función de copia de respaldo del FusionInsight Manager para hacer una copia de respaldo de los directorios HDFS en el nivel de tabla Hive, las tablas Hive no se pueden eliminar y volver a crear.

Prerrequisitos

- Si es necesario realizar una copia de respaldo de los datos en el HDFS remoto, ha preparado un clúster en espera para la copia de respaldo de los datos. El modo de autenticación del clúster en espera es el mismo que el del clúster activo. Para otros modos de copia de respaldo, no es necesario preparar el clúster en espera.
- Si el clúster activo se despliega en modo de seguridad y los clústeres activo y en espera no son gestionados por el mismo FusionInsight Manager, se ha configurado la confianza mutua. Para obtener más información, consulte **Configuración de la confianza mutua Cross-Manager entre clústeres**. Si el clúster activo se despliega en modo normal, no se requiere confianza mutua.
- Se ha configurado la replicación entre clústeres para los clústeres activo y en espera. Para obtener más información, consulte **Habilitación de la replicación entre clústeres**.
- El tiempo es consistente entre los clústeres activos y en espera y los servicios NTP en los clústeres activos y en espera utilizan la misma fuente de tiempo.
- Las políticas de copia de respaldo, incluido el tipo de tarea de copia de respaldo, el período, el objeto de copia de respaldo, el directorio de copia de respaldo y la cola de Yarn que requiere la tarea de copia de respaldo, se planifican según los requisitos de servicio.
- El HDFS del clúster en espera tiene suficiente espacio. Se recomienda guardar los archivos de copia de respaldo en un directorio personalizado.
- En el cliente HDFS, ha ejecutado el comando **hdfs lsSnapshottableDir** como usuario **hdfs** para comprobar la lista de directorios para los que se han creado instantáneas HDFS

en el clúster actual y asegurarse de que el directorio o subdirectorio principal HDFS donde se almacenan los archivos de datos que se van a hacer una copia de respaldo no tiene Instantáneas de HDFS. De lo contrario, no se puede crear la tarea de copia de respaldo.

- Si desea realizar una copia de respaldo de los datos en el NAS, ha desplegado el servidor NAS por adelantado.

Procedimiento

Paso 1 En FusionInsight Manager, seleccione **O&M** > **Backup and Restoration** > **Backup Management**.

Paso 2 Haga clic en **Create**.

Paso 3 Establezca **Name** en el nombre de la tarea de copia de respaldo.

Paso 4 Seleccione el clúster que se va a operar desde **Backup Object**.

Paso 5 Establezca **Mode** en el tipo de tarea de copia de respaldo.

Periodic indica que la tarea de copia de respaldo es ejecutada por el sistema periódicamente. **Manual** indica que la tarea de copia de respaldo se ejecuta manualmente.

Tabla 7-80 Parámetros de copia de respaldo periódico

Parámetro	Descripción
Started	Indica la hora a la que se inicia la tarea por primera vez.
Period	Indica el intervalo de ejecución de la tarea. Las opciones incluyen **Hours** y **Days**.
Backup Policy	- **Copia de respaldo completa la primera vez y copia de respaldo incremental posteriormente** - **Copia de respaldo completa cada vez** - **Copia de respaldo completa una vez cada n veces** **NOTA** - No se admite la copia de respaldo incremental cuando se realizan copias de respaldo de los datos de Manager y los metadatos de los componentes. Solo se admite **Copia de respaldo completa cada vez**. - Si **Path Type** se establece en **NFS** o **CIFS**, no se puede utilizar la copia de respaldo incremental. Cuando se utiliza la copia de respaldo incremental para la copia de respaldo de NFS o CIFS, los datos de copia de respaldo completa más recientes se actualizan cada vez que se realiza la copia de respaldo incremental. Por lo tanto, no se genera ningún nuevo punto de recuperación.

Paso 6 En **Configuration**, elija **Hive** > **Hive**.

Paso 7 Establezca **Path Type** de **Hive** en un tipo de directorio de copia de respaldo.

Se admiten los siguientes tipos de directorio de copia de respaldo:

- **RemoteHDFS**: indica que los archivos de copia de respaldo se almacenan en el directorio de HDFS del clúster en espera. Si selecciona esta opción, establezca los siguientes parámetros:

  - **Destination NameService Name**: indica el nombre de NameService del clúster en espera. Puede establecerlo en el nombre de NameService (**haclusterX**, **haclusterX1**, **haclusterX2**, **haclusterX3**, o **haclusterX4**) del clúster remoto integrado del clúster, o el nombre de NameService de un clúster remoto configurado.
  - **IP Mode**: indica el modo de la dirección IP de destino. El sistema selecciona automáticamente el modo de dirección IP en función del tipo de red del clúster, por ejemplo **IPv4** o **IPv6**.
  - **Target NameNode IP Address**: indica la dirección IP del plano de servicio NameNode en el clúster en espera. Puede ser de un nodo activo o en espera.
  - **Target Path**: indica el directorio HDFS para almacenar los datos de copia de respaldo del clúster en espera. La ruta de almacenamiento no puede ser un directorio oculto de HDFS, como un directorio de instantáneas o papelera de reciclaje, o un directorio de sistema predeterminado, como **/hbase** o **/user/hbase/backup**.
  - **Maximum Number of Backup Copies**: indica el número de conjuntos de archivos de copia de respaldo que se pueden retener en el directorio de copia de respaldo.
  - **Queue Name**: indica el nombre de la cola de Yarn utilizada para la ejecución de tareas de copia de respaldo. El nombre debe ser el mismo que el nombre de la cola que se está ejecutando correctamente en el clúster.
  - **Maximum Number of Maps**: indica el número máximo de map en una tarea de MapReduce. El valor predeterminado es **20**.
  - **Maximum Bandwidth of a Map (MB/s)**: indica el ancho de banda máximo de un map. El valor predeterminado es **100**.
  - **NameService Name**: indica el nombre NameService del directorio de copia de respaldo. El valor predeterminado es **hacluster**.
- **NFS**: indica que los archivos de copia de respaldo se almacenan en el NAS mediante el protocolo NFS. Si selecciona esta opción, establezca los siguientes parámetros:
  - **IP Mode**: indica el modo de la dirección IP de destino. El sistema selecciona automáticamente el modo de dirección IP en función del tipo de red del clúster, por ejemplo **IPv4** o **IPv6**.
  - **Server IP Address**: indica la dirección IP del servidor NAS.
  - **Maximum Number of Backup Copies**: indica el número de conjuntos de archivos de copia de respaldo que se pueden retener en el directorio de copia de respaldo.
  - **Server Shared Path**: indica el directorio compartido configurado del servidor NAS. (La ruta de acceso compartida del servidor no se puede establecer en el directorio raíz, y el grupo de usuarios y el grupo de propietarios de la ruta de acceso compartida deben ser **nobody:nobody**.)
  - **Queue Name**: indica el nombre de la cola de Yarn utilizada para la ejecución de tareas de copia de respaldo. El nombre debe ser el mismo que el nombre de la cola que se está ejecutando correctamente en el clúster.
  - **Maximum Number of Maps**: indica el número máximo de map en una tarea de MapReduce. El valor predeterminado es **20**.
  - **Maximum Bandwidth of a Map (MB/s)**: indica el ancho de banda máximo de un map. El valor predeterminado es **100**.
  - **NameService Name**: indica el nombre NameService del directorio de copia de respaldo. El valor predeterminado es **hacluster**.

- **CIFS**: indica que los archivos de copia de respaldo se almacenan en el NAS mediante el protocolo CIFS. Si selecciona esta opción, establezca los siguientes parámetros:
  - **IP Mode**: indica el modo de la dirección IP de destino. El sistema selecciona automáticamente el modo de dirección IP en función del tipo de red del clúster, por ejemplo **IPv4** o **IPv6**.
  - **Server IP Address**: indica la dirección IP del servidor NAS.
  - **Port**: indica el número de puerto utilizado para conectarse al servidor NAS a través del protocolo CIFS. El valor predeterminado es **445**.
  - **Username**: indica el nombre de usuario establecido cuando se configura el protocolo CIFS.
  - **Password**: indica la contraseña establecida cuando se configura el protocolo CIFS.
  - **Maximum Number of Backup Copies**: indica el número de conjuntos de archivos de copia de respaldo que se pueden retener en el directorio de copia de respaldo.
  - **Server Shared Path**: indica el directorio compartido configurado del servidor NAS. (La ruta de acceso compartida del servidor no se puede establecer en el directorio raíz, y el grupo de usuarios y el grupo de propietarios de la ruta de acceso compartida deben ser **nobody:nobody**.)
  - **Queue Name**: indica el nombre de la cola de Yarn utilizada para la ejecución de tareas de copia de respaldo. El nombre debe ser el mismo que el nombre de la cola que se está ejecutando correctamente en el clúster.
  - **Maximum Number of Maps**: indica el número máximo de map en una tarea de MapReduce. El valor predeterminado es **20**.
  - **Maximum Bandwidth of a Map (MB/s)**: indica el ancho de banda máximo de un map. El valor predeterminado es **100**.
  - **NameService Name**: indica el nombre NameService del directorio de copia de respaldo. El valor predeterminado es **hacluster**.
- **SFTP**: indica que los archivos de copia de respaldo se almacenan en el servidor mediante el protocolo SFTP.

  Si selecciona esta opción, establezca los siguientes parámetros:
  - **IP Mode**: indica el modo de la dirección IP de destino. El sistema selecciona automáticamente el modo de dirección IP en función del tipo de red del clúster, por ejemplo **IPv4** o **IPv6**.
  - **Server IP Address**: indica la dirección IP del servidor donde se almacenan los datos de copia de respaldo.
  - **Port**: indica el número de puerto utilizado para conectarse al servidor de copia de respaldo a través del protocolo SFTP. El valor predeterminado es **22**.
  - **Username**: indica el nombre de usuario para conectarse al servidor mediante el protocolo SFTP.
  - **Password**: indica la contraseña para conectarse al servidor mediante el protocolo SFTP.
  - **Server Shared Path**: indica la ruta de copia de respaldo en el servidor SFTP.
  - **Maximum Number of Backup Copies**: indica el número de conjuntos de archivos de copia de respaldo que se pueden retener en el directorio de copia de respaldo.
  - **Queue Name**: indica el nombre de la cola de Yarn utilizada para la ejecución de tareas de copia de respaldo. El nombre debe ser el mismo que el nombre de la cola que se está ejecutando correctamente en el clúster.

- **Maximum Number of Maps**: indica el número máximo de map en una tarea de MapReduce. El valor predeterminado es **20**.
- **Maximum Bandwidth of a Map (MB/s)**: indica el ancho de banda máximo de un map. El valor predeterminado es **100**.
- **NameService Name**: indica el nombre NameService del directorio de copia de respaldo. El valor predeterminado es **hacluster**.

Paso 8 Establezca **Maximum Number of Recovery Points** en el número de instantáneas que se pueden retener en el clúster.

Paso 9 Establezca **Backup Content** en una o varias tablas Hive para realizar una copia de respaldo.

Puede seleccionar los datos de copia de respaldo utilizando cualquiera de los siguientes métodos:

- Adición de un archivo de datos de copia de respaldo

  Haga clic en el nombre de una base de datos en el árbol de navegación para mostrar todas las tablas de la base de datos y seleccione las tablas especificadas.
- Selección del uso de expresiones regulares
  a. Haga clic en **Query Regular Expression**.
  b. Introduzca la base de datos en la que se encuentran las tablas de Hive en el primer cuadro de texto según se le solicite. La base de datos debe ser la misma que la base de datos existente, por ejemplo, **default**.
  c. Escriba una expresión regular en el segundo cuadro de texto. Se admiten expresiones regulares estándar. Por ejemplo, para obtener todas las tablas de la base de datos, escriba **([\s\S]*?)**. Para obtener tablas cuyos nombres consisten en letras y dígitos, por ejemplo, **tb1**, escriba **tb\d***.
  d. Haga clic en **Refresh** para ver las tablas mostradas en **Directory Name**.
  e. Haga clic en **Synchronize** para guardar el resultado.

  NOTA

  - Cuando escriba expresiones regulares, haga clic en + o − para agregar o eliminar una expresión.
  - Si la tabla o el directorio seleccionado no es correcto, haga clic en **Clear Selected Node** para anular la selección.

Paso 10 Haga clic en **Verify** para comprobar si la tarea de copia de respaldo está configurada correctamente.

Las posibles causas de falla de verificación son las siguientes:

- La dirección IP del NameNode de destino es incorrecta.
- El nombre de la cola es incorrecto.
- El directorio primario o subdirectorio del directorio HDFS donde se almacenan los archivos de datos que se van a realizar una copia de respaldo tiene instantáneas HDFS.
- El directorio o la tabla que se va a hacer una copia de respaldo no existe.
- El nombre del NameService es incorrecto.

Paso 11 Haga clic en **OK**.

Paso 12 En la columna **Operation** de la tarea creada en la lista de tareas de copia de respaldo, haga clic en **More** y seleccione **Back Up Now** para ejecutar la tarea de copia de respaldo.

Después de ejecutar la tarea de copia de respaldo, el sistema crea automáticamente un subdirectorio para cada tarea de copia de respaldo en el directorio de copia de respaldo. El formato del nombre del subdirectorio es *Backup task name_Data source_Task creation time* y el subdirectorio se utiliza para guardar los últimos archivos de copia de respaldo de origen de datos. Todos los conjuntos de archivos de copia de respaldo se almacenan en los directorios de instantáneas relacionados.

----Fin

7.10.2.11 Copia de respaldo de metadatos de Kafka

Escenario

Para garantizar la seguridad de los metadatos de Kafka o antes de una operación importante de ZooKeeper (como la actualización o la migración), debe hacer una copia de respaldo de los metadatos de Kafka. Los datos de copia de respaldo se pueden utilizar para recuperar el sistema si se produce una excepción o la operación no ha logrado el resultado esperado, minimizando los impactos adversos en los servicios.

Puede crear una tarea de copia de respaldo en FusionInsight Manager para hacer una copia de respaldo de los metadatos de Kafka. Se admiten tareas de copia de respaldo tanto automáticas como manuales.

Prerrequisitos

- Si es necesario realizar una copia de respaldo de los datos en el HDFS remoto, ha preparado un clúster en espera para la copia de respaldo de los datos. El modo de autenticación del clúster en espera es el mismo que el del clúster activo. Para otros modos de copia de respaldo, no es necesario preparar el clúster en espera.
- Si el clúster activo se despliega en modo de seguridad y los clústeres activo y en espera no son gestionados por el mismo FusionInsight Manager, se ha configurado la confianza mutua. Para obtener más información, consulte **Configuración de la confianza mutua Cross-Manager entre clústeres**. Si el clúster activo se despliega en modo normal, no se requiere confianza mutua.
- Se ha configurado la replicación entre clústeres para los clústeres activos y en espera. Para obtener más información, consulte **Habilitación de la replicación entre clústeres**.
- El tiempo es consistente entre los clústeres activos y en espera y los servicios NTP en los clústeres activos y en espera utilizan la misma fuente de tiempo.
- El tipo de copia de respaldo, el período, la política y otras especificaciones se han planificado en función de los requisitos de servicio y se ha comprobado si *Data storage path*/**LocalBackup/** tiene suficiente espacio en los nodos de gestión activo y en espera.
- Si desea realizar una copia de respaldo de los datos en el NAS, ha desplegado el servidor NAS por adelantado.
- Si desea realizar una copia de respaldo de los datos en OBS, ha conectado el clúster actual a OBS y tiene el permiso para acceder a OBS.

Procedimiento

Paso 1 En FusionInsight Manager, seleccione **O&M** > **Backup and Restoration** > **Backup Management**.

Paso 2 Haga clic en **Create**.

Paso 3 Establezca **Name** en el nombre de la tarea de copia de respaldo.

Paso 4 Seleccione el clúster que se va a operar desde **Backup Object**.

Paso 5 Establezca **Mode** en el tipo de tarea de copia de respaldo.

Periodic indica que la tarea de copia de respaldo es ejecutada por el sistema periódicamente. **Manual** indica que la tarea de copia de respaldo se ejecuta manualmente.

Tabla 7-81 Parámetros de copia de respaldo periódico

Parámetro	Descripción
Comenzado	Indica la hora a la que se inicia la tarea por primera vez.
Period	Indica el intervalo de ejecución de la tarea. Las opciones incluyen **Hours** y **Days**.
Backup Policy	● **Copia de respaldo completa la primera vez y copia de respaldo incremental posteriormente** ● **Copia de respaldo completa cada vez** ● **Copia de respaldo completa una vez cada n veces** **NOTA** ● No se admite la copia de respaldo incremental cuando se realizan copias de respaldo de los datos de Manager y los metadatos de los componentes. Solo se admite **Copia de respaldo completa cada vez**. ● Si **Path Type** se establece en **NFS** o **CIFS**, no se puede utilizar la copia de respaldo incremental. Cuando se utiliza la copia de respaldo incremental para la copia de respaldo de NFS o CIFS, los datos de copia de respaldo completa más recientes se actualizan cada vez que se realiza la copia de respaldo incremental. Por lo tanto, no se genera ningún nuevo punto de recuperación.

Paso 6 En **Configuration**, seleccione **Kafka**.

Paso 7 Establezca **Path Type** de **Kafka** en un tipo de directorio de copia de respaldo.

Se admiten los siguientes tipos de directorio de copia de respaldo:

- **LocalDir**: indica que los archivos de copia de respaldo se almacenan en el disco local del nodo de gestión activo y el nodo de gestión en espera sincroniza automáticamente los archivos de copia de respaldo. De forma predeterminada, los archivos de copia de respaldo se almacenan en *Data storage path*/**LocalBackup/**.

  Si selecciona esta opción, debe establecer el número máximo de réplicas para especificar el número de conjuntos de archivos de copia de respaldo que se pueden conservar en el directorio de copia de respaldo.
- **LocalHDFS**: indica que los archivos de copia de respaldo se almacenan en el directorio de HDFS del clúster actual.

  Si selecciona esta opción, establezca los siguientes parámetros:

  – **Target Path**: indica el directorio de HDFS para almacenar los archivos de copia de respaldo. La ruta de almacenamiento no puede ser un directorio oculto de HDFS, como un directorio de instantáneas o papelera de reciclaje, o un directorio de sistema predeterminado, como **/hbase** o **/user/hbase/backup**.

  - **Maximum Number of Backup Copies**: indica el número de conjuntos de archivos de copia de respaldo que se pueden retener en el directorio de copia de respaldo.
  - **Target NameService Name**: indica el nombre de NameService del directorio de copia de respaldo. El valor predeterminado es **hacluster**.

- **RemoteHDFS**: indica que los archivos de copia de respaldo se almacenan en el directorio de HDFS del clúster en espera.

  Si selecciona esta opción, establezca los siguientes parámetros:

  - **Destination NameService Name**: indica el nombre de NameService del clúster en espera. Puede establecerlo en el nombre de NameService (**haclusterX**, **haclusterX1**, **haclusterX2**, **haclusterX3**, o **haclusterX4**) del clúster remoto integrado del clúster, o el nombre de NameService de un clúster remoto configurado.
  - **IP Mode**: indica el modo de la dirección IP de destino. El sistema selecciona automáticamente el modo de dirección IP en función del tipo de red del clúster, por ejemplo **IPv4** o **IPv6**.
  - **Target NameNode IP Address**: indica la dirección IP del plano de servicio NameNode en el clúster en espera. Puede ser de un nodo activo o en espera.
  - **Target Path**: indica el directorio HDFS para almacenar los datos de copia de respaldo del clúster en espera. La ruta de almacenamiento no puede ser un directorio oculto de HDFS, como un directorio de instantáneas o papelera de reciclaje, o un directorio de sistema predeterminado, como **/hbase** o **/user/hbase/backup**.
  - **Maximum Number of Backup Copies**: indica el número de conjuntos de archivos de copia de respaldo que se pueden retener en el directorio de copia de respaldo.
  - **Queue Name**: indica el nombre de la cola de Yarn utilizada para la ejecución de tareas de copia de respaldo. El nombre debe ser el mismo que el nombre de la cola que se está ejecutando correctamente en el clúster.

- **NFS**: indica que los archivos de copia de respaldo se almacenan en el NAS mediante el protocolo NFS.

  Si selecciona esta opción, establezca los siguientes parámetros:

  - **IP Mode**: indica el modo de la dirección IP de destino. El sistema selecciona automáticamente el modo de dirección IP en función del tipo de red del clúster, por ejemplo **IPv4** o **IPv6**.
  - **Server IP Address**: indica la dirección IP del servidor NAS.
  - **Server Shared Path**: indica el directorio compartido configurado del servidor NAS. (La ruta de acceso compartida del servidor no se puede establecer en el directorio raíz, y el grupo de usuarios y el grupo de propietarios de la ruta de acceso compartida deben ser **nobody:nobody**.)
  - **Maximum Number of Backup Copies**: indica el número de conjuntos de archivos de copia de respaldo que se pueden retener en el directorio de copia de respaldo.

- **CIFS**: indica que los archivos de copia de respaldo se almacenan en el NAS mediante el protocolo CIFS.

  Si selecciona esta opción, establezca los siguientes parámetros:

  - **IP Mode**: indica el modo de la dirección IP de destino. El sistema selecciona automáticamente el modo de dirección IP en función del tipo de red del clúster, por ejemplo **IPv4** o **IPv6**.
  - **Server IP Address**: indica la dirección IP del servidor NAS.

  - **Port**: indica el número de puerto utilizado para conectarse al servidor NAS a través del protocolo CIFS. El valor predeterminado es **445**.
  - **Username**: indica el nombre de usuario establecido cuando se configura el protocolo CIFS.
  - **Password**: indica la contraseña establecida cuando se configura el protocolo CIFS.
  - **Server Shared Path**: indica el directorio compartido configurado del servidor NAS. (La ruta de acceso compartida del servidor no se puede establecer en el directorio raíz, y el grupo de usuarios y el grupo de propietarios de la ruta de acceso compartida deben ser **nobody:nobody**.)
  - **Maximum Number of Backup Copies**: indica el número de conjuntos de archivos de copia de respaldo que se pueden retener en el directorio de copia de respaldo.
- **OBS**: indica que los archivos de copia de respaldo se almacenan en OBS.

  Si selecciona esta opción, establezca los siguientes parámetros:
  - **Target Path**: indica el directorio OBS para almacenar los datos de copia de respaldo.
  - **Maximum Number of Backup Copies**: indica el número de conjuntos de archivos de copia de respaldo que se pueden retener en el directorio de copia de respaldo.

    NOTA

    Solo MRS 3.1.0 o posterior admite la copia de respaldo de datos en OBS.

Paso 8 Haga clic en **OK**.

Paso 9 En la columna **Operation** de la tarea creada en la lista de tareas de copia de respaldo, haga clic en **More** y seleccione **Back Up Now** para ejecutar la tarea de copia de respaldo.

Después de ejecutar la tarea de copia de respaldo, el sistema crea automáticamente un subdirectorio para cada tarea de copia de respaldo en el directorio de copia de respaldo. El formato del nombre del subdirectorio es de *Backup task name_Task creation time* y el subdirectorio se utiliza para guardar los archivos de copia de respaldo de origen de datos. El formato del nombre del archivo de copia de respaldo es *Version_Data source_Task execution time***.tar.gz**.

----Fin

7.10.3 Recuperación de datos

7.10.3.1 Restauración de datos del Manager

Escenario

Los datos del administrador deben recuperarse en los siguientes escenarios: los datos se modifican o eliminan inesperadamente y deben restaurarse. Después de que un administrador realice un ajuste de datos críticos en FusionInsight Manager, se produce una excepción o la operación no ha logrado el resultado esperado. Todos los módulos están defectuosos y no están disponibles.

Los administradores del sistema pueden crear una tarea de restauración en FusionInsight Manager para recuperar datos del Manager. Sólo se admiten las tareas de restauración manuales.

AVISO

- La restauración de datos solo se puede realizar cuando la versión del sistema es coherente con la de la copia de respaldo de datos.
- Para recuperar datos cuando el servicio se está ejecutando correctamente, se le aconseja hacer una copia de respaldo manual de los datos de gestión más recientes antes de recuperar los datos. De lo contrario, se perderán los datos del Manager que se generan después de la copia de respaldo de datos y antes de la restauración de datos.

Impacto en el sistema

- En el proceso de restauración, es necesario reiniciar el Controller y el FusionInsight Manager no se puede iniciar sesión u operar durante el reinicio.
- En el proceso de restauración, todos los clústeres deben reiniciarse y no se puede acceder a ellos durante el reinicio.
- Después de la restauración de datos, se perderán los datos, tales como la configuración del sistema, la información del usuario, la información de alarma y la información de auditoría, que se generan después de la copia de respaldo de datos y antes de la restauración de datos. Esto puede provocar un error de consulta de datos o un error de acceso al clúster.
- Después de recuperar los datos del Manager, el sistema fuerza al LdapServer de cada grupo a sincronizar los datos del OLadp.

Prerrequisitos

- Para restaurar datos desde un HDFS remoto, debe preparar un clúster en espera. Si el clúster activo se despliega en modo de seguridad y los clústeres activo y en espera no son gestionados por el mismo FusionInsight Manager, es necesario configurar la confianza mutua del sistema. Para obtener más información, consulte **Configuración de la confianza mutua Cross-Manager entre clústeres**. Si el clúster activo se despliega en modo normal, no se requiere confianza mutua.
- Se ha configurado la replicación entre clústeres para los clústeres activo y en espera. Para obtener más información, consulte **Habilitación de la replicación entre clústeres**.
- El tiempo es consistente entre los clústeres activos y en espera y los servicios NTP en los clústeres activos y en espera utilizan la misma fuente de tiempo.
- El estado de los recursos de OMS y las instancias LdapServer de cada clúster es normal. Si el estado es anormal, no se puede realizar la restauración de datos.
- El estado de los hosts y servicios del clúster es normal. Si el estado es anormal, no se puede realizar la restauración de datos.
- Las topologías del host del clúster durante la restauración de datos y la copia de respaldo de datos son las mismas. Si las topologías son diferentes, no se puede realizar la restauración de datos y es necesario realizar una copia de respaldo de los datos de nuevo.
- Los servicios agregados al clúster durante la restauración de datos y la copia de respaldo de datos son los mismos. Si las topologías son diferentes, no se puede realizar la restauración de datos y es necesario realizar una copia de respaldo de los datos de nuevo.
- Las aplicaciones de capa superior que dependen del clúster se detienen.

Procedimiento

Paso 1 En FusionInsight Manager, seleccione **O&M** > **Backup and Restoration** > **Backup Management**.

Paso 2 En la columna **Operation** de una tarea especificada en la lista de tareas, elija **More** > **View History** para ver los registros históricos de ejecución de tareas de copia de respaldo.

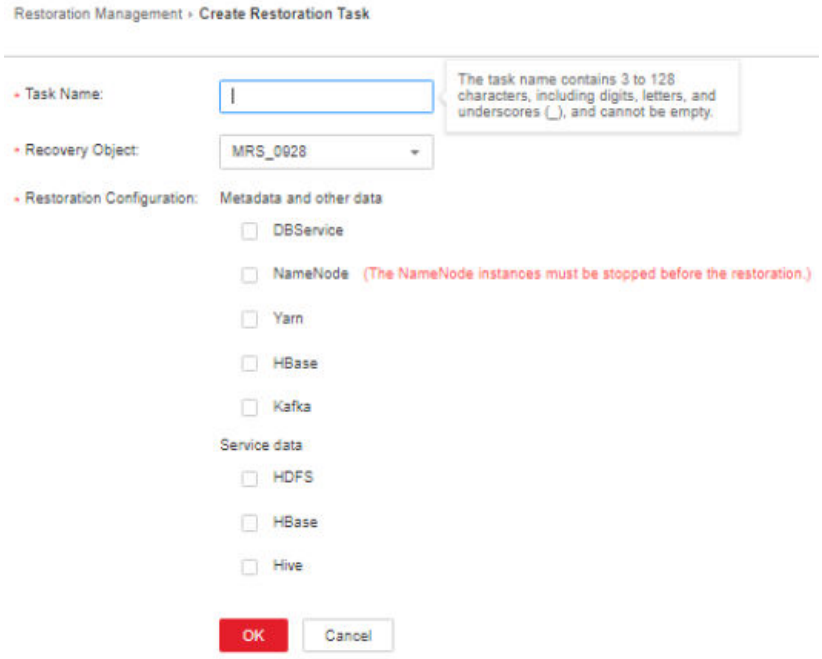
En la ventana que se muestra, busque un registro de éxito especificado y haga clic en **View** en la columna **Backup Path** para ver la información de la ruta de copia de respaldo de la tarea y buscar la siguiente información:

- **Backup Object** especifica el origen de datos de los datos de copia de respaldo.
- **Backup Path** especifica la ruta completa donde se guardan los archivos de copia de respaldo.

  Seleccione el elemento correcto y copie manualmente la ruta completa de los archivos de copia de respaldo de **Backup Path**.

Paso 3 En FusionInsight Manager, seleccione **O&M** > **Backup and Restore** > **Restoring Management**. En la página mostrada, haga clic en **Create**.

Figura 7-59 Creación de una tarea de restauración



Paso 4 Establezca **Task Name** en el nombre de la tarea de restauración.

Paso 5 Ajuste **Recovery Object** a **OMS**.

Paso 6 Seleccione **OMS**.

Paso 7 Establezca **Path Type** de **OMS** en un tipo de directorio de copia de respaldo.

La configuración varía según los tipos de directorios de copia de respaldo:

- **LocalDir**: indica que los archivos de copia de respaldo se almacenan en el disco local del nodo de gestión activa.

Si selecciona **LocalDir**, también debe configurar **Source Path** para que seleccione el archivo de copia de respaldo que se va a restaurar, por ejemplo, *Version_Data source_Task execution time***.tar.gz**.

- **LocalHDFS**: indica que los archivos de copia de respaldo se almacenan en el directorio de HDFS del clúster actual.

  Si selecciona **LocalHDFS**, establezca los siguientes parámetros:

  – **Source Path**: indica la ruta completa del archivo de copia de respaldo en el HDFS, por ejemplo, *Backup path/Backup task name_Task creation time/Version_Data source_Task execution time***.tar.gz**.

  – **Cluster for Restoration**: Introduzca el nombre del clúster utilizado durante la ejecución de la tarea de restauración.

  – **Source NameService Name**: indica el nombre NameService que corresponde al directorio de copia de respaldo cuando se ejecuta una tarea de restauración. El valor predeterminado es **hacluster**.

- **RemoteHDFS**: indica que los archivos de copia de respaldo se almacenan en el directorio de HDFS del clúster en espera.

  Si selecciona **RemoteHDFS**, establezca los siguientes parámetros:

  – **Source NameService Name**: indica el nombre de NameService del clúster de datos de copia de respaldo. Puede introducir el nombre integrado de NameService del clúster remoto, por ejemplo, **haclusterX**, **haclusterX1**, **haclusterX2**, **haclusterX3** o **haclusterX4**. También puede introducir un nombre NameService configurado del clúster remoto.

  – **IP Mode**: indica el modo de la dirección IP de destino. El sistema selecciona automáticamente el modo de dirección IP en función del tipo de red del clúster, por ejemplo **IPv4** o **IPv6**.

  – **Source NameNode IP Address**: indica la dirección IP del plano de servicio NameNode del clúster en espera, que admite el nodo activo o el nodo en espera.

  – **Source Path**: indica la ruta completa del directorio HDFS para almacenar los datos de copia de respaldo del clúster en espera, por ejemplo, *Backup path/Backup task name_Data source_Task creation time/Version_Data source_Task execution time***.tar.gz**.

  – **Source Cluster**: Seleccione el clúster de la cola de Yarn utilizada por los datos de recuperación.

  – **Queue Name**: indica el nombre de la cola de Yarn utilizada para la ejecución de tareas de copia de respaldo. El nombre debe ser el mismo que el nombre de la cola que se está ejecutando correctamente en el clúster.

- **NFS**: indica que los archivos de copia de respaldo se almacenan en el NAS mediante el protocolo NFS. Si selecciona **NFS**, establezca los siguientes parámetros:

  – **IP Mode**: indica el modo de la dirección IP de destino. El sistema selecciona automáticamente el modo de dirección IP en función del tipo de red del clúster, por ejemplo **IPv4** o **IPv6**.

  – **Server IP Address**: indica la dirección IP del servidor NAS.

  – **Source Path**: indica la ruta completa del archivo de copia de respaldo en el servidor NAS, por ejemplo, *Backup path/Backup task name_Data source_Task creation time/Version_Data source_Task execution time***.tar.gz**.

- **CIFS**: indica que los archivos de copia de respaldo se almacenan en el NAS mediante el protocolo CIFS. Si selecciona **CIFS**, establezca los siguientes parámetros:

  - **IP Mode**: indica el modo de la dirección IP de destino. El sistema selecciona automáticamente el modo de dirección IP en función del tipo de red del clúster, por ejemplo **IPv4** o **IPv6**.
  - **Server IP Address**: indica la dirección IP del servidor NAS.
  - **Port**: indica el número de puerto utilizado para conectarse al servidor NAS a través del protocolo CIFS. El valor predeterminado es **445**.
  - **Username**: indica el nombre de usuario establecido cuando se configura el protocolo CIFS.
  - **Password**: indica la contraseña establecida cuando se configura el protocolo CIFS.
  - **Source Path**: indica la ruta completa del archivo de copia de respaldo en el servidor NAS, por ejemplo, *Backup path/Backup task name_Data source_Task creation time/Version_Data source_Task execution time***.tar.gz**.

- **SFTP**: indica que los archivos de copia de respaldo se almacenan en el servidor mediante el protocolo SFTP.

  Si selecciona **SFTP**, establezca los siguientes parámetros:

  - **IP Mode**: indica el modo de la dirección IP de destino. El sistema selecciona automáticamente el modo de dirección IP en función del tipo de red del clúster, por ejemplo **IPv4** o **IPv6**.
  - **Server IP Address**: indica la dirección IP del servidor donde se almacenan los datos de copia de respaldo.
  - **Port**: indica el número de puerto utilizado para conectarse al servidor de copia de respaldo a través del protocolo SFTP. El valor predeterminado es **22**.
  - **Username**: indica el nombre de usuario para conectarse al servidor mediante el protocolo SFTP.
  - **Password**: indica la contraseña para conectarse al servidor mediante el protocolo SFTP.
  - **Source Path**: indica la ruta completa del archivo de copia de respaldo en el servidor de copia de respaldo, por ejemplo, *Backup path/Backup task name_Data source_Task creation time/Version_Data source_Task execution time***.tar.gz**.

- **OBS**: indica que los archivos de copia de respaldo se almacenan en OBS.

  Si selecciona **OBS**, establezca los siguientes parámetros:

  - **Source Path**: indica la ruta de acceso OBS completa de un archivo de copia de respaldo, por ejemplo, *Backup path/Backup task name_Data source_Task creation time/Version_Data source_Task execution time***.tar.gz**.

    NOTA

    Solo MRS 3.1.0 o posterior admite el almacenamiento de archivos de copia de respaldo en OBS.

Paso 8 Haga clic en **OK**.

Paso 9 En la lista de tareas de restauración, busque una tarea creada y haga clic en **Start** en la columna **Operation** para ejecutar la tarea de restauración.

- Después de que la restauración es exitosa, la barra de progreso está en verde.
- Una vez que la restauración se realiza correctamente, la tarea de restauración no se puede ejecutar de nuevo.
- Si la tarea de restauración falla durante la primera ejecución, rectifique el error y haga clic en **Retry** para volver a ejecutar la tarea.

Paso 10 Inicie sesión en los nodos de gestión activo y en espera como **omm** de usuario mediante PuTTY.

Paso 11 Ejecute el siguiente comando para reiniciar OMS:

sh ${BIGDATA_HOME}/om-server/om/sbin/restart-oms.sh

El comando se ejecuta correctamente si se muestra la siguiente información:

```
iniciar HA con éxito.
```

Ejecute **sh ${BIGDATA_HOME}/om-server/om/sbin/status-oms.sh** para comprobar si el **HAAllResOK** del nodo de gestión es **Normal** y si el Administrador de FusionInsight puede iniciar sesión de nuevo. En caso afirmativo, OMS se reinicia correctamente.

Paso 12 En FusionInsight Manager, haga clic en **Cluster**, haga clic en el nombre del clúster de destino y elija **Services** > **KrbServer**. En la página mostrada, elija **More** > **Synchronize Configuration**, haga clic en **OK** y espere a que se sincronice la configuración KrbServer y se reinicie el servicio.

Paso 13 Elija **Cluster**, haga clic en el nombre del clúster deseado y elija **More** > **Synchronize Configurations**, haga clic en **OK** y espere hasta que la configuración del clúster se sincronice correctamente.

Paso 14 En FusionInsight Manager, haga clic en **Cluster**, haga clic en el nombre del clúster de destino y elija **More** > **Restart**. En la página mostrada, introduzca la contraseña del usuario de inicio de sesión actual, haga clic en **OK** y espere a que se reinicie el clúster.

----Fin

7.10.3.2 Restauración de metadatos de ClickHouse

Escenario

Los metadatos de ClickHouse deben restaurarse en los siguientes escenarios: Los datos se modifican o eliminan inesperadamente y deben restaurarse. Una vez que un usuario realiza operaciones importantes (como la actualización y la migración) de ClickHouse se produce una excepción o no se logra el resultado esperado. El componente ClickHouse está defectuoso y no está disponible. Los datos se migran a un nuevo clúster.

Los usuarios pueden crear una tarea de restauración de ClickHouse en FusionInsight Manager. Solo se admiten las tareas de restauración manuales.

AVISO

- Esta función solo es compatible con MRS 3.1.0 o posterior.
- La restauración de datos solo se puede realizar cuando la versión del sistema es coherente con la de la copia de respaldo de datos.
- Para restaurar los metadatos de ClickHouse cuando el servicio se está ejecutando correctamente, se recomienda realizar una copia de respaldo manual de los metadatos de ClickHouse más recientes antes de la restauración. De lo contrario, se perderán los metadatos de ClickHouse que se generan después de la copia de respaldo de datos y antes de la restauración de datos.
- La restauración de metadatos de ClickHouse y la restauración de datos de servicio no se pueden realizar al mismo tiempo. De lo contrario, la restauración de datos de servicio falla. Se recomienda restaurar los datos de servicio después de que se complete la restauración de metadatos.

Impacto en el sistema

- Después de restaurar los metadatos, se pierden los datos generados después de la copia de respaldo de datos y antes de la restauración de datos.
- Después de restaurar los metadatos, es necesario iniciar las aplicaciones de capa superior de ClickHouse.

Prerrequisitos

- Ha comprobado la ruta para almacenar archivos de copia de respaldo de metadatos de ClickHouse.
- Si necesita restaurar datos desde un HDFS remoto, prepare un clúster en espera. Si los clústeres activos y en espera se despliegan en modo de seguridad y no son gestionados por el mismo FusionInsight Manager, se debe configurar la confianza mutua. Para obtener más información, consulte **Configuración de la confianza mutua Cross-Manager entre clústeres**. Si los clústeres activos y en espera se despliegan en modo normal, no se requiere confianza mutua.
- En el clúster activo/en espera, al restaurar datos desde el HDFS remoto al host local, asegúrese de que el valor de **HADOOP_RPC_PROTECTION** de ClickHouse es el mismo que el de **hadoop.rpc.protection** de HDFS.

Procedimiento

Paso 1 En FusionInsight Manager, seleccione **O&M** > **Backup and Restoration** > **Backup Management**.

Paso 2 En la columna **Operation** de la tarea especificada en la lista de tareas, elija **More** > **View History**.

En la ventana que se muestra, seleccione un registro de éxito y haga clic en **View** en la columna **Backup Path** para ver la información de su ruta de copia de respaldo y buscar la siguiente información:

- **Backup Object**: indica el origen de datos de la copia de respaldo.
- **Backup Path**: indica la ruta completa donde se almacenan los archivos de copia de respaldo.

Seleccione la ruta correcta y copie manualmente la ruta completa de los archivos de copia de respaldo de **Backup Path**.

Paso 3 En FusionInsight Manager, seleccione **O&M** > **Backup and Restoration** > **Restoration Management**.

Paso 4 Haga clic en **Create**.

Paso 5 Establezca **Task Name** en el nombre de la tarea de restauración.

Paso 6 Seleccione el clúster que se va a operar desde **Recovery Object**.

Paso 7 En **Restoration Configuration**, seleccione **ClickHouse** en **Metadata and other data**.

Paso 8 Establezca **Path Type** de **ClickHouse** en un tipo de directorio de restauración.

Las configuraciones varían según los tipos de directorio de copia de respaldo:

- **LocalDir**: indica que los datos se restauran desde el disco local del nodo de gestión activo.

  Si selecciona este valor, también debe configurar los siguientes parámetros:

  – **Source Path**: archivo de copia de respaldo que se debe restaurar, por ejemplo, *Backup task name_Data source_Task execution time***.tar.gz**.

  – **Logical Cluster**: Ingrese el clúster lógico ClickHouse cuyos datos se han copiado.

- **RemoteHDFS**: indica que los datos se restauran desde el directorio HDFS del clúster en espera.

  Si selecciona esta opción de valor, también debe configurar los siguientes parámetros:

  – **Source NameService Name**: indica el nombre de NameService del clúster de datos de copia de respaldo, por ejemplo, **hacluster**. Puede obtenerlo en la página **NameService Management** de HDFS del clúster en espera.

  – **IP Mode**: indica el modo de la dirección IP de destino. El sistema selecciona automáticamente el modo de dirección IP en función del tipo de red del clúster, por ejemplo **IPv4** o **IPv6**.

  – **Source NameNode IP Address**: indica la dirección IP del plano de servicio NameNode en el clúster en espera. Puede ser de un nodo activo o en espera.

  – **Source Path**: indica la ruta completa del directorio HDFS para almacenar los datos de copia de respaldo del clúster en espera, por ejemplo, *Backup path/Backup task name_Data source_Task creation time/Data source_Task execution time***.tar.gz**.

Paso 9 Haga clic en **OK**.

Paso 10 En la lista de tareas de restauración, busque la fila donde se encuentra la tarea creada y haga clic en **Start** en la columna **Operation**. En el cuadro de diálogo mostrado, haga clic en **OK** para iniciar la tarea de restauración.

- Después de que la restauración es exitosa, la barra de progreso está en verde.
- Una vez que la restauración se realiza correctamente, la tarea de restauración no se puede ejecutar de nuevo.
- Si la tarea de restauración falla durante la primera ejecución, rectifique el error y haga clic en **Retry** para volver a ejecutar la tarea.

Paso 11 Elija **Cluster** > **Services** e inicie el servicio ClickHouse.

----Fin

7.10.3.3 Restauración de datos de servicio de ClickHouse

Escenario

Los datos de ClickHouse deben restaurarse en los siguientes escenarios: Los datos se modifican o eliminan inesperadamente y deben restaurarse. Una vez que un usuario realiza operaciones importantes (como la actualización y la migración) de ClickHouse se produce una excepción o no se logra el resultado esperado. Todos los módulos están defectuosos y no están disponibles. Los datos se migran a un nuevo clúster.

Los usuarios pueden crear una tarea de restauración de ClickHouse en FusionInsight Manager para restaurar los datos. Solo se admiten las tareas de restauración manuales.

Las funciones de copia de respaldo y restauración de ClickHouse no pueden identificar las relaciones de servicio y estructura de objetos como tablas, índices y vistas de ClickHouse. Al ejecutar tareas de copia de respaldo y restauración, debe gestionar puntos de restauración unificados basados en escenarios de servicio para garantizar la ejecución adecuada del servicio.

AVISO

- Esta función solo es compatible con MRS 3.1.0 o posterior.
- La restauración de datos solo se puede realizar cuando la versión del sistema es coherente con la de la copia de respaldo de datos.
- Para restaurar los datos cuando los servicios son normales, realice primero una copia de respaldo manual de los datos de gestión más recientes y, a continuación, restaure los datos. De lo contrario, los datos de ClickHouse que se generan después de la copia de respaldo de datos y antes de la restauración de datos se perderán.
- La restauración de metadatos de ClickHouse y la restauración de datos de servicio no se pueden realizar al mismo tiempo. De lo contrario, la restauración de datos de servicio falla. Se recomienda restaurar los datos de servicio después de que se complete la restauración de metadatos.

Impacto en el sistema

- Durante la restauración de datos, la autenticación del usuario se detiene y los usuarios no pueden crear nuevas conexiones.
- Después de restaurar los datos, se pierden los datos generados después de la copia de respaldo de datos y antes de la restauración de datos.
- Después de restaurar los datos, es necesario iniciar las aplicaciones de capa superior de ClickHouse.

Prerrequisitos

- Si necesita restaurar datos desde un HDFS remoto, prepare un clúster en espera. Si los clústeres activos y en espera se despliegan en modo de seguridad y no son gestionados por el mismo FusionInsight Manager, se debe configurar la confianza mutua. Para obtener más información, consulte **Configuración de la confianza mutua Cross-Manager entre clústeres**. Si los clústeres activos y en espera se despliegan en modo normal, no se requiere confianza mutua.

- El tiempo es consistente entre los clústeres activos y en espera y los servicios NTP en los clústeres activos y en espera utilizan la misma fuente de tiempo.
- Se planifican la base de datos para almacenar tablas de datos restauradas, la ruta de guardado HDFS de tablas de datos y la lista de usuarios que pueden acceder a los datos restaurados.
- La ruta de guardado del archivo de copia de respaldo de ClickHouse es correcta.
- Las aplicaciones de capa superior de ClickHouse se detienen.
- En el clúster activo/en espera, al restaurar datos desde el HDFS remoto al host local, asegúrese de que el valor de **HADOOP_RPC_PROTECTION** de ClickHouse es el mismo que el de **hadoop.rpc.protection** de HDFS.

Procedimiento

Paso 1 En FusionInsight Manager, seleccione **O&M** > **Backup and Restoration** > **Backup Management**.

Paso 2 En la fila donde se encuentra la tarea de copia de respaldo especificada, elija **More** > **View History** en la columna **Operation** para mostrar los registros históricos de ejecución de la tarea de copia de respaldo.

En la ventana que se muestra, seleccione un registro de éxito y haga clic en **View** en la columna **Backup Path** para ver la información de su ruta de copia de respaldo y buscar la siguiente información:

- **Backup Object**: indica el origen de datos de la copia de respaldo.
- **Backup Path**: indica la ruta completa donde se almacenan los archivos de copia de respaldo.

  Seleccione la ruta correcta y copie manualmente la ruta completa de los archivos de copia de respaldo de **Backup Path**.

Paso 3 En FusionInsight Manager, seleccione **O&M** > **Backup and Restoration** > **Restoration Management**.

Paso 4 Haga clic en **Create**.

Paso 5 Establezca **Task Name** en el nombre de la tarea de restauración.

Paso 6 Seleccione el clúster que se va a operar desde **Recovery Object**.

Paso 7 En **Restoration Configuration**, seleccione **ClickHouse** en **Service data**.

Paso 8 Establezca **Path Type** de **ClickHouse** en un tipo de directorio de copia de respaldo.

Actualmente, el directorio de copia de respaldo solo admite el tipo **RemoteHDFS**.

- **RemoteHDFS**: indica que los archivos de copia de respaldo se almacenan en el directorio de HDFS del clúster en espera. Si selecciona esta opción de valor, también debe configurar los siguientes parámetros:
  - **Source NameService Name**: indica el nombre de NameService del clúster de datos de copia de respaldo, por ejemplo, **hacluster**. Puede obtenerlo en la página **NameService Management** de HDFS del clúster en espera.
  - **IP Mode**: indica el modo de la dirección IP de destino. El sistema selecciona automáticamente el modo de dirección IP en función del tipo de red del clúster, por ejemplo **IPv4** o **IPv6**.

- **Source NameNode IP Address**: indica la dirección IP del plano de servicio NameNode en el clúster en espera. Puede ser de un nodo activo o en espera.
- Ruta de origen: indica la ruta completa del directorio HDFS para almacenar datos de copia de respaldo del clúster en espera. Para más detalles, véase el **Backup Path** obtenido en el paso 2, por ejemplo, *Backup path/Backup task name_Data source_Task creation time*.
- **Maximum Number of Maps**: indica el número máximo de map en una tarea de MapReduce. El valor predeterminado es **20**.
- **Maximum Bandwidth of a Map (MB/s)**: indica el ancho de banda máximo de un map. El valor predeterminado es **100**.

Paso 9 Haga clic en **OK**.

Paso 10 En la lista de tareas de restauración, busque la fila donde se encuentra la tarea creada y haga clic en **Start** en la columna **Operation**.

- Después de que la restauración es exitosa, la barra de progreso está en verde.
- Una vez que la restauración se realiza correctamente, la tarea de restauración no se puede ejecutar de nuevo.
- Si la tarea de restauración falla durante la primera ejecución, rectifique el error y haga clic en **Retry** para volver a ejecutar la tarea.

----Fin

7.10.3.4 Restauración de datos de DBService

Escenario

Los datos de DBService deben recuperarse en los siguientes escenarios: los datos se modifican o eliminan inesperadamente y deben restaurarse. Después de que un administrador realice un ajuste de datos críticos en DBService, se produce una excepción o la operación no ha logrado el resultado esperado. Todos los módulos están defectuosos y no están disponibles. Los datos se migran a un nuevo clúster.

Los administradores del sistema pueden crear una tarea de recuperación en FusionInsight Manager para recuperar datos de DBService. Sólo se admiten las tareas de restauración manuales.

AVISO

- La restauración de datos solo se puede realizar cuando la versión del sistema es coherente con la de la copia de respaldo de datos.
- Para recuperar datos cuando el servicio se está ejecutando correctamente, se le aconseja hacer una copia de respaldo manual de los datos de gestión más recientes antes de recuperar los datos. De lo contrario, los datos DBService que se generan después de la copia de respaldo de datos y antes de la recuperación de datos se perderán.
- De forma predeterminada, los clústeres de usan DBService para almacenar metadatos de Hive, Hue, Loader, Spark, y Oozie. Al restaurar los datos de DBService se restaurarán los metadatos de todos estos componentes.

Impacto en el sistema

- Después de restaurar los datos, se pierden los datos generados después de la copia de respaldo de datos y antes de la restauración de datos.
- Después de restaurar los datos, las configuraciones de los componentes que dependen de DBService pueden caducar y estos componentes deben reiniciarse.

Prerrequisitos

- Para restaurar datos desde un HDFS remoto, debe preparar un clúster en espera. Si el clúster activo se despliega en modo de seguridad y los clústeres activo y en espera no son gestionados por el mismo FusionInsight Manager, se ha configurado la confianza mutua. Para obtener más información, consulte **Configuración de la confianza mutua Cross-Manager entre clústeres**. Si el clúster activo se despliega en modo normal, no se requiere confianza mutua.
- Se ha configurado la replicación entre clústeres para los clústeres activo y en espera. Para obtener más información, consulte **Habilitación de la replicación entre clústeres**.
- El tiempo es consistente entre los clústeres activos y en espera y los servicios NTP en los clústeres activos y en espera utilizan la misma fuente de tiempo.
- El estado de las instancias de DBService activas y en espera es normal. Si el estado es anormal, no se puede realizar la restauración de datos.

Procedimiento

Paso 1 En FusionInsight Manager, seleccione **O&M** > **Backup and Restoration** > **Backup Management**.

Paso 2 En la columna **Operation** de una tarea especificada en la lista de tareas, elija **More** > **View History** para ver los registros históricos de ejecución de tareas de copia de respaldo.

En la ventana que se muestra, busque un registro de éxito especificado y haga clic en **View** en la columna **Backup Path** para ver la información de la ruta de copia de respaldo de la tarea y buscar la siguiente información:

- **Backup Object** especifica el origen de datos de los datos de copia de respaldo.
- **Backup Path** especifica la ruta completa donde se guardan los archivos de copia de respaldo.

  Seleccione el elemento correcto y copie manualmente la ruta completa de los archivos de copia de respaldo de **Backup Path**.

Paso 3 En FusionInsight Manager, seleccione **O&M** > **Backup and Restoration** > **Restoration Management**.

Paso 4 Haga clic en **Create**.

Paso 5 Establezca **Task Name** en el nombre de la tarea de restauración.

Paso 6 Seleccione el clúster que se va a operar desde **Recovery Object**.

Paso 7 En el área **Restoration Configuration**, seleccione **DBService**.

NOTA

Si hay varios DBServices instalados, seleccione los DBServices que desea restaurar.

Paso 8 Establecer **Path Type** de **DBService** en un tipo de directorio de copia de respaldo.

La configuración varía según los tipos de directorios de copia de respaldo:

- **LocalDir**: indica que los archivos de copia de respaldo se almacenan en el disco local del nodo de gestión activa.

  Si selecciona **LocalDir**, también debe configurar **Source Path** para que seleccione el archivo de copia de respaldo que se va a restaurar, por ejemplo, *Version_Data source_Task execution time***.tar.gz**.

- **LocalHDFS**: indica que los archivos de copia de respaldo se almacenan en el directorio de HDFS del clúster actual.

  Si selecciona **LocalHDFS**, establezca los siguientes parámetros:

  – **Source Path**: indica la ruta completa del archivo de copia de respaldo en el HDFS, por ejemplo, *Backup path/Backup task name_Task creation time/Version_Data source_Task execution time***.tar.gz**.

  – **Source NameService Name**: indica el nombre NameService que corresponde al directorio de copia de respaldo cuando se ejecuta una tarea de restauración. El valor predeterminado es **hacluster**.

- **RemoteHDFS**: indica que los archivos de copia de respaldo se almacenan en el directorio de HDFS del clúster en espera.

  Si selecciona **RemoteHDFS**, establezca los siguientes parámetros:

  – **Source NameService Name**: indica el nombre de NameService del clúster de datos de copia de respaldo. Puede introducir el nombre integrado de NameService del clúster remoto, por ejemplo, **haclusterX**, **haclusterX1**, **haclusterX2**, **haclusterX3** o **haclusterX4**. También puede introducir un nombre NameService configurado del clúster remoto.

  – **IP Mode**: indica el modo de la dirección IP de destino. El sistema selecciona automáticamente el modo de dirección IP en función del tipo de red del clúster, por ejemplo **IPv4** o **IPv6**.

  – **Source NameNode IP Address**: indica la dirección IP del plano de servicio NameNode del clúster en espera, que admite el nodo activo o el nodo en espera.

  – **Source Path**: indica la ruta completa del directorio HDFS para almacenar los datos de copia de respaldo del clúster en espera, por ejemplo, *Backup path/Backup task name_Data source_Task creation time/Version_Data source_Task execution time***.tar.gz**.

  – **Queue Name**: indica el nombre de la cola de Yarn utilizada para la ejecución de tareas de copia de respaldo. El nombre debe ser el mismo que el nombre de la cola que se está ejecutando correctamente en el clúster.

- **NFS**: indica que los archivos de copia de respaldo se almacenan en el NAS mediante el protocolo NFS.

  Si selecciona **NFS**, establezca los siguientes parámetros:

  – **IP Mode**: indica el modo de la dirección IP de destino. El sistema selecciona automáticamente el modo de dirección IP en función del tipo de red del clúster, por ejemplo **IPv4** o **IPv6**.

  – **Server IP Address**: indica la dirección IP del servidor NAS.

  – **Source Path**: indica la ruta completa del archivo de copia de respaldo en el servidor NAS, por ejemplo, *Backup path/Backup task name_Data source_Task creation time/Version_Data source_Task execution time***.tar.gz**.

- **CIFS**: indica que los archivos de copia de respaldo se almacenan en el NAS mediante el protocolo CIFS.

  Si selecciona **CIFS**, establezca los siguientes parámetros:

  – **IP Mode**: indica el modo de la dirección IP de destino. El sistema selecciona automáticamente el modo de dirección IP en función del tipo de red del clúster, por ejemplo **IPv4** o **IPv6**.

  – **Server IP Address**: indica la dirección IP del servidor NAS.

  – **Port**: indica el número de puerto utilizado para conectarse al servidor NAS a través del protocolo CIFS. El valor predeterminado es **445**.

  – **Username**: indica el nombre de usuario establecido cuando se configura el protocolo CIFS.

  – **Password**: indica la contraseña establecida cuando se configura el protocolo CIFS.

  – **Source Path**: indica la ruta completa del archivo de copia de respaldo en el servidor NAS, por ejemplo, *Backup path/Backup task name_Data source_Task creation time/Version_Data source_Task execution time***.tar.gz**.

- **SFTP**: indica que los archivos de copia de respaldo se almacenan en el servidor mediante el protocolo SFTP.

  Si selecciona **SFTP**, establezca los siguientes parámetros:

  – **IP Mode**: indica el modo de la dirección IP de destino. El sistema selecciona automáticamente el modo de dirección IP en función del tipo de red del clúster, por ejemplo **IPv4** o **IPv6**.

  – **Server IP Address**: indica la dirección IP del servidor donde se almacenan los datos de copia de respaldo.

  – **Port**: indica el número de puerto utilizado para conectarse al servidor de copia de respaldo a través del protocolo SFTP. El valor predeterminado es **22**.

  – **Username**: indica el nombre de usuario para conectarse al servidor mediante el protocolo SFTP.

  – **Password**: indica la contraseña para conectarse al servidor mediante el protocolo SFTP.

  – **Source Path**: indica la ruta completa del archivo de copia de respaldo en el servidor de copia de respaldo, por ejemplo, *Backup path/Backup task name_Data source_Task creation time/Version_Data source_Task execution time***.tar.gz**.

- **OBS**: indica que los archivos de copia de respaldo se almacenan en OBS.

  Si selecciona **OBS**, establezca los siguientes parámetros:

  – **Source Path**: indica la ruta de acceso OBS completa de un archivo de copia de respaldo, por ejemplo, *Backup path/Backup task name_Data source_Task creation time/Version_Data source_Task execution time***.tar.gz**.

  > NOTA
  >
  > Solo MRS 3.1.0 o posterior admite el almacenamiento de archivos de copia de respaldo en OBS.

Paso 9 Haga clic en **OK**.

Paso 10 En la lista de tareas de restauración, busque una tarea creada y haga clic en **Start** en la columna **Operation** para ejecutar la tarea de restauración.

- Después de que la restauración es exitosa, la barra de progreso está en verde.

- Una vez que la restauración se realiza correctamente, la tarea de restauración no se puede ejecutar de nuevo.
- Si la tarea de restauración falla durante la primera ejecución, rectifique el error y haga clic en **Retry** para volver a ejecutar la tarea.

----Fin

7.10.3.5 Restauración de los metadatos de Flink

Escenario

Los metadatos de Flink deben restaurarse en los siguientes escenarios: Los datos se modifican o eliminan inesperadamente y deben restaurarse. Después de que un administrador realice operaciones importantes (como la actualización y el ajuste de datos) en Flink, se produce una excepción o no se logra el resultado esperado. El componente Flink está defectuoso y no está disponible. Los datos se migran a un nuevo clúster.

Los administradores del sistema pueden crear una tarea de restauración de Flink en FusionInsight Manager. Solo se admiten las tareas de restauración manuales.

AVISO

- La restauración de datos solo se puede realizar cuando la versión del sistema es coherente con la de la copia de respaldo de datos.
- Para restaurar los metadatos de Flink cuando el servicio se está ejecutando correctamente, se recomienda realizar una copia de respaldo manual de los metadatos de Flink más recientes antes de la restauración. De lo contrario, se perderán los metadatos de Flink que se generan después de la copia de respaldo de datos y antes de la restauración de datos.
- La restauración de metadatos de Flink y la restauración de datos de servicio no se pueden realizar al mismo tiempo. De lo contrario, la restauración de datos de servicio falla. Se recomienda restaurar los datos de servicio después de que se complete la restauración de metadatos.

Impacto en el sistema

- Antes de restaurar los metadatos, debe detener el servicio Flink. Durante este período, todas las aplicaciones de capa superior se ven afectadas y no pueden funcionar correctamente.
- Después de restaurar los metadatos, se pierden los datos generados después de la copia de respaldo de datos y antes de la restauración de datos.
- Después de restaurar los metadatos, es necesario iniciar las aplicaciones de la capa superior de Flink de Solr.

Prerrequisitos

- Ha comprobado la ruta para almacenar los archivos de copia de respaldo de metadatos de Flink.
- El servicio Flink se ha detenido antes de restaurar sus metadatos.
- Si necesita restaurar datos desde un HDFS remoto, prepare un clúster en espera. Si el clúster activo se despliega en modo de seguridad y los clústeres activo y en espera no son

gestionados por el mismo FusionInsight Manager, se ha configurado la confianza mutua. Para obtener más información, consulte **Configuración de la confianza mutua Cross-Manager entre clústeres**. Si el clúster activo se despliega en modo normal, no se requiere confianza mutua.

- Se ha configurado la replicación entre clústeres para los clústeres activos y en espera. Para obtener más información, consulte **Habilitación de la replicación entre clústeres**.

Procedimiento

Paso 1 En FusionInsight Manager, seleccione **O&M** > **Backup and Restoration** > **Backup Management**.

Paso 2 En la columna **Operation** de la tarea especificada en la lista de tareas, elija **More** > **View History**.

En la ventana mostrada, seleccione un registro de éxito y haga clic en **View** en la columna **Backup Path** para ver la información de su ruta de copia de respaldo y buscar la siguiente información:

- **Backup Object** especifica el origen de datos de los datos de copia de respaldo.
- **Backup Path** especifica la ruta completa donde se guardan los archivos de copia de respaldo.

  Seleccione la ruta correcta y copie manualmente la ruta completa de los archivos de copia de respaldo de **Backup Path**.

Paso 3 En FusionInsight Manager, seleccione **O&M** > **Backup and Restoration** > **Restoration Management**.

Paso 4 Haga clic en **Create**.

Paso 5 Establezca **Task Name** en el nombre de la tarea de restauración.

Paso 6 Seleccione el clúster que se va a operar desde **Recovery Object**.

Paso 7 En **Restoration Configuration**, seleccione **Flink** en **Metadata and other data**.

Paso 8 Establezca **Path Type** de **Flink** en un tipo de directorio de restauración.

La configuración varía según los tipos de directorios de copia de respaldo:

- **LocalDir**: indica que los datos se restauran desde el disco local del nodo de gestión activo.

  Si selecciona **LocalDir** también debe configurar **Source Path** para que seleccione el archivo de copia de respaldo que se va a restaurar, por ejemplo, *Backup task name_Data source_Task execution time***.tar.gz**.
- **LocalHDFS**: indica que los archivos de copia de respaldo se almacenan en el directorio de HDFS del clúster actual.

  Si selecciona **LocalHDFS**, establezca los siguientes parámetros:

  – **Source Path**: indica la ruta completa del archivo de copia de respaldo en el HDFS, por ejemplo, *Backup path/Backup task name_Task creation time/Version_Data source_Task execution time***.tar.gz**.

  – **Source NameService Name**: indica el nombre NameService que corresponde al directorio de copia de respaldo cuando se ejecuta una tarea de restauración.
- **RemoteHDFS**: indica que los datos se restauran desde el directorio HDFS del clúster en espera.

Si selecciona **RemoteHDFS**, establezca los siguientes parámetros:

- **Source NameService Name**: indica el nombre de NameService del clúster de datos de copia de respaldo. Puede introducir el nombre integrado de NameService del clúster remoto, por ejemplo, **haclusterX**, **haclusterX1**, **haclusterX2**, **haclusterX3** o **haclusterX4**. También puede introducir un nombre NameService configurado del clúster remoto.
- **IP Mode**: indica el modo de la dirección IP de destino. El sistema selecciona automáticamente el modo de dirección IP en función del tipo de red del clúster, por ejemplo **IPv4** o **IPv6**.
- **Source NameNode IP Address**: indica la dirección IP del plano de servicio NameNode del clúster en espera, que admite el nodo activo o el nodo en espera.
- **Source Path**: indica la ruta completa del directorio HDFS para almacenar los datos de copia de respaldo del clúster en espera, por ejemplo, *Backup path/Backup task name_Data source_Task creation time/Data source_Task execution time***.tar.gz**.
- **Queue Name**: indica el nombre de la cola de Yarn utilizada para la ejecución de tareas de copia de respaldo. El nombre debe ser el mismo que el nombre de la cola que se está ejecutando correctamente en el clúster de origen.

Paso 9 Haga clic en **OK**.

Paso 10 En la lista de tareas de restauración, busque la fila donde se encuentra la tarea creada y haga clic en **Start** en la columna **Operation**. En el cuadro de diálogo mostrado, haga clic en **OK** para iniciar la tarea de restauración.

- Después de que la restauración es exitosa, la barra de progreso está en verde.
- Una vez que la restauración se realiza correctamente, la tarea de restauración no se puede ejecutar de nuevo.
- Si la tarea de restauración falla durante la primera ejecución, rectifique el error y haga clic en **Retry** para volver a ejecutar la tarea.

Paso 11 Elija **Cluster** > **Services** e inicie el servicio Flink.

----Fin

7.10.3.6 Restauración de metadatos de HBase

Escenario

Para garantizar la seguridad de los metadatos de HBase (incluidos los archivos tableinfo y HFiles) o antes de una operación importante en las tablas del sistema HBase (como la actualización o la migración), debe realizar una copia de respaldo de los metadatos de HBase para evitar la indisponibilidad del servicio HBase causada por el directorio de tablas del sistema HBase o los daños en los archivos. Los datos de copia de respaldo se pueden utilizar para recuperar el sistema si se produce una excepción o la operación no ha logrado el resultado esperado, minimizando los impactos adversos en los servicios.

Los administradores del sistema pueden crear una tarea de recuperación en FusionInsight Manager para recuperar metadatos de HBase. Sólo se admiten las tareas de restauración manuales.

AVISO

- La restauración de datos solo se puede realizar cuando la versión del sistema es coherente con la de la copia de respaldo de datos.
- Para recuperar datos cuando el servicio se está ejecutando correctamente, se le aconseja hacer una copia de respaldo manual de los datos de gestión más recientes antes de recuperar los datos. De lo contrario, los datos de HBase que se generan después de la copia de respaldo de datos y antes de la recuperación de datos se perderán.
- Se recomienda que una tarea de restauración de datos restaure los metadatos de un solo componente para evitar que la restauración de datos de otros componentes se vea afectada al detener un servicio o una instancia. Si se restauran datos de varios componentes al mismo tiempo, la restauración de datos puede fallar.

  Los metadatos de HBase no se pueden restaurar al mismo tiempo que los metadatos de NameNode. Como resultado, la restauración de datos falla.

Impacto en el sistema

- Antes de restaurar los metadatos, debe detener el servicio HBase, durante el cual las aplicaciones de capa superior de HBase no están disponibles.
- Después de restaurar los metadatos, se pierden los datos generados después de la copia de respaldo de datos y antes de la restauración de datos.
- Después de restaurar los metadatos, es necesario iniciar las aplicaciones de capa superior de HBase.

Prerrequisitos

- Si necesita restaurar datos desde un HDFS remoto, prepare un clúster en espera. Si el clúster activo se despliega en modo de seguridad y los clústeres activo y en espera no son gestionados por el mismo FusionInsight Manager, se ha configurado la confianza mutua. Para obtener más información, consulte **Configuración de la confianza mutua Cross-Manager entre clústeres**. Si el clúster activo se despliega en modo normal, no se requiere confianza mutua.
- Se ha configurado la replicación entre clústeres para los clústeres activo y en espera. Para obtener más información, consulte **Habilitación de la replicación entre clústeres**.
- Ha comprobado la ruta para almacenar los archivos de copia de respaldo de metadatos de HBase.
- El servicio HBase se ha detenido antes de restaurar sus metadatos.

Procedimiento

Paso 1 En FusionInsight Manager, seleccione **O&M** > **Backup and Restoration** > **Backup Management**.

Paso 2 En la columna **Operation** de una tarea especificada en la lista de tareas, elija **More** > **View History** para ver los registros históricos de ejecución de tareas de copia de respaldo.

En la ventana que se muestra, busque un registro de éxito especificado y haga clic en **View** en la columna **Backup Path** para ver la información de la ruta de copia de respaldo de la tarea y buscar la siguiente información:

- **Backup Object** especifica el origen de datos de los datos de copia de respaldo.
- **Backup Path** especifica la ruta completa donde se guardan los archivos de copia de respaldo.

  Seleccione el elemento correcto y copie manualmente la ruta completa de los archivos de copia de respaldo de **Backup Path**.

Paso 3 En FusionInsight Manager, seleccione **O&M** > **Backup and Restoration** > **Restoration Management**.

Paso 4 Haga clic en **Create**.

Paso 5 Establezca **Task Name** en el nombre de la tarea de restauración.

Paso 6 Seleccione el clúster que se va a operar desde **Recovery Object**.

Paso 7 En **Restoration Configuration**, seleccione **HBase** en **Metadata and other data**.

NOTA

Si se instalan varios servicios HBase, seleccione los servicios HBase que se van a restaurar.

Paso 8 Establezca **Path Type** de **HBase** en un tipo de directorio de copia de respaldo.

La configuración varía según los tipos de directorios de copia de respaldo:

- **LocalDir**: indica que los archivos de copia de respaldo se almacenan en el disco local del nodo de gestión activa.

  Si selecciona **LocalDir**, también debe configurar **Source Path** para que seleccione el archivo de copia de respaldo que se va a restaurar, por ejemplo, *Version_Data source_Task execution time*.**tar.gz**.
- **RemoteHDFS**: indica que los archivos de copia de respaldo se almacenan en el directorio de HDFS del clúster en espera.

  Si selecciona **RemoteHDFS**, establezca los siguientes parámetros:

  - **Source NameService Name**: indica el nombre de NameService del clúster de datos de copia de respaldo. Puede introducir el nombre integrado de NameService del clúster remoto, por ejemplo, **haclusterX**, **haclusterX1**, **haclusterX2**, **haclusterX3** o **haclusterX4**. También puede introducir un nombre NameService configurado del clúster remoto.
  - **IP Mode**: indica el modo de la dirección IP de destino. El sistema selecciona automáticamente el modo de dirección IP en función del tipo de red del clúster, por ejemplo **IPv4** o **IPv6**.
  - **Source NameNode IP Address**: indica la dirección IP del plano de servicio NameNode del clúster en espera, que admite el nodo activo o el nodo en espera.
  - **Source Path**: indica la ruta completa del directorio HDFS para almacenar los datos de copia de respaldo del clúster en espera, por ejemplo, *Backup path/Backup task name_Data source_Task creation time/Version_Data source_Task execution time*.**tar.gz**.
  - **Queue Name**: indica el nombre de la cola de Yarn utilizada para la ejecución de tareas de copia de respaldo. El nombre debe ser el mismo que el nombre de la cola que se está ejecutando correctamente en el clúster.
- **NFS**: indica que los archivos de copia de respaldo se almacenan en el NAS mediante el protocolo NFS.

  Si selecciona **NFS**, establezca los siguientes parámetros:

  - **IP Mode**: indica el modo de la dirección IP de destino. El sistema selecciona automáticamente el modo de dirección IP en función del tipo de red del clúster, por ejemplo **IPv4** o **IPv6**.
  - **Server IP Address**: indica la dirección IP del servidor NAS.
  - **Source Path**: indica la ruta completa del archivo de copia de respaldo en el servidor NAS, por ejemplo, *Backup path/Backup task name_Data source_Task creation time/Version_Data source_Task execution time***.tar.gz**.

- **CIFS**: indica que los archivos de copia de respaldo se almacenan en el NAS mediante el protocolo CIFS.

  Si selecciona **CIFS**, establezca los siguientes parámetros:

  - **IP Mode**: indica el modo de la dirección IP de destino. El sistema selecciona automáticamente el modo de dirección IP en función del tipo de red del clúster, por ejemplo **IPv4** o **IPv6**.
  - **Server IP Address**: indica la dirección IP del servidor NAS.
  - **Port**: indica el número de puerto utilizado para conectarse al servidor NAS a través del protocolo CIFS. El valor predeterminado es **445**.
  - **Username**: indica el nombre de usuario establecido cuando se configura el protocolo CIFS.
  - **Password**: indica la contraseña establecida cuando se configura el protocolo CIFS.
  - **Source Path**: indica la ruta completa del archivo de copia de respaldo en el servidor NAS, por ejemplo, *Backup path/Backup task name_Data source_Task creation time/Version_Data source_Task execution time***.tar.gz**.

- **SFTP**: indica que los archivos de copia de respaldo se almacenan en el servidor mediante el protocolo SFTP.

  Si selecciona **SFTP**, establezca los siguientes parámetros:

  - **IP Mode**: indica el modo de la dirección IP de destino. El sistema selecciona automáticamente el modo de dirección IP en función del tipo de red del clúster, por ejemplo **IPv4** o **IPv6**.
  - **Server IP Address**: indica la dirección IP del servidor donde se almacenan los datos de copia de respaldo.
  - **Port**: indica el número de puerto utilizado para conectarse al servidor de copia de respaldo a través del protocolo SFTP. El valor predeterminado es **22**.
  - **Username**: indica el nombre de usuario para conectarse al servidor mediante el protocolo SFTP.
  - **Password**: indica la contraseña para conectarse al servidor mediante el protocolo SFTP.
  - **Source Path**: indica la ruta completa del archivo de copia de respaldo en el servidor de copia de respaldo, por ejemplo, *Backup path/Backup task name_Data source_Task creation time/Version_Data source_Task execution time***.tar.gz**.

- **OBS**: indica que los archivos de copia de respaldo se almacenan en OBS.

  Si selecciona **OBS**, establezca los siguientes parámetros:

  - **Source Path**: indica la ruta de acceso OBS completa de un archivo de copia de respaldo, por ejemplo, *Backup path/Backup task name_Data source_Task creation time/Version_Data source_Task execution time***.tar.gz**.

NOTA

Solo MRS 3.1.0 o posterior admite el almacenamiento de archivos de copia de respaldo en OBS.

Paso 9 Haga clic en **OK**.

Paso 10 En la lista de tareas de restauración, busque una tarea creada y haga clic en **Start** en la columna **Operation** para ejecutar la tarea de restauración.

- Después de que la restauración es exitosa, la barra de progreso está en verde.
- Una vez que la restauración se realiza correctamente, la tarea de restauración no se puede ejecutar de nuevo.
- Si la tarea de restauración falla durante la primera ejecución, rectifique el error y haga clic en **Retry** para volver a ejecutar la tarea.

----Fin

7.10.3.7 Restauración de datos de servicio de HBase

Escenario

Los datos de HBase deben recuperarse en los siguientes escenarios: los datos se modifican o eliminan inesperadamente y deben restaurarse. Después de que un administrador realice un ajuste de datos críticos en HBase, se produce una excepción o la operación no ha logrado el resultado esperado. Todos los módulos están defectuosos y no están disponibles. Los datos se migran a un nuevo clúster.

Los administradores del sistema pueden crear una tarea de recuperación en FusionInsight Manager para recuperar datos de HBase. Sólo se admiten las tareas de restauración manuales.

AVISO

- La restauración de datos solo se puede realizar cuando la versión del sistema es coherente con la de la copia de respaldo de datos.
- Para recuperar datos cuando el servicio se está ejecutando correctamente, se le aconseja hacer una copia de respaldo manual de los datos de gestión más recientes antes de recuperar los datos. De lo contrario, los datos de HBase que se generan después de la copia de respaldo de datos y antes de la recuperación de datos se perderán.

Impacto en el sistema

- Durante el proceso de recuperación de datos, el sistema inhabilita la tabla HBase que se va a recuperar y no se puede acceder a la tabla en este momento. El proceso de recuperación de datos dura varios minutos, durante los cuales las aplicaciones de capa superior de HBase no están disponibles.
- Durante la restauración de datos, la autenticación del usuario se detiene y los usuarios no pueden crear nuevas conexiones.
- Después de restaurar los datos, se pierden los datos generados después de la copia de respaldo de datos y antes de la restauración de datos.
- Después de recuperar los datos, es necesario iniciar las aplicaciones de capa superior de HBase.

Prerrequisitos

- Si necesita restaurar datos desde un HDFS remoto, prepare un clúster en espera. Si el clúster activo se despliega en modo de seguridad y los clústeres activo y en espera no son gestionados por el mismo FusionInsight Manager, se ha configurado la confianza mutua. Para obtener más información, consulte **Configuración de la confianza mutua Cross-Manager entre clústeres**. Si el clúster activo se despliega en modo normal, no se requiere confianza mutua.
- Se ha configurado la replicación entre clústeres para los clústeres activo y en espera. Para obtener más información, consulte **Habilitación de la replicación entre clústeres**.
- El tiempo es consistente entre los clústeres activos y en espera y los servicios NTP en los clústeres activos y en espera utilizan la misma fuente de tiempo.
- Se ha comprobado el directorio para guardar el archivo de copia de respaldo.
- Las aplicaciones de capa superior de HBase se han detenido.

Procedimiento

Paso 1 En FusionInsight Manager, seleccione **O&M** > **Backup and Restoration** > **Backup Management**.

Paso 2 En la columna **Operation** de una tarea especificada en la lista de tareas, elija **More** > **View History** para ver los registros históricos de ejecución de tareas de copia de respaldo.

En la ventana que se muestra, busque un registro de éxito especificado y haga clic en **View** en la columna **Backup Path** para ver la información de la ruta de copia de respaldo de la tarea y buscar la siguiente información:

- **Backup Object** especifica el origen de datos de los datos de copia de respaldo.
- **Backup Path** especifica la ruta completa donde se guardan los archivos de copia de respaldo.

  Seleccione el elemento correcto y copie manualmente la ruta completa de los archivos de copia de respaldo de **Backup Path**.

Paso 3 En FusionInsight Manager, seleccione **O&M** > **Backup and Restoration** > **Restoration Management**.

Paso 4 Haga clic en **Create**.

Paso 5 Establezca **Task Name** en el nombre de la tarea de restauración.

Paso 6 Seleccione el clúster que se va a operar desde **Recovery Object**.

Paso 7 En **Restoration Configuration**, seleccione **HBase** en **Service Data**.

Paso 8 Establezca **Path Type** de **HBase** en un tipo de directorio de copia de respaldo.

Se admiten los siguientes tipos de directorio de copia de respaldo:

- **RemoteHDFS**: indica que los archivos de copia de respaldo se almacenan en el directorio de HDFS del clúster en espera. Si selecciona **RemoteHDFS**, establezca los siguientes parámetros:
  - **Source NameService Name**: indica el nombre de NameService del clúster de datos de copia de respaldo. Puede introducir el nombre integrado de NameService del clúster remoto, por ejemplo, **haclusterX**, **haclusterX1**, **haclusterX2**, **haclusterX3** o **haclusterX4**. También puede introducir un nombre NameService configurado del clúster remoto.

  - **IP Mode**: indica el modo de la dirección IP de destino. El sistema selecciona automáticamente el modo de dirección IP en función del tipo de red del clúster, por ejemplo **IPv4** o **IPv6**.
  - **Source NameNode IP Address**: indica la dirección IP del plano de servicio NameNode del clúster en espera, que admite el nodo activo o el nodo en espera.
  - **Source Path** indica la ruta completa del archivo de copia de respaldo en HDFS, por ejemplo, *Backup path/Backup task name_Data source_Task creation time*.
  - **Queue Name**: indica el nombre de la cola de Yarn utilizada para la ejecución de tareas de copia de respaldo.
  - **Recovery Point List**: Haga clic en **Refresh** y seleccione un directorio HDFS del que se ha realizado una copia de respaldo en el clúster en espera.
  - **Maximum Number of Maps**: indica el número máximo de map en una tarea de MapReduce. El valor predeterminado es **20**.
  - **Maximum Bandwidth of a Map (MB/s)**: indica el ancho de banda máximo de un map. El valor predeterminado es **100**.
- **NFS**: indica que los archivos de copia de respaldo se almacenan en el NAS mediante el protocolo NFS. Si selecciona **NFS**, establezca los siguientes parámetros:
  - **IP Mode**: indica el modo de la dirección IP de destino. El sistema selecciona automáticamente el modo de dirección IP en función del tipo de red del clúster, por ejemplo **IPv4** o **IPv6**.
  - **Server IP Address**: indica la dirección IP del servidor NAS.
  - **Source Path**: indica la ruta completa del archivo de copia de respaldo en el servidor de NAS, por ejemplo, *Backup path/Backup task name_Data source_Task creation time*.
  - **Queue Name**: indica el nombre de la cola de Yarn utilizada para la ejecución de tareas de copia de respaldo.
  - **Recovery Point List**: Haga clic en **Refresh** y seleccione un directorio HDFS del que se ha realizado una copia de respaldo en el clúster en espera.
  - **Maximum Number of Maps**: indica el número máximo de map en una tarea de MapReduce. El valor predeterminado es **20**.
  - **Maximum Bandwidth of a Map (MB/s)**: indica el ancho de banda máximo de un map. El valor predeterminado es **100**.
- **CIFS**: indica que los archivos de copia de respaldo se almacenan en el NAS mediante el protocolo CIFS. Si selecciona **CIFS**, establezca los siguientes parámetros:
  - **IP Mode**: indica el modo de la dirección IP de destino. El sistema selecciona automáticamente el modo de dirección IP en función del tipo de red del clúster, por ejemplo **IPv4** o **IPv6**.
  - **Server IP Address**: indica la dirección IP del servidor NAS.
  - **Port**: indica el número de puerto utilizado para conectarse al servidor NAS a través del protocolo CIFS. El valor predeterminado es **445**.
  - **Username**: indica el nombre de usuario establecido cuando se configura el protocolo CIFS.
  - **Password**: indica la contraseña establecida cuando se configura el protocolo CIFS.
  - **Source Path**: indica la ruta completa del archivo de copia de respaldo en el servidor de NAS, por ejemplo, *Backup path/Backup task name_Data source_Task creation time*.

- **Queue Name**: indica el nombre de la cola de Yarn utilizada para la ejecución de tareas de copia de respaldo.
- **Recovery Point List**: Haga clic en **Refresh** y seleccione un directorio HDFS del que se ha realizado una copia de respaldo en el clúster en espera.
- **Maximum Number of Maps**: indica el número máximo de map en una tarea de MapReduce. El valor predeterminado es **20**.
- **Maximum Bandwidth of a Map (MB/s)**: indica el ancho de banda máximo de un map. El valor predeterminado es **100**.

- **SFTP**: indica que los archivos de copia de respaldo se almacenan en el servidor mediante el protocolo SFTP.

  Si selecciona **SFTP**, establezca los siguientes parámetros:

  - **IP Mode**: indica el modo de la dirección IP de destino. El sistema selecciona automáticamente el modo de dirección IP en función del tipo de red del clúster, por ejemplo **IPv4** o **IPv6**.
  - **Server IP Address**: indica la dirección IP del servidor donde se almacenan los datos de copia de respaldo.
  - **Port**: indica el número de puerto utilizado para conectarse al servidor de copia de respaldo a través del protocolo SFTP. El valor predeterminado es **22**.
  - **Username**: indica el nombre de usuario para conectarse al servidor mediante el protocolo SFTP.
  - **Password**: indica la contraseña para conectarse al servidor mediante el protocolo SFTP.
  - **Source Path**: indica la ruta completa del archivo de copia de respaldo en el servidor de copia de respaldo, por ejemplo, *Backup path/Backup task name_Data source_Task creation time/Version_Data source_Task execution time***.tar.gz**.
  - **Queue Name**: indica el nombre de la cola de Yarn utilizada para la ejecución de tareas de copia de respaldo.
  - **Recovery Point List**: Haga clic en **Refresh** y seleccione un directorio HDFS del que se ha realizado una copia de respaldo en el clúster en espera.
  - **Maximum Number of Maps**: indica el número máximo de map en una tarea de MapReduce. El valor predeterminado es **20**.
  - **Maximum Bandwidth of a Map (MB/s)**: indica el ancho de banda máximo de un map. El valor predeterminado es **100**.

Paso 9 Establezca la columna **Backup Data** de **Data Configuration** en una o varias fuentes de datos de copia de respaldo que se recuperarán. En la columna **Target Namespace**, especifique el espacio de nombres de destino después de la recuperación de datos de copia de respaldo.

Se recomienda establecer **Target Namespace** en una ubicación que sea diferente del espacio de nombres de copia de respaldo.

Paso 10 Establezca **Force recovery** en **true** que indica que debe recuperar a la fuerza todos los datos de copia de respaldo cuando ya existe una tabla de datos con el mismo nombre. Si la tabla de datos contiene nuevos datos agregados después de la copia de respaldo, los nuevos datos se perderán después de la recuperación de datos. Si establece el parámetro en **false**, la tarea de restauración no se ejecuta si existe una tabla de datos con el mismo nombre.

Paso 11 Haga clic en **Verify** para comprobar si la tarea de restauración está configurada correctamente.

- Si el nombre de la cola es incorrecto, la verificación falla.
- Si el espacio de nombres especificado no existe, la verificación falla.
- Si no se cumplen las condiciones de sustitución forzada, la verificación falla.

Paso 12 Haga clic en **OK** para guardar la configuración.

Paso 13 En la lista de tareas de restauración, busque una tarea creada y haga clic en **Start** en la columna **Operation** para ejecutar la tarea de restauración.

- Después de que la restauración es exitosa, la barra de progreso está en verde.
- Una vez que la restauración se realiza correctamente, la tarea de restauración no se puede ejecutar de nuevo.
- Si la tarea de restauración falla durante la primera ejecución, rectifique el error y haga clic en **Retry** para volver a ejecutar la tarea.

Paso 14 Compruebe si los datos de HBase se restauran en un entorno donde HBase se ha instalado o reinstalado recientemente.

- En caso afirmativo, el administrador debe establecer un nuevo permiso para los roles en FusionInsight Manager según el plan de servicio original.
- En caso negativo, no se requiere ninguna operación adicional.

----Fin

7.10.3.8 Restauración de datos de NameNode

Escenario

Los datos de NameNode deben recuperarse en los siguientes escenarios: los datos se modifican o eliminan inesperadamente y deben restaurarse. Una vez que un administrador realiza un ajuste de datos críticos de NameNode, se produce una excepción o la operación no ha logrado el resultado esperado. Todos los módulos están defectuosos y no están disponibles. Los datos se migran a un nuevo clúster.

Los administradores del sistema pueden crear una tarea de recuperación en FusionInsight Manager para recuperar datos de NameNode. Sólo se admiten las tareas de restauración manuales.

AVISO

- La restauración de datos solo se puede realizar cuando la versión del sistema es coherente con la de la copia de respaldo de datos.
- Para recuperar datos cuando el servicio se está ejecutando correctamente, se le aconseja hacer una copia de respaldo manual de los datos de gestión más recientes antes de recuperar los datos. De lo contrario, los datos NameNode que se generan después de la copia de respaldo de datos y antes de la recuperación de datos se perderán.
- Se recomienda que una tarea de restauración de datos restaure los metadatos de un solo componente para evitar que la restauración de datos de otros componentes se vea afectada al detener un servicio o una instancia. Si se restauran datos de varios componentes al mismo tiempo, la restauración de datos puede fallar.

  Los metadatos de HBase no se pueden restaurar al mismo tiempo que los metadatos de NameNode. Como resultado, la restauración de datos falla.

Impacto en el sistema

- Después de restaurar los datos, se pierden los datos generados después de la copia de respaldo de datos y antes de la restauración de datos.
- Después de recuperar los datos, el NameNode debe reiniciarse y no está disponible durante el reinicio.
- Después de restaurar los datos, es posible que los metadatos y los datos de servicio no coincidan, el HDFS entra en el modo de seguridad y el servicio HDFS no se inicia. .

Prerrequisitos

- Si necesita restaurar datos desde un HDFS remoto, prepare un clúster en espera. Si el clúster activo se despliega en modo de seguridad y los clústeres activo y en espera no son gestionados por el mismo FusionInsight Manager, se ha configurado la confianza mutua. Para obtener más información, consulte **Configuración de la confianza mutua Cross-Manager entre clústeres**. Si el clúster activo se despliega en modo normal, no se requiere confianza mutua.
- Se ha configurado la replicación entre clústeres para los clústeres activo y en espera. Para obtener más información, consulte **Habilitación de la replicación entre clústeres**.
- El tiempo es consistente entre los clústeres activos y en espera y los servicios NTP en los clústeres activos y en espera utilizan la misma fuente de tiempo.
- En FusionInsight Manager, se detienen todas las instancias de rol NameNode cuyos datos se van a recuperar. Otras instancias de rol HDFS deben seguir ejecutándose. Después de recuperar los datos, las instancias de rol NameNode deben reiniciarse. No se puede acceder a las instancias de rol NameNode durante el reinicio.
- Los archivos de copia de respaldo NameNode se almacenan ***Data path*/LocalBackup/** en el nodo de gestión activa.

Procedimiento

Paso 1 En FusionInsight Manager, haga clic en **Cluster**, haga clic en el nombre del clúster deseado y elija **Services** > **HDFS**. En la página mostrada, haga clic en **Instance** y haga clic en **NameNode** para comprobar si se detienen las instancias NameNode de los datos que se van a restaurar. Si las instancias NameNode no se detienen, deténganlas.

Paso 2 En FusionInsight Manager, seleccione **O&M** > **Backup and Restoration** > **Backup Management**.

Paso 3 En la columna **Operation** de una tarea especificada en la lista de tareas, elija **More** > **View History** para ver los registros históricos de ejecución de tareas de copia de respaldo.

En la ventana que se muestra, busque un registro de éxito especificado y haga clic en **View** en la columna **Backup Path** para ver la información de la ruta de copia de respaldo de la tarea y buscar la siguiente información:

- **Backup Object** especifica el origen de datos de los datos de copia de respaldo.
- **Backup Path** especifica la ruta completa donde se guardan los archivos de copia de respaldo.

  Seleccione el elemento correcto y copie manualmente la ruta completa de los archivos de copia de respaldo de **Backup Path**.

Paso 4 En FusionInsight Manager, seleccione **O&M** > **Backup and Restoration** > **Restoration Management**.

Paso 5 Haga clic en **Create**.

Paso 6 Establezca **Task Name** en el nombre de la tarea de restauración.

Paso 7 Seleccione el clúster que se va a operar desde **Recovery Object**.

Paso 8 En el área **Restoration Configuration**, seleccione **NameNode**.

Paso 9 Establezca **Path Type** de **NameNode** en un tipo de directorio de copia de respaldo.

La configuración varía según los tipos de directorios de copia de respaldo:

- **LocalDir**: indica que los archivos de copia de respaldo se almacenan en el disco local del nodo de gestión activa.

  Si selecciona **LocalDir**, establezca los siguientes parámetros:

  - **Source Path**: indica la ruta completa del archivo de copia de respaldo en el disco local, por ejemplo, *Backup path/Backup task name_Task creation time/Version_Data source_Task execution time***.tar.gz**.
  - **Target NameService Name**: indica el nombre de NameService del directorio de copia de respaldo. El valor predeterminado es **hacluster**.

- **RemoteHDFS**: indica que los archivos de copia de respaldo se almacenan en el directorio de HDFS del clúster en espera.

  Si selecciona **RemoteHDFS**, establezca los siguientes parámetros:

  - **Source NameService Name**: indica el nombre de NameService del clúster de datos de copia de respaldo. Puede introducir el nombre integrado de NameService del clúster remoto, por ejemplo, **haclusterX**, **haclusterX1**, **haclusterX2**, **haclusterX3** o **haclusterX4**. También puede introducir un nombre NameService configurado del clúster remoto.
  - **IP Mode**: indica el modo de la dirección IP de destino. El sistema selecciona automáticamente el modo de dirección IP en función del tipo de red del clúster, por ejemplo **IPv4** o **IPv6**.
  - **Source NameNode IP Address**: indica la dirección IP del plano de servicio NameNode del clúster en espera, que admite el nodo activo o el nodo en espera.
  - **Source Path**: indica la ruta completa del directorio HDFS para almacenar los datos de copia de respaldo del clúster en espera, por ejemplo, *Backup path/Backup task name_Data source_Task creation time/Version_Data source_Task execution time***.tar.gz**.
  - **Queue Name**: indica el nombre de la cola de Yarn utilizada para la ejecución de tareas de copia de respaldo. El nombre debe ser el mismo que el nombre de la cola que se está ejecutando correctamente en el clúster.
  - **Target NameService Name**: indica el nombre de NameService del directorio de copia de respaldo. El valor predeterminado es **hacluster**.

- **NFS**: indica que los archivos de copia de respaldo se almacenan en el NAS mediante el protocolo NFS. Si selecciona **NFS**, establezca los siguientes parámetros:

  - **IP Mode**: indica el modo de la dirección IP de destino. El sistema selecciona automáticamente el modo de dirección IP en función del tipo de red del clúster, por ejemplo **IPv4** o **IPv6**.
  - **Server IP Address**: indica la dirección IP del servidor NAS.
  - **Source Path**: indica la ruta completa del archivo de copia de respaldo en el servidor NAS, por ejemplo, *Backup path/Backup task name_Data source_Task creation time/Version_Data source_Task execution time***.tar.gz**.

  - **Target NameService Name**: indica el nombre de NameService del directorio de copia de respaldo. El valor predeterminado es **hacluster**.

- **CIFS**: indica que los archivos de copia de respaldo se almacenan en el NAS mediante el protocolo CIFS. Si selecciona **CIFS**, establezca los siguientes parámetros:
  - **IP Mode**: indica el modo de la dirección IP de destino. El sistema selecciona automáticamente el modo de dirección IP en función del tipo de red del clúster, por ejemplo **IPv4** o **IPv6**.
  - **Server IP Address**: indica la dirección IP del servidor NAS.
  - **Port**: indica el número de puerto utilizado para conectarse al servidor NAS a través del protocolo CIFS. El valor predeterminado es **445**.
  - **Username**: indica el nombre de usuario establecido cuando se configura el protocolo CIFS.
  - **Password**: indica la contraseña establecida cuando se configura el protocolo CIFS.
  - **Source Path**: indica la ruta completa del archivo de copia de respaldo en el servidor NAS, por ejemplo, *Backup path/Backup task name_Data source_Task creation time/Version_Data source_Task execution time***.tar.gz**.
  - **Target NameService Name**: indica el nombre de NameService del directorio de copia de respaldo. El valor predeterminado es **hacluster**.
- **SFTP**: indica que los archivos de copia de respaldo se almacenan en el servidor mediante el protocolo SFTP.

  Si selecciona **SFTP**, establezca los siguientes parámetros:
  - **IP Mode**: indica el modo de la dirección IP de destino. El sistema selecciona automáticamente el modo de dirección IP en función del tipo de red del clúster, por ejemplo **IPv4** o **IPv6**.
  - **Server IP Address**: indica la dirección IP del servidor donde se almacenan los datos de copia de respaldo.
  - **Port**: indica el número de puerto utilizado para conectarse al servidor de copia de respaldo a través del protocolo SFTP. El valor predeterminado es **22**.
  - **Username**: indica el nombre de usuario para conectarse al servidor mediante el protocolo SFTP.
  - **Password**: indica la contraseña para conectarse al servidor mediante el protocolo SFTP.
  - **Source Path**: indica la ruta completa del archivo de copia de respaldo en el servidor de copia de respaldo, por ejemplo, *Backup path/Backup task name_Data source_Task creation time/Version_Data source_Task execution time***.tar.gz**.
  - **Target NameService Name**: indica el nombre de NameService del directorio de copia de respaldo. El valor predeterminado es **hacluster**.
- **OBS**: indica que los archivos de copia de respaldo se almacenan en OBS.

  Si selecciona **OBS**, establezca los siguientes parámetros:
  - **Source Path**: indica la ruta de acceso OBS completa de un archivo de copia de respaldo, por ejemplo, *Backup path/Backup task name_Data source_Task creation time/Version_Data source_Task execution time***.tar.gz**.
  - **NameService Name**: indica el nombre NameService del directorio de copia de respaldo. El valor predeterminado es **hacluster**.

NOTA

Solo MRS 3.1.0 o posterior admite el almacenamiento de archivos de copia de respaldo en OBS.

Paso 10 Haga clic en **OK**.

Paso 11 En la lista de tareas de restauración, busque una tarea creada y haga clic en **Start** en la columna **Operation** para ejecutar la tarea de restauración.

- Después de que la restauración es exitosa, la barra de progreso está en verde.
- Una vez que la restauración se realiza correctamente, la tarea de restauración no se puede ejecutar de nuevo.
- Si la tarea de restauración falla durante la primera ejecución, rectifique el error y haga clic en **Retry** para volver a ejecutar la tarea.

Paso 12 En FusionInsight Manager, haga clic en **Cluster**, haga clic en el nombre del clúster deseado y elija **Services** > **HDFS**. En la página mostrada, haga clic en **Configurations** y haga clic en **All Configurations**.

En la página mostrada, ingrese la contraseña del administrador que ha iniciado sesión para la autenticación y haga clic en **OK**. Después de que el sistema muestre "Operation succeeded", haga clic en **Finish**. El servicio se inicia correctamente.

----Fin

7.10.3.9 Restauración de datos de servicio de HDFS

Escenario

Los datos de HDFS deben recuperarse en los siguientes escenarios: los datos se modifican o eliminan inesperadamente y deben restaurarse. Después de que un administrador realice un ajuste de datos críticos en el HDFS, se produce una excepción o la operación no ha logrado el resultado esperado. Todos los módulos están defectuosos y no están disponibles. Los datos se migran a un nuevo clúster.

Los administradores del sistema pueden crear una tarea de recuperación en FusionInsight Manager para recuperar datos de HDFS. Sólo se admiten las tareas de restauración manuales.

AVISO

- La restauración de datos solo se puede realizar cuando la versión del sistema es coherente con la de la copia de respaldo de datos.
- Para recuperar datos cuando el servicio se está ejecutando correctamente, se le aconseja hacer una copia de respaldo manual de los datos de gestión más recientes antes de recuperar los datos. De lo contrario, los datos de HDFS que se generan después de la copia de respaldo de datos y antes de la recuperación de datos se perderán.
- La operación de restauración HDFS no se puede realizar para los directorios que se utilizan al ejecutar tareas de Yarn, por ejemplo, **/tmp/logs**, **/tmp/archived** y **/tmp/hadoop-yarn/staging**. De lo contrario, la restauración de datos mediante tareas de Distcp falla debido a la pérdida de archivos.

Impacto en el sistema

- Durante la restauración de datos, la autenticación del usuario se detiene y los usuarios no pueden crear nuevas conexiones.
- Después de restaurar los datos, se pierden los datos generados después de la copia de respaldo de datos y antes de la restauración de datos.
- Después de recuperar los datos, es necesario iniciar las aplicaciones de capa superior HDFS.

Prerrequisitos

- Si necesita restaurar datos desde un HDFS remoto, prepare un clúster en espera. Si el clúster activo se despliega en modo de seguridad y los clústeres activo y en espera no son gestionados por el mismo FusionInsight Manager, se ha configurado la confianza mutua. Para obtener más información, consulte **Configuración de la confianza mutua Cross-Manager entre clústeres**. Si el clúster activo se despliega en modo normal, no se requiere confianza mutua.
- Se ha configurado la replicación entre clústeres para los clústeres activo y en espera. Para obtener más información, consulte **Habilitación de la replicación entre clústeres**.
- El tiempo es consistente entre los clústeres activos y en espera y los servicios NTP en los clústeres activos y en espera utilizan la misma fuente de tiempo.
- La ruta de guardado del archivo de copia de respaldo de HDFS es correcta.
- Las aplicaciones de capa superior de HDFS se detienen.

Procedimiento

Paso 1 En FusionInsight Manager, seleccione **O&M** > **Backup and Restoration** > **Backup Management**.

Paso 2 En la columna **Operation** de una tarea especificada en la lista de tareas, elija **More** > **View History** para ver los registros históricos de ejecución de tareas de copia de respaldo.

En la ventana que se muestra, busque un registro de éxito especificado y haga clic en **View** en la columna **Backup Path** para ver la información de la ruta de copia de respaldo de la tarea y buscar la siguiente información:

- **Backup Object** especifica el origen de datos de los datos de copia de respaldo.
- **Backup Path** especifica la ruta completa donde se guardan los archivos de copia de respaldo.

  Seleccione el elemento correcto y copie manualmente la ruta completa de los archivos de copia de respaldo de **Backup Path**.

Paso 3 En FusionInsight Manager, seleccione **O&M** > **Backup and Restoration** > **Restoration Management**.

Paso 4 Haga clic en **Create**.

Paso 5 Establezca **Task Name** en el nombre de la tarea de restauración.

Paso 6 Seleccione el clúster que se va a operar desde **Recovery Object**.

Paso 7 En **Restoration Configuration**, seleccione **HDFS** en **Service Data**.

Paso 8 Establezca **Path Type** de **HDFS** en un tipo de directorio de copia de respaldo.

Se admiten los siguientes tipos de directorio de copia de respaldo:

- **RemoteHDFS**: indica que los archivos de copia de respaldo se almacenan en el directorio de HDFS del clúster en espera.

  Si selecciona **RemoteHDFS**, establezca los siguientes parámetros:

  - **Source NameService Name**: indica el nombre de NameService del clúster de datos de copia de respaldo. Puede introducir el nombre integrado de NameService del clúster remoto, por ejemplo, **haclusterX**, **haclusterX1**, **haclusterX2**, **haclusterX3** o **haclusterX4**. También puede introducir un nombre NameService configurado del clúster remoto.
  - **IP Mode**: indica el modo de la dirección IP de destino. El sistema selecciona automáticamente el modo de dirección IP en función del tipo de red del clúster, por ejemplo **IPv4** o **IPv6**.
  - **Source NameNode IP Address**: indica la dirección IP del plano de servicio NameNode del clúster en espera, que admite el nodo activo o el nodo en espera.
  - **Source Path**: indica la ruta completa del directorio HDFS para almacenar los datos de copia de respaldo del clúster en espera, por ejemplo, *Backup path/Backup task name_Data source_Task creation time*.
  - **Queue Name**: indica el nombre de la cola de Yarn utilizada para la ejecución de tareas de copia de respaldo.
  - **Recovery Point List**: Haga clic en **Refresh** y seleccione un directorio HDFS del que se ha realizado una copia de respaldo en el clúster en espera.
  - **Target NameService Name**: indica el nombre de NameService del directorio de copia de respaldo. El valor predeterminado es **hacluster**.
  - **Maximum Number of Maps**: indica el número máximo de map en una tarea de MapReduce. El valor predeterminado es **20**.
  - **Maximum Bandwidth of a Map (MB/s)**: indica el ancho de banda máximo de un map. El valor predeterminado es **100**.

- **NFS**: indica que los archivos de copia de respaldo se almacenan en el NAS mediante el protocolo NFS. Si selecciona **NFS**, establezca los siguientes parámetros:

  - **IP Mode**: indica el modo de la dirección IP de destino. El sistema selecciona automáticamente el modo de dirección IP en función del tipo de red del clúster, por ejemplo **IPv4** o **IPv6**.
  - **Server IP Address**: indica la dirección IP del servidor NAS.
  - **Source Path**: indica la ruta completa del archivo de copia de respaldo en el servidor de NAS, por ejemplo, *Backup path/Backup task name_Data source_Task creation time*.
  - **Queue Name**: indica el nombre de la cola de Yarn utilizada para la ejecución de tareas de copia de respaldo.
  - **Recovery Point List**: Haga clic en **Refresh** y seleccione un directorio HDFS del que se ha realizado una copia de respaldo en el clúster en espera.
  - **Target NameService Name**: indica el nombre de NameService del directorio de copia de respaldo. El valor predeterminado es **hacluster**.
  - **Maximum Number of Maps**: indica el número máximo de map en una tarea de MapReduce. El valor predeterminado es **20**.
  - **Maximum Bandwidth of a Map (MB/s)**: indica el ancho de banda máximo de un map. El valor predeterminado es **100**.

- **CIFS**: indica que los archivos de copia de respaldo se almacenan en el NAS mediante el protocolo CIFS. Si selecciona **CIFS**, establezca los siguientes parámetros:
  - **IP Mode**: indica el modo de la dirección IP de destino. El sistema selecciona automáticamente el modo de dirección IP en función del tipo de red del clúster, por ejemplo **IPv4** o **IPv6**.
  - **Server IP Address**: indica la dirección IP del servidor NAS.
  - **Port**: indica el número de puerto utilizado para conectarse al servidor NAS a través del protocolo CIFS. El valor predeterminado es **445**.
  - **Username**: indica el nombre de usuario establecido cuando se configura el protocolo CIFS.
  - **Password**: indica la contraseña establecida cuando se configura el protocolo CIFS.
  - **Source Path**: indica la ruta completa del archivo de copia de respaldo en el servidor de NAS, por ejemplo, *Backup path/Backup task name_Data source_Task creation time*.
  - **Queue Name**: indica el nombre de la cola de Yarn utilizada para la ejecución de tareas de copia de respaldo.
  - **Recovery Point List**: Haga clic en **Refresh** y seleccione un directorio HDFS del que se ha realizado una copia de respaldo en el clúster en espera.
  - **Target NameService Name**: indica el nombre de NameService del directorio de copia de respaldo. El valor predeterminado es **hacluster**.
  - **Maximum Number of Maps**: indica el número máximo de map en una tarea de MapReduce. El valor predeterminado es **20**.
  - **Maximum Bandwidth of a Map (MB/s)**: indica el ancho de banda máximo de un map. El valor predeterminado es **100**.
- **SFTP**: indica que los archivos de copia de respaldo se almacenan en el servidor mediante el protocolo SFTP.

  Si selecciona **SFTP**, establezca los siguientes parámetros:
  - **IP Mode**: indica el modo de la dirección IP de destino. El sistema selecciona automáticamente el modo de dirección IP en función del tipo de red del clúster, por ejemplo **IPv4** o **IPv6**.
  - **Server IP Address**: indica la dirección IP del servidor donde se almacenan los datos de copia de respaldo.
  - **Port**: indica el número de puerto utilizado para conectarse al servidor de copia de respaldo a través del protocolo SFTP. El valor predeterminado es **22**.
  - **Username**: indica el nombre de usuario para conectarse al servidor mediante el protocolo SFTP.
  - **Password**: indica la contraseña para conectarse al servidor mediante el protocolo SFTP.
  - **Source Path**: indica la ruta completa del archivo de copia de respaldo en el servidor de copia de respaldo, por ejemplo, *Backup path/Backup task name_Data source_Task creation time/Version_Data source_Task execution time***.tar.gz**.
  - **Queue Name**: indica el nombre de la cola de Yarn utilizada para la ejecución de tareas de copia de respaldo.
  - **Recovery Point List**: Haga clic en **Refresh** y seleccione un directorio HDFS del que se ha realizado una copia de respaldo en el clúster en espera.
  - **Target NameService Name**: indica el nombre de NameService del directorio de copia de respaldo. El valor predeterminado es **hacluster**.

- **Maximum Number of Maps**: indica el número máximo de map en una tarea de MapReduce. El valor predeterminado es **20**.
- **Maximum Bandwidth of a Map (MB/s)**: indica el ancho de banda máximo de un map. El valor predeterminado es **100**.

Paso 9 En la columna **Backup Data** de la página **Data Configuration**, seleccione una o más piezas de datos de copia de respaldo que deben restaurarse según los requisitos de servicio. En la columna **Target Path**, especifique la ubicación de destino después de la restauración de los datos de copia de respaldo.

Se recomienda establecer **Target Path** en una nueva ruta que sea diferente de la ruta de copia de respaldo.

Paso 10 Haga clic en **Verify** para comprobar si la tarea de restauración está configurada correctamente.

- Si el nombre de la cola es incorrecto, la verificación falla.
- Si el directorio especificado que se va a restaurar no existe, la verificación falla.

Paso 11 Haga clic en **OK**.

Paso 12 En la lista de tareas de restauración, busque una tarea creada y haga clic en **Start** en la columna **Operation** para ejecutar la tarea de restauración.

- Después de que la restauración es exitosa, la barra de progreso está en verde.
- Una vez que la restauración se realiza correctamente, la tarea de restauración no se puede ejecutar de nuevo.
- Si la tarea de restauración falla durante la primera ejecución, rectifique el error y haga clic en **Retry** para volver a ejecutar la tarea.

----Fin

7.10.3.10 Restauración de datos de servicio de Hive

Escenario

Los datos de Hive deben recuperarse en los siguientes escenarios: los datos se modifican o eliminan inesperadamente y deben restaurarse. Después de que un administrador realice un ajuste de datos críticos en Hive, se produce una excepción o la operación no ha logrado el resultado esperado. Todos los módulos están defectuosos y no están disponibles. Los datos se migran a un nuevo clúster.

Los administradores del sistema pueden crear una tarea de recuperación en FusionInsight Manager para recuperar datos de Hive. Sólo se admiten las tareas de restauración manuales.

La copia de respaldo y restauración de Hive no pueden identificar las relaciones de servicio y estructura de objetos como tablas, índices y vistas de Hive. Al ejecutar tareas de copia de respaldo y restauración, debe gestionar puntos de restauración unificados basados en escenarios de servicio para garantizar la ejecución adecuada del servicio.

AVISO

- La restauración de datos solo se puede realizar cuando la versión del sistema es coherente con la de la copia de respaldo de datos.
- Para recuperar datos cuando el servicio se está ejecutando correctamente, se le aconseja hacer una copia de respaldo manual de los datos de gestión más recientes antes de recuperar los datos. De lo contrario, los datos de Hive que se generan después de la copia de respaldo de datos y antes de la recuperación de datos se perderán.

Impacto en el sistema

- Durante la restauración de datos, la autenticación del usuario se detiene y los usuarios no pueden crear nuevas conexiones.
- Después de restaurar los datos, se pierden los datos generados después de la copia de respaldo de datos y antes de la restauración de datos.
- Después de recuperar los datos, es necesario iniciar las aplicaciones de capa superior de Hive.

Prerrequisitos

- Si necesita restaurar datos desde un HDFS remoto, prepare un clúster en espera. Si el clúster activo se despliega en modo de seguridad y los clústeres activo y en espera no son gestionados por el mismo FusionInsight Manager, se ha configurado la confianza mutua. Para obtener más información, consulte **Configuración de la confianza mutua Cross-Manager entre clústeres**. Si el clúster activo se despliega en modo normal, no se requiere confianza mutua.
- Se ha configurado la replicación entre clústeres para los clústeres activo y en espera. Para obtener más información, consulte **Habilitación de la replicación entre clústeres**.
- El tiempo es consistente entre los clústeres activos y en espera y los servicios NTP en los clústeres activos y en espera utilizan la misma fuente de tiempo.
- Se planifican la base de datos para almacenar tablas de datos restauradas, la ruta de guardado HDFS de tablas de datos y la lista de usuarios que pueden acceder a los datos restaurados.
- La ruta de guardado del archivo de copia de respaldo de Hive es correcta.
- Las aplicaciones de la capa superior de Hive se detienen.

Procedimiento

Paso 1 En FusionInsight Manager, seleccione **O&M** > **Backup and Restoration** > **Backup Management**.

Paso 2 En la columna **Operation** de una tarea especificada en la lista de tareas, elija **More** > **View History** para ver los registros históricos de ejecución de tareas de copia de respaldo.

En la ventana que se muestra, busque un registro de éxito especificado y haga clic en **View** en la columna **Backup Path** para ver la información de la ruta de copia de respaldo de la tarea y buscar la siguiente información:

- **Backup Object** especifica el origen de datos de los datos de copia de respaldo.
- **Backup Path** especifica la ruta completa donde se guardan los archivos de copia de respaldo.

Seleccione el elemento correcto y copie manualmente la ruta completa de los archivos de copia de respaldo de **Backup Path**.

Paso 3 En FusionInsight Manager, seleccione **O&M** > **Backup and Restoration** > **Restoration Management**.

Paso 4 Haga clic en **Create**.

Paso 5 Establezca **Task Name** en el nombre de la tarea de restauración.

Paso 6 Seleccione el clúster que se va a operar desde **Recovery Object**.

Paso 7 En el área **Restoration Configuration**, seleccione **Hive**.

Paso 8 Establezca **Path Type** de **Hive** en un tipo de directorio de copia de respaldo.

Se admiten los siguientes tipos de directorio de copia de respaldo:

- **RemoteHDFS**: indica que los archivos de copia de respaldo se almacenan en el directorio de HDFS del clúster en espera. Si selecciona **RemoteHDFS**, establezca los siguientes parámetros:
  - **Source NameService Name**: indica el nombre de NameService del clúster de datos de copia de respaldo. Puede introducir el nombre integrado de NameService del clúster remoto, por ejemplo, **haclusterX**, **haclusterX1**, **haclusterX2**, **haclusterX3** o **haclusterX4**. También puede introducir un nombre NameService configurado del clúster remoto.
  - **IP Mode**: indica el modo de la dirección IP de destino. El sistema selecciona automáticamente el modo de dirección IP en función del tipo de red del clúster, por ejemplo **IPv4** o **IPv6**.
  - **Source NameNode IP Address**: indica la dirección IP del plano de servicio NameNode del clúster en espera, que admite el nodo activo o el nodo en espera.
  - **Source Path**: indica la ruta completa del directorio HDFS para almacenar los datos de copia de respaldo del clúster en espera, por ejemplo, *Backup path/Backup task name_Data source_Task creation time*.
  - **Queue Name**: indica el nombre de la cola de Yarn utilizada para la ejecución de tareas de copia de respaldo.
  - **Recovery Point List**: Haga clic en **Refresh** y seleccione un conjunto de archivos de copia de respaldo de Hive del que se ha hecho una copia de respaldo en el clúster en espera.
  - **Target NameService Name**: indica el nombre de NameService del directorio de copia de respaldo. El valor predeterminado es **hacluster**.
  - **Maximum Number of Maps**: indica el número máximo de map en una tarea de MapReduce. El valor predeterminado es **20**.
  - **Maximum Bandwidth of a Map (MB/s)**: indica el ancho de banda máximo de un map. El valor predeterminado es **100**.
- **NFS**: indica que los archivos de copia de respaldo se almacenan en el NAS mediante el protocolo NFS. Si selecciona **NFS**, establezca los siguientes parámetros:
  - **IP Mode**: indica el modo de la dirección IP de destino. El sistema selecciona automáticamente el modo de dirección IP en función del tipo de red del clúster, por ejemplo **IPv4** o **IPv6**.
  - **Server IP Address**: indica la dirección IP del servidor NAS.

  - **Source Path**: indica la ruta completa del archivo de copia de respaldo en el servidor de NAS, por ejemplo, *Backup path/Backup task name_Data source_Task creation time*.
  - **Queue Name**: indica el nombre de la cola de Yarn utilizada para la ejecución de tareas de copia de respaldo.
  - **Recovery Point List**: Haga clic en **Refresh** y seleccione un conjunto de archivos de copia de respaldo de Hive del que se ha hecho una copia de respaldo en el clúster en espera.
  - **Target NameService Name**: indica el nombre de NameService del directorio de copia de respaldo. El valor predeterminado es **hacluster**.
  - **Maximum Number of Maps**: indica el número máximo de map en una tarea de MapReduce. El valor predeterminado es **20**.
  - **Maximum Bandwidth of a Map (MB/s)**: indica el ancho de banda máximo de un map. El valor predeterminado es **100**.
- **CIFS**: indica que los archivos de copia de respaldo se almacenan en el NAS mediante el protocolo CIFS. Si selecciona **CIFS**, establezca los siguientes parámetros:
  - **IP Mode**: indica el modo de la dirección IP de destino. El sistema selecciona automáticamente el modo de dirección IP en función del tipo de red del clúster, por ejemplo **IPv4** o **IPv6**.
  - **Server IP Address**: indica la dirección IP del servidor NAS.
  - **Port**: indica el número de puerto utilizado para conectarse al servidor NAS a través del protocolo CIFS. El valor predeterminado es **445**.
  - **Username**: indica el nombre de usuario establecido cuando se configura el protocolo CIFS.
  - **Password**: indica la contraseña establecida cuando se configura el protocolo CIFS.
  - **Source Path**: indica la ruta completa del archivo de copia de respaldo en el servidor de NAS, por ejemplo, *Backup path/Backup task name_Data source_Task creation time*.
  - **Queue Name**: indica el nombre de la cola de Yarn utilizada para la ejecución de tareas de copia de respaldo.
  - **Recovery Point List**: Haga clic en **Refresh** y seleccione un conjunto de archivos de copia de respaldo de Hive del que se ha hecho una copia de respaldo en el clúster en espera.
  - **Target NameService Name**: indica el nombre de NameService del directorio de copia de respaldo. El valor predeterminado es **hacluster**.
  - **Maximum Number of Maps**: indica el número máximo de map en una tarea de MapReduce. El valor predeterminado es **20**.
  - **Maximum Bandwidth of a Map (MB/s)**: indica el ancho de banda máximo de un map. El valor predeterminado es **100**.
- **SFTP**: indica que los archivos de copia de respaldo se almacenan en el servidor mediante el protocolo SFTP.

  Si selecciona **SFTP**, establezca los siguientes parámetros:
  - **IP Mode**: indica el modo de la dirección IP de destino. El sistema selecciona automáticamente el modo de dirección IP en función del tipo de red del clúster, por ejemplo **IPv4** o **IPv6**.
  - **Server IP Address**: indica la dirección IP del servidor donde se almacenan los datos de copia de respaldo.

- **Port**: indica el número de puerto utilizado para conectarse al servidor de copia de respaldo a través del protocolo SFTP. El valor predeterminado es **22**.
- **Username**: indica el nombre de usuario para conectarse al servidor mediante el protocolo SFTP.
- **Password**: indica la contraseña para conectarse al servidor mediante el protocolo SFTP.
- **Source Path**: indica la ruta completa del archivo de copia de respaldo en el servidor de copia de respaldo, por ejemplo, *Backup path/Backup task name_Data source_Task creation time*.
- **Queue Name**: indica el nombre de la cola de Yarn utilizada para la ejecución de tareas de copia de respaldo.
- **Recovery Point List**: Haga clic en **Refresh** y seleccione un directorio HDFS del que se ha realizado una copia de respaldo en el clúster en espera.
- **Target NameService Name**: indica el nombre de NameService del directorio de copia de respaldo. El valor predeterminado es **hacluster**.
- **Maximum Number of Maps**: indica el número máximo de map en una tarea de MapReduce. El valor predeterminado es **20**.
- **Maximum Bandwidth of a Map (MB/s)**: indica el ancho de banda máximo de un map. El valor predeterminado es **1**.

Paso 9 Establezca **Backup Data** en el **Data Configuration** en uno o varios orígenes de datos de copia de respaldo que se recuperarán según los requisitos de servicio. En las columnas **Target Database** y **Target Path**, especifique la base de datos de destino y la ruta de guardado del archivo después de la recuperación de los datos de copia de respaldo.

Restricciones de configuración:

- Los datos se pueden restaurar en la base de datos original, pero las tablas de datos deben almacenarse en una nueva ruta que sea diferente de la ruta de copia de respaldo.
- Para restaurar las tablas de índice de Hive, seleccione las tablas de datos de Hive que correspondan a las tablas de índice de Hive que se van a restaurar.
- Si se selecciona un nuevo directorio de restauración para evitar que afecte a los datos actuales, se debe conceder manualmente el permiso HDFS para que los usuarios que tienen permiso para realizar copias de respaldo de tablas puedan tener acceso a este directorio.
- Los datos se pueden restaurar en otras bases de datos. En este caso, el permiso HDFS debe concederse manualmente para que los usuarios que tienen permiso de las tablas de copia de respaldo puedan acceder al directorio HDFS que corresponde a la base de datos.

Paso 10 Establezca **Force recovery** en **true** que indica que debe recuperar a la fuerza todos los datos de copia de respaldo cuando ya existe una tabla de datos con el mismo nombre. Si la tabla de datos contiene nuevos datos agregados después de la copia de respaldo, los nuevos datos se perderán después de la recuperación de datos. Si establece el parámetro en **false**, la tarea de restauración no se ejecuta si existe una tabla de datos con el mismo nombre.

Paso 11 Haga clic en **Verify** para comprobar si la tarea de restauración está configurada correctamente.

- Si el nombre de la cola es incorrecto, la verificación falla.
- Si el directorio especificado que se va a restaurar no existe, la verificación falla.
- Si no se cumplen las condiciones de sustitución forzada, la verificación falla.

Paso 12 Haga clic en **OK**.

Paso 13 En la lista de tareas de restauración, busque una tarea creada y haga clic en **Start** en la columna **Operation** para ejecutar la tarea de restauración.

- Después de que la restauración es exitosa, la barra de progreso está en verde.
- Una vez que la restauración se realiza correctamente, la tarea de restauración no se puede ejecutar de nuevo.
- Si la tarea de restauración falla durante la primera ejecución, rectifique el error y haga clic en **Retry** para volver a ejecutar la tarea.

----Fin

7.10.3.11 Restauración de metadatos de Kafka

Escenario

Los datos de Kafka deben recuperarse en los siguientes escenarios: los datos se modifican o eliminan inesperadamente y deben restaurarse. Una vez que un administrador realiza un ajuste de datos críticos de ZooKeeper se produce una excepción o la operación no ha logrado el resultado esperado. Todos los módulos de Kafka están defectuosos y no están disponibles. Los datos se migran a un nuevo clúster.

Los administradores del sistema pueden crear una tarea de recuperación en FusionInsight Manager para recuperar datos de Kafka. Sólo se admiten las tareas de restauración manuales.

AVISO

- La restauración de datos solo se puede realizar cuando la versión del sistema es coherente con la de la copia de respaldo de datos.
- Para restaurar los metadatos de Kafka cuando el servicio se está ejecutando correctamente, se recomienda realizar una copia de respaldo manual de los metadatos de Kafka más recientes antes de la restauración. De lo contrario, los metadatos de Kafka que se generan después de la copia de respaldo de datos y antes de la restauración de datos se perderán.

Impacto en el sistema

- Después de restaurar los metadatos, se pierden los datos generados después de la copia de respaldo de datos y antes de la restauración de datos.
- Después de restaurar los metadatos, la información de desplazamiento almacenada en el ZooKeeper por los consumidores de Kafka se revierte, lo que resulta en un consumo repetido.

Prerrequisitos

- Si necesita restaurar datos desde un HDFS remoto, prepare un clúster en espera. Si el clúster activo se despliega en modo de seguridad y los clústeres activo y en espera no son gestionados por el mismo FusionInsight Manager, se ha configurado la confianza mutua. Para obtener más información, consulte **Configuración de la confianza mutua Cross-Manager entre clústeres**. Si el clúster activo se despliega en modo normal, no se requiere confianza mutua.

- Se ha configurado la replicación entre clústeres para los clústeres activo y en espera. Para obtener más información, consulte **Habilitación de la replicación entre clústeres**.
- El tiempo es consistente entre los clústeres activos y en espera y los servicios NTP en los clústeres activos y en espera utilizan la misma fuente de tiempo.
- El servicio Kafka se deshabilita primero y, a continuación, se habilita al restaurar los datos.

Procedimiento

Paso 1 En FusionInsight Manager, seleccione **O&M** > **Backup and Restoration** > **Backup Management**.

Paso 2 En la columna **Operation** de una tarea especificada en la lista de tareas, elija **More** > **View History** para ver los registros históricos de ejecución de tareas de copia de respaldo.

En la ventana que se muestra, busque un registro de éxito especificado y haga clic en **View** en la columna **Backup Path** para ver la información de la ruta de copia de respaldo de la tarea y buscar la siguiente información:

- **Backup Object** especifica el origen de datos de los datos de copia de respaldo.
- **Backup Path** especifica la ruta completa donde se guardan los archivos de copia de respaldo.

  Seleccione el elemento correcto y copie manualmente la ruta completa de los archivos de copia de respaldo de **Backup Path**.

Paso 3 En FusionInsight Manager, seleccione **O&M** > **Backup and Restoration** > **Restoration Management**.

Paso 4 Haga clic en **Create**.

Paso 5 Establezca **Task Name** en el nombre de la tarea de restauración.

Paso 6 Seleccione el clúster que se va a operar desde **Recovery Object**.

Paso 7 En el área **Restoration Configuration**, seleccione **Kafka**.

Paso 8 Establezca **Path Type** de **Kafka** en un tipo de directorio de copia de respaldo.

La configuración varía según los tipos de directorios de copia de respaldo:

- **LocalDir**: indica que los archivos de copia de respaldo se almacenan en el disco local del nodo de gestión activa.

  Si selecciona **LocalDir**, también debe configurar **Source Path** para que seleccione el archivo de copia de respaldo que se va a restaurar, por ejemplo, *Version_Data source_Task execution time*.**tar.gz**.
- **LocalHDFS**: indica que los archivos de copia de respaldo se almacenan en el directorio de HDFS del clúster actual.

  Si selecciona **LocalHDFS**, establezca los siguientes parámetros:
  - **Source Path**: indica la ruta completa del archivo de copia de respaldo en el HDFS, por ejemplo, *Backup path/Backup task name_Task creation time/Version_Data source_Task execution time*.**tar.gz**.
  - **Source NameService Name**: indica el nombre NameService que corresponde al directorio de copia de respaldo cuando se ejecuta una tarea de restauración. El valor predeterminado es **hacluster**.

- **RemoteHDFS**: indica que los archivos de copia de respaldo se almacenan en el directorio de HDFS del clúster en espera.

  Si selecciona **RemoteHDFS**, establezca los siguientes parámetros:

  – **Source NameService Name**: indica el nombre de NameService del clúster de datos de copia de respaldo. Puede introducir el nombre integrado de NameService del clúster remoto, por ejemplo, **haclusterX**, **haclusterX1**, **haclusterX2**, **haclusterX3** o **haclusterX4**. También puede introducir un nombre NameService configurado del clúster remoto.

  – **IP Mode**: indica el modo de la dirección IP de destino. El sistema selecciona automáticamente el modo de dirección IP en función del tipo de red del clúster, por ejemplo **IPv4** o **IPv6**.

  – **Source NameNode IP Address**: indica la dirección IP del plano de servicio NameNode del clúster en espera, que admite el nodo activo o el nodo en espera.

  – **Source Path**: indica la ruta completa del directorio HDFS para almacenar los datos de copia de respaldo del clúster en espera, por ejemplo, *Backup path/Backup task name_Data source_Task creation time/Version_Data source_Task execution time***.tar.gz**.

  – **Queue Name**: indica el nombre de la cola de Yarn utilizada para la ejecución de tareas de copia de respaldo. El nombre debe ser el mismo que el nombre de la cola que se está ejecutando correctamente en el clúster.

- **NFS**: indica que los archivos de copia de respaldo se almacenan en el NAS mediante el protocolo NFS.

  Si selecciona **NFS**, establezca los siguientes parámetros:

  – **IP Mode**: indica el modo de la dirección IP de destino. El sistema selecciona automáticamente el modo de dirección IP en función del tipo de red del clúster, por ejemplo **IPv4** o **IPv6**.

  – **Server IP Address**: indica la dirección IP del servidor NAS.

  – **Source Path**: indica la ruta completa del archivo de copia de respaldo en el servidor NAS, por ejemplo, *Backup path/Backup task name_Data source_Task creation time/Version_Data source_Task execution time***.tar.gz**.

- **CIFS**: indica que los archivos de copia de respaldo se almacenan en el NAS mediante el protocolo CIFS.

  Si selecciona **CIFS**, establezca los siguientes parámetros:

  – **IP Mode**: indica el modo de la dirección IP de destino. El sistema selecciona automáticamente el modo de dirección IP en función del tipo de red del clúster, por ejemplo **IPv4** o **IPv6**.

  – **Server IP Address**: indica la dirección IP del servidor NAS.

  – **Port**: indica el número de puerto utilizado para conectarse al servidor NAS a través del protocolo CIFS. El valor predeterminado es **445**.

  – **Username**: indica el nombre de usuario establecido cuando se configura el protocolo CIFS.

  – **Password**: indica la contraseña establecida cuando se configura el protocolo CIFS.

  – **Source Path**: indica la ruta completa del archivo de copia de respaldo en el servidor NAS, por ejemplo, *Backup path/Backup task name_Data source_Task creation time/Version_Data source_Task execution time***.tar.gz**.

- **OBS**: indica que los archivos de copia de respaldo se almacenan en OBS.

  Si selecciona **OBS**, establezca los siguientes parámetros:

– **Source Path**: indica la ruta de acceso OBS completa de un archivo de copia de respaldo, por ejemplo, *Backup path/Backup task name_Data source_Task creation time/Version_Data source_Task execution time***.tar.gz**.

NOTA

Solo MRS 3.1.0 o posterior admite el almacenamiento de archivos de copia de respaldo en OBS.

Paso 9 Haga clic en **OK**.

Paso 10 En la lista de tareas de restauración, busque una tarea creada y haga clic en **Start** en la columna **Operation** para ejecutar la tarea de restauración.

- Después de que la restauración es exitosa, la barra de progreso está en verde.
- Una vez que la restauración se realiza correctamente, la tarea de restauración no se puede ejecutar de nuevo.
- Si la tarea de restauración falla durante la primera ejecución, rectifique el error y haga clic en **Retry** para volver a ejecutar la tarea.

AVISO

– Si el servicio Kafka se elimina una vez completada la copia de respaldo, reinstale el servicio Kafka, restaure sus metadatos y reinicie el servicio Kafka. Se encuentra que el servicio Broker no se puede iniciar. En este caso, el archivo **/var/log/Bigdata/kafka/broker/server.log** contiene un error. Un ejemplo de error es el siguiente:

```
ERROR Fatal error during KafkaServer startup. Prepare to shutdown
(kafka.server.KafkaServer)kafka.common.InconsistentClusterIdException: The
Cluster ID kVSgfurUQFGGpHMTBqBPiw doesn't match stored clusterId
Some(0Qftv9yBTAmf2iDPSlIk7g) in meta.properties. The broker is trying to
join the wrong cluster. Configured zookeeper.connect may be wrong. at
kafka.server.KafkaServer.startup(KafkaServer.scala:220) at
kafka.server.KafkaServerStartable.startup(KafkaServerStartable.scala:44)
at kafka.Kafka$.main(Kafka.scala:84) at kafka.Kafka.main(Kafka.scala)
```

Compruebe el valor de **log.dirs** en el archivo de configuración de Kafka Broker **${BIGDATA_HOME}/Fusionsight_Current/*Broker/etc/server.properties**. El valor es el directorio de datos de Kafka. Vaya al directorio de datos de Kafka y cambie el valor **0Qftv9yBTAmf2iDPSlIk7g** de **cluster.id** en **meta.properties** a **kVSgfurUQFGGpHMTBqBPiw** (el último valor en el registro de errores).

– La modificación anterior debe realizarse en cada nodo donde se encuentra Broker. Después de la modificación, reinicie el servicio Kafka.

----Fin

7.10.4 Habilitación de la replicación entre clústeres

Escenario

DistCp se utiliza para replicar los datos almacenados en HDFS desde un clúster a otro clúster. DistCp depende de la función de replicación entre clústeres, que está deshabilitada de forma predeterminada. Necesita habilitarlo para ambos clústeres.

Esta sección describe cómo modificar parámetros en FusionInsight Manager para habilitar la función de replicación entre clústeres. Una vez habilitada esta función, puede crear una tarea

de copia de respaldo para realizar copias de respaldo de los datos en el HDFS remoto (RemoteHDFS).

Impacto en el sistema

Yarn necesita reiniciarse para habilitar la función de replicación entre clústeres y no se puede acceder durante el reinicio.

Prerrequisitos

- El parámetro **hadoop.rpc.protection** de HDFS en los dos clústeres para la replicación de datos debe utilizar el mismo modo de transmisión de datos. El valor predeterminado es **privacy**, que indica la transmisión cifrada. El valor **authentication** indica que la transmisión no está cifrada.
- Para los clústeres en modo de seguridad, debe configurar la confianza mutua entre clústeres.

Procedimiento

Paso 1 Inicie sesión en FusionInsight Manager de uno de los dos clústeres.

Paso 2 Elija **Cluster** > ***Name of the desired cluster*** **> Services** > **Yarn** > **Configurations** y haga clic en **All Configurations**.

Paso 3 En el panel de navegación, elija **Yarn** >**Distcp**.

Paso 4 Modifique **dfs.NameNode.rpc-address** y establezca **haclusterX.remotenn1** en la dirección IP del servicio y el puerto RPC de una instancia de NameNode del clúster de pares, y establezca **haclusterX.remotenn2** en la dirección IP del servicio y el número de puerto RPC de la otra instancia de NameNode del clúster de pares.

haclusterX.remotenn1 y **haclusterX.remotenn2** no distinguen las NameNodes activas y en espera. El puerto RPC de NameNode predeterminado es 8020 y no se puede modificar en Manager.

Ejemplos de valores de parámetros modificados: **10.1.1.1:8020** y **10.1.1.2:8020**.

NOTA

- Si los datos del clúster actual necesitan ser respaldados en el HDFS de varios clústeres, puede configurar las direcciones RPC de NameNode correspondientes en haclusterX1, haclusterX2, haclusterX3 y haclusterX4.

Paso 5 Haga clic en **Save**. En el cuadro de diálogo de confirmación, haga clic en **OK**.

Paso 6 Reinicie el servicio Yarn.

Paso 7 Inicie sesión en FusionInsight Manager del otro clúster y repita **Paso 2** a **Paso 6**.

----Fin

7.10.5 Gestión de tareas de restauración rápida locales

Escenario

Cuando se utiliza DistCp para realizar una copia de respaldo de los datos, la instantánea de copia de respaldo se guarda en HDFS del clúster activo. FusionInsight Manager admite el uso

de la instantánea local para una restauración rápida de datos, lo que requiere menos tiempo que la restauración de datos desde el clúster en espera.

Utilice FusionInsight Manager y las instantáneas en HDFS del clúster activo para crear una tarea de restauración rápida local y ejecutar la tarea.

Procedimiento

Paso 1 En FusionInsight Manager, seleccione **O&M** > **Backup and Restoration** > **Backup Management**.

Paso 2 En la lista de tareas de copia de respaldo, busque una tarea creada y haga clic en **Restore** en la columna **Operation**.

Paso 3 Compruebe si el sistema muestra "No data is available for quick restoration. Create a task on the restoration management page to restore data".

- En caso afirmativo, haga clic en **OK** para cerrar el cuadro de diálogo. No se crea ninguna instantánea de datos de copia de respaldo en el clúster activo y no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 4** para crear una tarea de restauración rápida local.

NOTA

Los metadatos no admiten la restauración rápida.

Paso 4 Establezca **Name** en el nombre de la tarea de restauración rápida local.

Paso 5 Establezca **Configuration** en un origen de datos.

Paso 6 Establezca **Recovery Point List** en un punto de recuperación que contenga los datos de copia de respaldo.

Paso 7 Establezca **Queue Name** en el nombre de la cola Yarn utilizada en la ejecución de la tarea. El nombre debe ser el mismo que el nombre de la cola que se está ejecutando correctamente en el clúster.

Paso 8 Establezca **Data Configuration** en el objeto que se va a recuperar.

Paso 9 Haga clic en **Verify** y espere a que el sistema muestre "The restoration task configuration is verified successfully."

Paso 10 Haga clic en **OK**.

Paso 11 En la lista de tareas de restauración, busque una tarea creada y haga clic en **Start** en la columna **Operation** para ejecutar la tarea de restauración.

Una vez completada la tarea, **Task Status** de la tarea se muestra como **Successful**.

----Fin

7.10.6 Modificación de una tarea de copia de respaldo

Escenario

Esta sección describe cómo modificar los parámetros de una tarea de copia de respaldo creada en FusionInsight Manager para cumplir con los requisitos de servicio cambiantes. Los parámetros de las tareas de restauración solo se pueden ver, pero no se pueden modificar.

Impacto en el sistema

Después de modificar una tarea de copia de respaldo, los nuevos parámetros surten efecto cuando la tarea se ejecute la próxima vez.

Prerrequisitos

- Se ha creado una tarea de copia de respaldo.
- Se ha planificado una nueva política de tareas de copia de respaldo en función de la situación real.

Procedimiento

Paso 1 En FusionInsight Manager, seleccione **O&M** > **Backup and Restoration** > **Backup Management**.

Paso 2 En la lista de tareas, busque una tarea especificada, haga clic en **Configure** en la columna **Operation** para ir a la página de modificación de configuración.

En la página mostrada, modifique los siguientes parámetros:

- Started
- Period
- Destination NameService Name
- Target NameNode IP Address
- Target Path
- Max Number of Backup Copies
- Maximum Number of Recovery Points
- Maximum Number of Maps
- Maximum Bandwidth of a Map

NOTA

Después de modificar el parámetro **Target Path** de una tarea de copia de respaldo, esta tarea se realizará como una tarea de copia de respaldo completa por primera vez de forma predeterminada.

Paso 3 Haga clic en **OK** para guardar la configuración.

----Fin

7.10.7 Consulta de tareas de copia de respaldo y restauración

Escenario

Esta sección describe cómo ver las tareas de copia de respaldo y recuperación creadas y comprobar su estado de ejecución en FusionInsight Manager.

Prerrequisitos

Ha iniciado sesión en FusionInsight Manager.

Procedimiento

Paso 1 En FusionInsight Manager, elija **O&M** >**Backup and Restoration**.

Paso 2 Haga clic en **Backup Management** o **Restoration Management**.

Paso 3 En la lista de tareas, obtenga el resultado de ejecución anterior en las columnas **Task Status** y **Task Progress**. El verde indica que la tarea se ejecuta correctamente y el rojo indica que la ejecución falla.

Paso 4 En la columna **Operation** de una tarea especificada en la lista de tareas, elija **More** > **View History** o haga clic en **View History** para ver el registro histórico de la ejecución de tareas de copia de respaldo y restauración.

En la ventana mostrada, haga clic en antes de un registro especificado para mostrar información de registro sobre la ejecución.

----Fin

Tareas relacionadas

- Iniciar una tarea de copia de respaldo o restauración

  En la lista de tareas, busque una tarea especificada y elija **More** > **Back Up Now** o haga clic en **Start** en la columna **Operation** para iniciar una tarea de copia de respaldo o restauración que esté lista o no se ejecute. Las tareas de restauración ejecutadas no se pueden ejecutar repetidamente.

- Detener una tarea de copia de respaldo o restauración

  En la lista de tareas, busque una tarea especificada y elija **More** > **Stop** o haga clic en **Stop** en la columna **Operation** para detener una tarea de copia de respaldo o restauración que se está ejecutando. Una vez que la tarea se detiene correctamente, su **Task Status** cambia a **Stopped**.

- Eliminar una tarea de copia de respaldo o restauración

  En la lista de tareas, busque una tarea especificada y elija **More** > **Delete** o haga clic en **Delete** en la columna **Operation** para eliminar una tarea de copia de respaldo o restauración. Los datos de copia de respaldo se reservarán de forma predeterminada después de eliminar una tarea.

- Suspender una tarea de copia de respaldo

  En la lista de tareas, busque una tarea especificada y elija **More** > **Suspend** en la columna **Operation** para suspender una tarea de copia de respaldo. Solo se pueden suspender las tareas de copia de respaldo periódicas. Las tareas de copia de respaldo suspendidas ya no se ejecutan automáticamente. Cuando suspende una tarea de copia de respaldo que se está ejecutando, la ejecución de la tarea se detiene. Para reanudar una tarea, elija **More** >**Resume**.

7.10.8 ¿Cómo configuro el entorno al crear una tarea de copia de respaldo de ClickHouse en el FusionInsight Manager y establecer el tipo de ruta en RemoteHDFS?

NOTA

Esta sección se aplica únicamente a MRS 3.1.0 y 3.1.2.

Pregunta

¿Cómo configuro el entorno al crear una tarea de copia de respaldo de ClickHouse en el FusionInsight Manager y establecer el tipo de ruta en RemoteHDFS?

Respuesta

Paso 1 Inicie sesión en FusionInsight Manager del clúster en espera.

Paso 2 Elija **Cluster** > **Services** > **HDFS** y seleccione **More** > **Download Client**. Establezca **Select Client Type** en **Configuration Files Only** y seleccione **x86_64** para x86 o **aarch64** para ARM en función del tipo del nodo en el que se va a instalar el cliente y haga clic en **OK**.

Paso 3 Después de generar el paquete de archivo del cliente, descargue el cliente en el PC local como se le solicite y descomprima el paquete.

Por ejemplo, si el paquete de archivo del cliente es **FusionInsight_Cluster_1_HDFS_Client.tar** descomprima para obtener **FusionInsight_Cluster_1_HDFS_ClientConfig_ConfigFiles.tar** y, a continuación, descomprima **FusionInsight_Cluster_1_HDFS_ClientConfig_ConfigFiles.tar** en el directorio **D:\FusionInsight_Cluster_1_HDFS_ClientConfig_ConfigFiles** del PC local. El nombre del directorio no puede contener espacios.

Paso 4 Vaya al directorio del cliente **FusionInsight_Cluster_1_HDFS_ClientConfig_ConfigFiles** y obtenga el archivo **hosts**.

Paso 5 Vaya a **FusionInsight_Cluster_1_HDFS_ClientConfig_ConfigFiles\HDFS\config** para obtener los archivos **core-site.xml** y **hdfs-site.xml**.

Paso 6 Inicie sesión en FusionInsight Manager del clúster de origen.

Paso 7 Elija **Cluster** > **Services** > **ClickHouse**, elija **Configurations** > **All Configurations**, y seleccione **backup** bajo **ClickHouse(Service)**.

Para **remote_connect_core_config_file**, haga clic en **Upload File** y seleccione el archivo **core-site.xml** preparado en **Paso 5**.

Para **remote_connect_hdfs_config_file**, haga clic en **Upload File** y seleccione el archivo **hdfs-site.xml** preparado en **Paso 5**.

Paso 8 Haga clic en **Save**, confirme la información y haga clic en **OK** para guardar la configuración. Después de guardar las configuraciones, haga clic en **Finish**.

Paso 9 Elija **Cluster** > **Services** > **ClickHouse**, haga clic en **Instance**, y vea la dirección IP de instancia de **ClickHouseServer**.

Paso 10 Inicie sesión en los nodos host de las instancias ClickHouseServer como usuario **root** y compruebe si el archivo **/etc/hosts** contiene la información del host en **Paso 4**. Si no es así, agregue la información del host en **Paso 4** al archivo **/etc/hosts**.

----Fin

7.11 Gestión de la seguridad

7.11.1 Descripción de seguridad

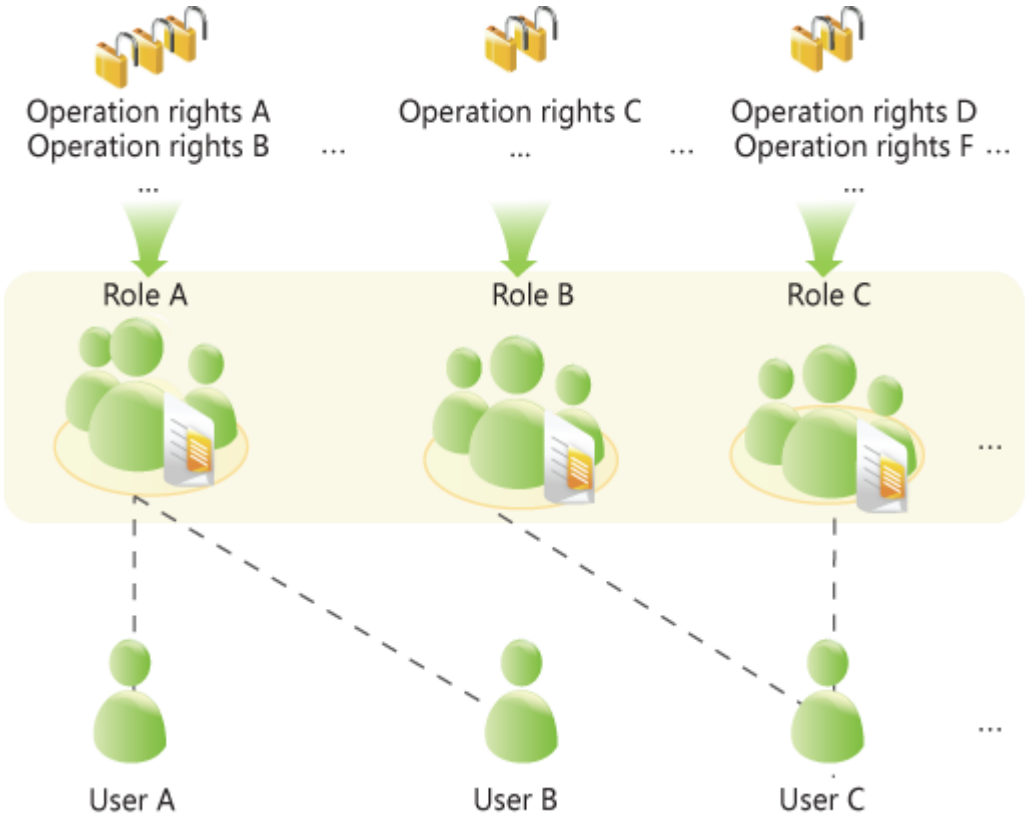
7.11.1.1 Modelo de derecho

Control de acceso basado en roles

FusionInsight adopta el modo de control de acceso basado en roles (RBAC) para gestionar los derechos en el sistema de big data. Integra las funciones de gestión correctas de los componentes para gestionar de forma centralizada los derechos. Los usuarios comunes están protegidos de los detalles internos de gestión de derechos, y las operaciones de gestión correctas se simplifican para los administradores, mejorando la usabilidad y la experiencia del usuario de la gestión correctas.

El modelo correcto de FusionInsight consta de cuatro partes, es decir, usuarios, grupos de usuarios, roles y derechos.

Figura 7-60 Modelo de derecho



- **Derecho**

  Derecho, que está definida por componentes, permite a los usuarios acceder a un determinado recurso de un componente. Diferentes componentes tienen derechos diferentes para sus recursos.

  Por ejemplo:

  – HDFS proporciona permisos de lectura, escritura y ejecución en archivos.
  – HBase proporciona permisos de creación, lectura y escritura en tablas.

- **Rol**

  El rol es un conjunto de derechos de componente. Cada rol puede tener varios derechos de varios componentes. Diferentes roles pueden tener los derechos de un recurso de un componente.

- **Grupo de usuario**

  El grupo de usuarios es una colección de usuarios. Cuando un grupo de usuarios está enlazado a un rol, los usuarios de este grupo obtienen los derechos definidos por el rol.

  Se pueden asociar diferentes grupos de usuarios con el mismo rol. Un grupo de usuarios también puede estar asociado con ningún rol, y este grupo de usuarios no tiene los derechos de ningún recurso de componente.

  NOTA

  En algunos componentes, el sistema otorga derechos relacionados a grupos de usuarios específicos de forma predeterminada.

- **Usuario**

  Un usuario es un visitante del sistema. Cada usuario tiene los derechos del grupo de usuarios y el rol asociado al usuario. Los usuarios deben agregarse al grupo de usuarios o asociarse con roles para obtener los derechos correspondientes.

Control de acceso basado en políticas

El componente Ranger utiliza el control de acceso basado en políticas (PBAC) para gestionar derechos e implementar un control de acceso a datos detallado en componentes como HDFS, Hive y HBase.

NOTA

El componente solo soporta un mecanismo de control correcto. Una vez habilitada la política de control de derechos de Ranger para el componente, el derecho del componente en el rol creado en FusionInsight Manager no es válido (Las reglas ACL de HDFS y Yarn todavía entran en vigor). Debe agregar una política en la página de gestión de Ranger para conceder derechos sobre los recursos.

El modelo de derecho de Ranger consta de varias políticas correctas. Una política correcta consta de las siguientes partes:

- Recurso

  Los recursos son proporcionados por componentes y los usuarios pueden acceder a ellos, como archivos o carpetas HDFS, colas en Yarn y bases de datos, tablas y columnas en Hive.

- Usuario

  Un usuario es un visitante del sistema. Los derechos de cada usuario se obtienen en base a la política asociada al usuario. La información sobre usuarios, grupos de usuarios y roles en LDAP se sincroniza periódicamente con el Ranger.

- Permiso

  En una política, puede configurar varias condiciones de acceso para los recursos, como lectura y escritura de archivos, condiciones de permiso, condiciones de rechazo y condiciones de excepción.

7.11.1.2 Mecanismo de derecho

FusionInsight adopta el protocolo ligero de acceso a directorios (LDAP) para almacenar datos de usuarios y grupos de usuarios. La información sobre las definiciones de roles se almacena en la base de datos relacional y la asignación entre roles y derechos se guarda en componentes.

FusionInsight utiliza Kerberos para la autenticación unificada.

El proceso de verificación de los derechos de usuario es el siguiente:

1. Un cliente (un terminal de usuario o servicio de componente FusionInsight) invoca la interfaz de autenticación FusionInsight.
2. FusionInsight utiliza el nombre de usuario y la contraseña de inicio de sesión para la autenticación de Kerberos.
3. Si la autenticación se realiza correctamente, el cliente envía una solicitud para acceder al servidor (un servicio de componentes de FusionInsight).
4. El servidor encuentra el grupo de usuarios y el rol al que pertenece el usuario de inicio de sesión.
5. El servidor obtiene todos los derechos del grupo de usuarios y del rol.
6. El servidor comprueba si el cliente tiene derecho a acceder a los recursos para los que se aplica.

Ejemplo (RBAC):

Hay tres archivos en HDFS, es decir, fileA, fileB y fileC.

- roleA tiene derecho de lectura y escritura para fileA, y roleB tiene derecho de lectura para fileB.
- groupA está unido al roleA, y el groupB está unido al roleB.
- userA pertenece a groupA y roleB, y userB pertenece a groupB.

Cuando el usuarioA inicia sesión correctamente en el sistema y accede a HDFS:

1. HDFS obtiene el rol (roleB) al que está enlazado el userA.
2. HDFS también obtiene el rol (roleA) al que está enlazado el grupo de usuarios de userA.
3. En este caso, userA tiene todos los derechos de roleA y roleB.
4. Como resultado, userA tiene derechos de lectura y escritura para fileA, tiene el derecho de lectura en fileB, y no tiene derecho para fileC.

Del mismo modo, cuando el userB inicia sesión correctamente en el sistema y accede a HDFS:

1. userB solo tiene los derechos de roleB.
2. Como resultado, userB tiene el derecho de lectura en fileB, y no tiene derechos para fileA y fileC.

7.11.1.3 Políticas de autenticación

La plataforma de big data realiza autenticación de identidad de usuario para evitar que los usuarios no válidos accedan al clúster. El clúster proporciona capacidades de autenticación tanto en modo de seguridad como en modo normal.

Modo de seguridad

Los clústeres en modo de seguridad utilizan el protocolo de autenticación Kerberos para la autenticación de seguridad. El protocolo Kerberos admite la autenticación mutua entre clientes y servidores. Esto elimina los riesgos incurridos al enviar credenciales de usuario a través de la red para la autenticación simulada. En los clústeres, KrbServer proporciona soporte de autenticación de Kerberos.

Objeto de usuario de Kerberos

En el protocolo de Kerberos, cada objeto de usuario es un principal. Un principal completo consiste en nombre de usuario y nombre de dominio. En escenarios de O&M o desarrollo de aplicaciones, la identidad del usuario debe verificarse antes de que un cliente se conecte a un servidor. Los usuarios para operaciones de operación y mantenimiento se clasifican en usuarios hombre-máquina y máquina-máquina. La contraseña de los usuarios hombre-máquina se configura manualmente, mientras que la contraseña de los usuarios máquina-máquina se genera aleatoriamente por el sistema.

Autenticación de Kerberos

Kerberos admite la autenticación de contraseña y keytab. El período de validez de la autenticación es de 24 horas por defecto.

- Autenticación de contraseña: La identidad del usuario se verifica introduciendo la contraseña correcta. Este modo se utiliza principalmente en escenarios O&M donde se utilizan usuarios hombre-máquina. El comando de configuración es **kinit** *Username*.
- Autenticación de Keytab: Los archivos Keytab contienen información de credenciales encriptada y principal de los usuarios. Cuando se utilizan archivos keytab para la autenticación, el sistema utiliza automáticamente información de credenciales cifradas para realizar la autenticación y no es necesario introducir la contraseña de usuario. Este modo se utiliza principalmente en escenarios de desarrollo de aplicaciones de componentes en los que se utilizan usuarios máquina-máquina. La autenticación Keytab también se puede configurar mediante el comando **kinit**.

Modo normal

Los diferentes componentes de un clúster normal utilizan el modo de autenticación de código abierto nativo y no admiten el comando de autenticación **kinit**. FusionInsight Manager (incluidos DBService, KrbServer y LdapServer) utiliza el nombre de usuario y la contraseña para la autenticación. **Tabla 7-82** enumera los modos de autenticación utilizados por los componentes.

Tabla 7-82 Modos de autenticación de componentes

Servicio	Modo de autenticación
ClickHouse	Autenticación simple
Flume	Sin autenticación
HBase	● Web UI: sin autenticación ● Cliente: autenticación simple
HDFS	● Web UI: sin autenticación ● Cliente: autenticación simple
HetuEngine	● Web UI: sin autenticación ● Cliente: sin autenticación
Hive	Autenticación simple
Hue	Autenticación de nombre de usuario y contraseña
Kafka	Sin autenticación

Servicio	Modo de autenticación
Loader	● Web UI: autenticación de nombre de usuario y contraseña ● Cliente: sin autenticación
MapReduce	● Web UI: sin autenticación ● Cliente: sin autenticación
Oozie	● Web UI: autenticación de nombre de usuario y contraseña ● Cliente: autenticación simple
Spark2x	● Web UI: sin autenticación ● Cliente: autenticación simple
Storm	Sin autenticación
YARN	● Web UI: sin autenticación ● Cliente: autenticación simple
ZooKeeper	Autenticación simple

Los modos de autenticación son los siguientes:

- Autenticación simple: Cuando el cliente se conecta al servidor, el cliente autentica automáticamente al usuario (por ejemplo, el usuario del sistema operativo **root** o **omm**) de forma predeterminada. La autenticación es imperceptible para el administrador o usuario del servicio, que no requiere **kinit**.
- Autenticación de nombre de usuario y contraseña: utilice el nombre de usuario y la contraseña de los usuarios humano-máquina en el clúster para la autenticación.
- Sin autenticación: cualquier usuario puede acceder al servidor de forma predeterminada.

7.11.1.4 Políticas de verificación de permisos

Modo de seguridad

Después de que un usuario es autenticado por la plataforma de big data, el sistema determina si verificar el permiso del usuario basándose en la configuración de gestión de permisos real para asegurarse de que el usuario tiene permiso limitado o todos los permisos sobre recursos. Si el usuario no tiene el permiso para acceder a los recursos del clúster, el administrador del sistema debe conceder el permiso necesario al usuario. De lo contrario, el usuario no puede acceder a los recursos. El clúster proporciona capacidades de verificación de permisos tanto en modo de seguridad como en modo normal. Los elementos de permiso específicos de los componentes son los mismos en los dos modos.

De forma predeterminada, el servicio Ranger está instalado y la autenticación Ranger está habilitada para un clúster recién instalado en modo de seguridad. Puede establecer políticas de acceso de seguridad detalladas para acceder a los recursos del componente a través del complemento de permiso del componente. Si no se requiere la autenticación de Ranger, los administradores pueden deshabilitarla manualmente en la página de servicio. Después de deshabilitar la autenticación de Ranger, el sistema continúa realizando el control de permisos

basado en el modelo de rol del FusionInsight Manager al acceder a los recursos de los componentes.

En un clúster en modo de seguridad, los siguientes componentes admiten la autenticación de Ranger: HDFS, YARN, Kafka, Hive, HBase, Storm, Impala, HetuEngine, y Spark2x.

Para un clúster actualizado desde una versión anterior, la autenticación de Ranger no se utiliza de forma predeterminada cuando los usuarios acceden a los recursos de componentes. El administrador puede habilitar manualmente la autenticación de Ranger después de instalar Ranger.

De forma predeterminada, todos los componentes del clúster de la edición de seguridad autentican el acceso. La función de autenticación no se puede deshabilitar.

Modo normal

Diferentes componentes en un clúster normal utilizan su propio comportamiento de autenticación de código abierto nativo. **Tabla 7-83** lista modos detallados de verificación de permisos.

En un clúster normal, Ranger admite el control de permisos en recursos de componentes basados en usuarios de sistema operativo. Los siguientes componentes son compatibles con la autenticación de Ranger: HBase, HDFS, Hive, Spark2x y YARN.

Tabla 7-83 Modos de verificación de permisos de componentes en clústeres normales

Servicio	Verificación de permisos	Activación y desactivación de la verificación de permisos
ClickHouse	Requerido	No soportado
Flume	No requerido	No soportado
HBase	No requerido	Soportado
HDFS	Requerido	Soportado
HetuEngine	No requerido	No soportado
Hive	No requerido	No soportado
Hue	No requerido	No soportado
Kafka	No requerido	No soportado
Loader	No requerido	No soportado
MapReduce	No requerido	No soportado
Oozie	Requerido	No soportado
Spark2x	No requerido	No soportado
Storm	No requerido	No soportado
YARN	No requerido	Soportado
ZooKeeper	Requerido	Soportado

7.11.1.5 Lista de cuentas de usuario

Clasificación de usuario

El clúster de proporciona los tres tipos de usuarios siguientes. El administrador del sistema debe cambiar periódicamente las contraseñas. No se recomienda utilizar las contraseñas predeterminadas.

NOTA

En esta sección se describen los usuarios predeterminados en el clúster MRS.

Tipo de usuario	Descripción
Usuarios del sistema	● Usuario creado en FusionInsight Manager para escenarios de operación y servicio. Hay dos tipos de usuarios: – Usuario de **Human-machine**: utilizado en escenarios como FusionInsight Manager O&M y operaciones en un cliente de componentes. Al crear un usuario de este tipo, debe establecer una contraseña y confirmarla haciendo referencia a **Creación de un usuario**. – Usuario de **Machine-machine**: utilizado para el desarrollo de aplicaciones del sistema. ● Usuario que ejecuta procesos OMS
Usuarios internos del sistema	Usuario interno para realizar autenticación Kerberos, procesar comunicaciones, guardar información de grupo de usuarios y asociar permisos de usuario. Se recomienda que los usuarios internos del sistema no se utilicen en escenarios O&M. Las operaciones se pueden realizar como usuario **admin** de u otro usuario creado por el administrador del sistema en función de los requisitos de servicio.
Usuarios de la base de datos	● Usuario que gestiona la base de datos de OMS y accede a los datos ● Usuario que ejecuta componentes de servicio (Hue, Hive, HetuEngine, Loader, Oozie, Ranger, y DBService) en la base de datos.

Usuarios del sistema

NOTA

- Se requiere el usuario **root** del sistema operativo, la contraseña del **root** de usuario en todos los nodos debe ser la misma.
- Se requiere usuario **Idap** del sistema operativo. No elimine esta cuenta. De lo contrario, es posible que el clúster no funcione correctamente. El administrador del sistema operativo mantiene las políticas de gestión de contraseñas.

Tipo de usuario	Nombre de usuario	Contraseña inicial	Descripción	Método de cambio de contraseña
Administrador del sistema	admin	Contraseña definida por el usuario	Administrador de FusionInsight Manager. **NOTA** De forma predeterminada, el usuario **admin** no tiene el permiso de gestión en otros componentes. Por ejemplo, al acceder a la interfaz de usuario nativa de un componente, el usuario no puede acceder a la información completa del componente debido a un permiso de gestión insuficiente en el componente.	Para obtener más información, consulte **Cambio de la contraseña para el usuario admin**.
Usuario del sistema operativo del nodo	ommdba	Contraseña aleatoria	Usuario que crea la base de datos del sistema. Este usuario es un usuario del sistema operativo generado en el nodo de gestión y no requiere una contraseña unificada. Esta cuenta no se puede utilizar para el inicio de sesión remoto.	Para obtener más información, consulte **Cambio de la contraseña de un usuario de sistema operativo**.
	omm	Bigdata123@	Usuario interno en ejecución del sistema. Este usuario es un usuario del sistema operativo generado en todos los nodos y no requiere una contraseña unificada.	

Usuarios internos del sistema

Tipo de usuario	Usuario predeterminado	Contraseña inicial	Descripción	Método de cambio de contraseña
Administrador de Kerberos	kadmin/admin	Admin@123	Se utiliza para agregar, eliminar, modificar y consultar cuentas de usuario en Kerberos.	Para obtener más información, consulte **Cambio de la contraseña para el administrador de Kerberos**.

Tipo de usuario	Usuario predeterminado	Contraseña inicial	Descripción	Método de cambio de contraseña
Administrador de OMS Kerberos	kadmin/admin	Admin@123	Se utiliza para agregar, eliminar, modificar y consultar cuentas de usuario en OMS Kerberos.	Para obtener más información, consulte **Cambio de la contraseña para el administrador de OMS Kerberos**.
Administrador de LDAP	cn=root,dc=hadoop,dc=com	● Versiones anteriores a MRS 3.1.2: LdapChangeMe@123 ● MRS 3.1.2 o posterior: generado aleatoriamente por el sistema	Se utiliza para agregar, eliminar, modificar y consultar la información de la cuenta de usuario en LDAP.	● Para versiones anteriores a MRS 3.1.2, consulte **Cambio de las contraseñas del administrador LDAP y del usuario LDAP (incluido OMS LDAP)**. ● Para MRS 3.1.2 o posterior, consulte **Modificación de los parámetros de configuración del servicio OMS**.

Tipo de usuario	Usuario predeterminado	Contraseña inicial	Descripción	Método de cambio de contraseña
Administrador de OMS LDAP	cn=root,dc=hadoop,dc=com	• Versiones anteriores a MRS 3.1.2: LdapChangeMe@123 • MRS 3.1.2 o posterior: generado aleatoriamente por el sistema	Se utiliza para agregar, eliminar, modificar y consultar la información de la cuenta de usuario en LDAP de OMS.	
Usuario de LDAP	cn=pg_search_dn,ou=Users,dc=hadoop,dc=com	Generado aleatoriamente por el sistema	Se utiliza para consultar información acerca de usuarios y grupos de usuarios en LDAP.	
OMS LDAP user	cn=pg_search_dn,ou=Users,dc=hadoop,dc=com	Generado aleatoriamente por el sistema	Se utiliza para consultar información acerca de usuarios y grupos de usuarios en OMS LDAP.	

Tipo de usuario	Usuario predeterminado	Contraseña inicial	Descripción	Método de cambio de contraseña
Cuenta de administrador de LDAP	cn=krbkdc,ou=Users,dc=hadoop,dc=com	● Versiones anteriores a MRS 3.1.2: LdapChangeMe@123 ● MRS 3.1.2 o posterior: generado aleatoriamente por el sistema	Se utiliza para consultar información de cuenta de autenticación de componentes de Kerberos.	● Para versiones anteriores a MRS 3.1.2, consulte **Cambio de la contraseña del administrador LDAP**. ● Para MRS 3.1.2 o posterior, consulte **Modificación de los parámetros de configuración del servicio OMS**.
	cn=krbadmin,ou=Users,dc=hadoop,dc=com	● Versiones anteriores a MRS 3.1.2: LdapChangeMe@123 ● MRS 3.1.2 o posterior: generado aleatoriamente por el sistema	Se utiliza para agregar, eliminar, modificar y consultar información de cuenta de autenticación de componentes de Kerberos.	

Tipo de usuario	Usuario predeterminado	Contraseña inicial	Descripción	Método de cambio de contraseña
Usuario en ejecución de componentes	hdfs	Hdfs@123	Este usuario es administrador del sistema HDFS y tiene los siguientes permisos: 1. Permisos de operación del sistema de archivos: ● Visualiza, modifica y crea archivos. ● Visualiza y crea directorios. ● Visualiza y modifica los grupos a los que pertenecen los archivos. ● Visualiza y establece cuotas de disco para los usuarios. 2. Permisos de operación de gestión de HDFS: ● Visualiza el estado de la interfaz de usuario web. ● Muestra y establece el estado HDFS activo y en espera. ● Entra y sale del HDFS en modo de seguridad. ● Comprueba el sistema de archivos HDFS. 3. Inicia sesión en la página del servicio FTP.	Para obtener más información, consulte **Cambio de la contraseña de un usuario en ejecución de componentes**.

Tipo de usuario	Usuario predeterminado	Contraseña inicial	Descripción	Método de cambio de contraseña
	hbase	Hbase@123	Este usuario es el administrador del sistema HBase y HBase1 a HBase4 y tiene los siguientes permisos: ● Permiso de gestión de clústeres: realiza operaciones de **Enable** y **Disable** en tablas para desencadenar operaciones de MajorCompact y ACL. ● Concede y revoca permisos y cierra el clúster. ● Permiso de gestión de tablas: crea, modifica y elimina tablas. ● Permiso de gestión de datos: lee datos en tablas, familias de columnas y columnas. ● Inicia sesión en la interfaz de usuario web de HMaster. ● Inicia sesión en la página del servicio FTP.	

Tipo de usuario	Usuario predeterminado	Contraseña inicial	Descripción	Método de cambio de contraseña
	mapred	Mapred@123	Este usuario es administrador del sistema de MapReduce y tiene los siguientes permisos: ● Envía, detiene y visualiza las tareas de MapReduce. ● Modifica los parámetros de configuración de Yarn. ● Inicia sesión en la página del servicio FTP. ● Inicia sesión en la interfaz de usuario web de Yarn.	
	zookeeper	ZooKeeper@123	Este usuario es administrador del sistema ZooKeeper y tiene los siguientes permisos: ● Agrega, elimina, modifica y consulta todos los nodos de ZooKeeper. ● Modifica y consulta las cuotas de todos los nodos de ZooKeeper.	
	rangeradmin	Rangeradmin@123	Este usuario tiene los permisos de gestión del sistema Ranger y permisos de usuario: ● Permiso de gestión de la interfaz de usuario web de Ranger ● Permiso de gestión de cada componente que utiliza autenticación Ranger	

Tipo de usuario	Usuario predeterminado	Contraseña inicial	Descripción	Método de cambio de contraseña
	rangeraudito r	Rangerau ditor@12 3	Usuario de auditoría predeterminado del sistema Ranger.	
	hive	Hive@12 3	Este usuario es el administrador del sistema Hive y tiene los siguientes permisos: 1. Permisos de administrador de Hive: ● Crea, elimina y modifica una base de datos. ● Crea, consulta, modifica y elimina una tabla. ● Consulta, inserta y carga datos. 2. Permisos de operación de archivo HDFS: ● Visualiza, modifica y crea archivos. ● Visualiza y crea directorios. ● Visualiza y modifica los grupos a los que pertenecen los archivos. 3. Envía y detiene las tareas de MapReduce. 4. Permiso de gestión de políticas de Ranger	

Tipo de usuario	Usuario predeterminado	Contraseña inicial	Descripción	Método de cambio de contraseña
	hive1	Hive1@123	Este usuario es administrador del sistema Hive1 y tiene los siguientes permisos: 1. Permisos de administrador de Hive1: ● Crea, elimina y modifica una base de datos. ● Crea, consulta, modifica y elimina una tabla. ● Consulta, inserta y carga datos. 2. Permisos de operación de archivo HDFS: ● Visualiza, modifica y crea archivos. ● Visualiza y crea directorios. ● Visualiza y modifica los grupos a los que pertenecen los archivos. 3. Envía y detiene las tareas de MapReduce. 4. Permiso de gestión de políticas de Ranger	

Tipo de usuario	Usuario predeterminado	Contraseña inicial	Descripción	Método de cambio de contraseña
	hive2	Hive2@123	Este usuario es el administrador del sistema Hive2 y tiene los siguientes permisos: 1. Permisos de administrador de Hive2: ● Crea, elimina y modifica una base de datos. ● Crea, consulta, modifica y elimina una tabla. ● Consulta, inserta y carga datos. 2. Permisos de operación de archivo HDFS: ● Visualiza, modifica y crea archivos. ● Visualiza y crea directorios. ● Visualiza y modifica los grupos a los que pertenecen los archivos. 3. Envía y detiene las tareas de MapReduce. 4. Permiso de gestión de políticas de Ranger	

Tipo de usuario	Usuario predeterminado	Contraseña inicial	Descripción	Método de cambio de contraseña
	hive3	Hive3@123	Este usuario es el administrador del sistema Hive3 y tiene los siguientes permisos: 1. Permisos de administrador de Hive3: ● Crea, elimina y modifica una base de datos. ● Crea, consulta, modifica y elimina una tabla. ● Consulta, inserta y carga datos. 2. Permisos de operación de archivo HDFS: ● Visualiza, modifica y crea archivos. ● Visualiza y crea directorios. ● Visualiza y modifica los grupos a los que pertenecen los archivos. 3. Envía y detiene las tareas de MapReduce. 4. Permiso de gestión de políticas de Ranger	

Tipo de usuario	Usuario predeterminado	Contraseña inicial	Descripción	Método de cambio de contraseña
	hive4	Hive4@123	Este usuario es el administrador del sistema Hive4 y tiene los siguientes permisos: 1. Permisos de administrador de Hive4: ● Crea, elimina y modifica una base de datos. ● Crea, consulta, modifica y elimina una tabla. ● Consulta, inserta y carga datos. 2. Permisos de operación de archivo HDFS: ● Visualiza, modifica y crea archivos. ● Visualiza y crea directorios. ● Visualiza y modifica los grupos a los que pertenecen los archivos. 3. Envía y detiene las tareas de MapReduce. 4. Permiso de gestión de políticas de Ranger	

Tipo de usuario	Usuario predeterminado	Contraseña inicial	Descripción	Método de cambio de contraseña
	kafka	Kafka@123	Este usuario es el administrador del sistema Kafka y tiene los siguientes permisos: ● Crea, elimina, produce y consume el tema; modifica la configuración del tema. ● Controla los metadatos del clúster, modifica la configuración, migra la réplica, elige el leader y gestiona la ACL. ● Envía, consulta y elimina la compensación del grupo de consumidores. ● Consulta el token de delegación. ● Consulta y envía el Transaction.	
	storm	Admin@123	Administrador del sistema Storm Permiso del usuario: Envía tareas de Storm.	
	rangerusersync	Generado aleatoriamente por el sistema	Sincroniza usuarios y usuarios internos de grupos de usuarios.	
	rangertagsync	Generado aleatoriamente por el sistema	Usuario interno para sincronizar etiquetas.	
	oms/manager	Generado aleatoriamente por el sistema	Usuario de autenticación de Controller y NodeAgent. El usuario tiene el permiso en el grupo **supergroup**.	

Tipo de usuario	Usuario predeterminado	Contraseña inicial	Descripción	Método de cambio de contraseña
	backup/ manager	Generado aleatoriamente por el sistema	Usuario para ejecutar tareas de copia de respaldo y restauración. El usuario tiene el permiso para los grupos **supergroup**, **wheel** y **ficommon**. Después de configurar la confianza mutua entre sistemas, el usuario tiene el permiso para acceder a los datos en los sistemas HDFS, HBase, Hive y ZooKeeper.	

Tipo de usuario	Usuario predeterminado	Contraseña inicial	Descripción	Método de cambio de contraseña
	hdfs/ hadoop.<*System domain name*>	Generado aleatoriamente por el sistema	Este usuario es usado para iniciar el HDFS y tiene los siguientes permisos: 1. Permisos de operación del sistema de archivos: ● Visualiza, modifica y crea archivos. ● Visualiza y crea directorios. ● Visualiza y modifica los grupos a los que pertenecen los archivos. ● Visualiza y establece cuotas de disco para los usuarios. 2. Permisos de operación de gestión de HDFS: ● Visualiza el estado de la interfaz de usuario web. ● Muestra y establece el estado HDFS activo y en espera. ● Entra y sale del HDFS en modo de seguridad. ● Comprueba el sistema de archivos HDFS. 3. Inicia sesión en la página del servicio FTP.	

Tipo de usuario	Usuario predeterminado	Contraseña inicial	Descripción	Método de cambio de contraseña
	mapred/hadoop.<*System domain name*>	Generado aleatoriamente por el sistema	Este usuario es usado para iniciar el MapReduce y tiene los siguientes permisos: ● Envía, detiene y visualiza las tareas de MapReduce. ● Modifica los parámetros de configuración de Yarn. ● Inicia sesión en la página del servicio FTP. ● Inicia sesión en la interfaz de usuario web de Yarn.	
	mr_zk/hadoop.<*System domain name*>	Generado aleatoriamente por el sistema	Utilizado por MapReduce para acceder a ZooKeeper.	
	hbase/hadoop.<*System domain name*>	Generado aleatoriamente por el sistema	Usuario para la autenticación entre componentes internos durante el inicio del sistema HBase.	
	hbase/zkclient.<*System domain name*>	Generado aleatoriamente por el sistema	Usuario para que HBase realice la autenticación de ZooKeeper en un clúster de modo de seguridad.	
	thrift/hadoop.<*System domain name*>	Generado aleatoriamente por el sistema	Usuario de inicio del sistema de ThriftServer.	

Tipo de usuario	Usuario predeterminado	Contraseña inicial	Descripción	Método de cambio de contraseña
	thrift/<*hostname*>	Generado aleatoriamente por el sistema	Usuario para que el sistema ThriftServer acceda a HBase. Este usuario tiene los permisos de lectura, escritura, ejecución, creación y gestión en todos los NameSpaces y tablas de HBase. <*hostname*> indica el nombre del host donde está instalado el nodo ThriftServer en el clúster.	

Tipo de usuario	Usuario predeterminado	Contraseña inicial	Descripción	Método de cambio de contraseña
	hive/hadoop.<*System domain name*>	Generado aleatoriamente por el sistema	Usuario para la autenticación entre componentes internos durante el inicio del sistema Hive. Los permisos de usuario son los siguientes: 1. Permisos de administrador de Hive: ● Crea, elimina y modifica una base de datos. ● Crea, consulta, modifica y elimina una tabla. ● Consulta, inserta y carga datos. 2. Permisos de operación de archivo HDFS: ● Visualiza, modifica y crea archivos. ● Visualiza y crea directorios. ● Visualiza y modifica los grupos a los que pertenecen los archivos. 3. Envía y detiene las tareas de MapReduce.	

Tipo de usuario	Usuario predeterminado	Contraseña inicial	Descripción	Método de cambio de contraseña
	hive1/hadoop.<*System domain name*>	Generado aleatoriamente por el sistema	Usuario para la autenticación entre componentes internos durante el inicio del sistema Hive1. Los permisos de usuario son los siguientes: 1. Permisos de administrador de Hive1: ● Crea, elimina y modifica una base de datos. ● Crea, consulta, modifica y elimina una tabla. ● Consulta, inserta y carga datos. 2. Permisos de operación de archivo HDFS: ● Visualiza, modifica y crea archivos. ● Visualiza y crea directorios. ● Visualiza y modifica los grupos a los que pertenecen los archivos. 3. Envía y detiene las tareas de MapReduce.	

Tipo de usuario	Usuario predeterminado	Contraseña inicial	Descripción	Método de cambio de contraseña
	hive2/hadoop.<*System domain name*>	Generado aleatoriamente por el sistema	Usuario para la autenticación entre componentes internos durante el inicio del sistema Hive2. Los permisos de usuario son los siguientes: 1. Permisos de administrador de Hive2: ● Crea, elimina y modifica una base de datos. ● Crea, consulta, modifica y elimina una tabla. ● Consulta, inserta y carga datos. 2. Permisos de operación de archivo HDFS: ● Visualiza, modifica y crea archivos. ● Visualiza y crea directorios. ● Visualiza y modifica los grupos a los que pertenecen los archivos. 3. Envía y detiene las tareas de MapReduce.	

Tipo de usuario	Usuario predeterminado	Contraseña inicial	Descripción	Método de cambio de contraseña
	hive3/hadoop.<*System domain name*>	Randomly generated by the system	Usuario para la autenticación entre componentes internos durante el inicio del sistema Hive3. Los permisos de usuario son los siguientes: 1. Permisos de administrador de Hive3: ● Crea, elimina y modifica una base de datos. ● Crea, consulta, modifica y elimina una tabla. ● Consulta, inserta y carga datos. 2. Permisos de operación de archivo HDFS: ● Visualiza, modifica y crea archivos. ● Visualiza y crea directorios. ● Visualiza y modifica los grupos a los que pertenecen los archivos. 3. Envía y detiene las tareas de MapReduce.	

Tipo de usuario	Usuario predeterminado	Contraseña inicial	Descripción	Método de cambio de contraseña
	hive4/hadoop.<*System domain name*>	Generado aleatoriamente por el sistema	Usuario para la autenticación entre componentes internos durante el inicio del sistema Hive4. Los permisos de usuario son los siguientes: 1. Permisos de administrador de Hive4: ● Crea, elimina y modifica una base de datos. ● Crea, consulta, modifica y elimina una tabla. ● Consulta, inserta y carga datos. 2. Permisos de operación de archivo HDFS: ● Visualiza, modifica y crea archivos. ● Visualiza y crea directorios. ● Visualiza y modifica los grupos a los que pertenecen los archivos. 3. Envía y detiene las tareas de MapReduce.	
	loader/hadoop.<*System domain name*>	Generado aleatoriamente por el sistema	Usuario para inicio de sistema de Loader y autenticación de Kerberos	

Tipo de usuario	Usuario predeterminado	Contraseña inicial	Descripción	Método de cambio de contraseña
	HTTP/<*hostname*>	Generado aleatoriamente por el sistema	Se utiliza para conectarse a la interfaz HTTP de cada componente. <*hostname*> indica el nombre de host de un nodo en el clúster.	
	hue	Generado aleatoriamente por el sistema	Usuario para inicio del sistema de Hue, autenticación de Kerberos y acceso a HDFS y Hive	
	flume	Generado aleatoriamente por el sistema	Usuario para el inicio del sistema de Flume y acceso a HDFS y Kafka. El usuario tiene permiso de lectura y escritura del directorio HDFS **/flume**.	
	flume_server	Generado aleatoriamente por el sistema	Usuario para el inicio del sistema de Flume y acceso a HDFS y Kafka. El usuario tiene permiso de lectura y escritura del directorio HDFS **/flume**.	
	spark2x/hadoop.<*System domain name*>	Generado aleatoriamente por el sistema	Este usuario es el administrador del sistema Spark2x y tiene los siguientes permisos de usuario: 1. Inicia el servicio Spark2x. 2. Envía tareas de Spark2x.	
	spark_zk/hadoop.<*System domain name*>	Generado aleatoriamente por el sistema	Utilizado por Spark2x para acceder a ZooKeeper.	

Tipo de usuario	Usuario predeterminado	Contraseña inicial	Descripción	Método de cambio de contraseña
	spark2x1/hadoop.<*System domain name*>	Generado aleatoriamente por el sistema	Este usuario es administrador de sistema Spark2x1 y tiene los siguientes permisos de usuario: 1. Inicia el servicio Spark2x1. 2. Envía tareas de Spark2x.	
	spark2x2/hadoop.<*System domain name*>	Generado aleatoriamente por el sistema	Este usuario es un administrador del sistema Spark2x2 y tiene los siguientes permisos de usuario: 1. Inicia el servicio Spark2x2. 2. Envía tareas de Spark2x.	
	spark2x3/hadoop.<*System domain name*>	Generado aleatoriamente por el sistema	Este usuario es un administrador del sistema Spark2x3 y tiene los siguientes permisos de usuario: 1. Inicia el servicio Spark2x3. 2. Envía tareas de Spark2x.	
	spark2x4/hadoop.<*System domain name*>	Generado aleatoriamente por el sistema	Este usuario es un administrador del sistema Spark2x4 y tiene los siguientes permisos de usuario: 1. Inicia el servicio Spark2x4. 2. Envía tareas de Spark2x.	
	zookeeper/hadoop.<*System domain name*>	Generado aleatoriamente por el sistema	Usuario de inicio del sistema de ZooKeeper.	

Tipo de usuario	Usuario predeterminado	Contraseña inicial	Descripción	Método de cambio de contraseña
	zkcli/hadoop.<*System domain name*>	Generado aleatoriamente por el sistema	Usuario de inicio de sesión del servidor ZooKeeper.	
	oozie	Generado aleatoriamente por el sistema	Usuario para el inicio del sistema de Oozie y la autenticación de Kerberos.	
	kafka/hadoop.<*System domain name*>	Generado aleatoriamente por el sistema	Utilizado para la autenticación de seguridad de Kafka.	
	storm/hadoop.<*System domain name*>	Generado aleatoriamente por el sistema	Usuario de inicio del sistema de Storm.	
	storm_zk/hadoop.<*System domain name*>	Generado aleatoriamente por el sistema	Se utiliza para el proceso Worker para acceder a ZooKeeper.	
	flink/hadoop.<*System domain name*>	Generado aleatoriamente por el sistema	Usuario interno del servicio Flink.	
	check_ker_M	Generado aleatoriamente por el sistema	Usuario que realiza una prueba interna del sistema acerca de si el servicio Kerberos es normal.	
	clickhouse/hadoop.<*System domain name*>	Generado aleatoriamente por el sistema	Se utiliza para la autenticación de seguridad de ClickHouse. Este usuario es un usuario interno y solo se puede utilizar en el clúster.	
	default	Ninguna	Usuario interno de ClickHouse , que es un usuario de administrador que solo se puede utilizar en modo no seguro.	

Tipo de usuario	Usuario predeterminado	Contraseña inicial	Descripción	Método de cambio de contraseña
	rangeradmin / hadoop.<*System domain name*>	Generado aleatoriamente por el sistema	Usuario de inicio del sistema Ranger, que se utiliza para la autenticación entre componentes internos.	
	tez	Generado aleatoriamente por el sistema	Usuario para inicio del sistema de TezUI, autenticación de Kerberos y acceso a Yarn	
	K/M	Generado aleatoriamente por el sistema	Usuario funcional interno de Kerberos. Este usuario no se puede eliminar y su contraseña no se puede cambiar. Esta cuenta interna solo se puede utilizar en los nodos donde está instalado el servicio Kerberos.	Ninguna
	kadmin/ changepw	Generado aleatoriamente por el sistema		
	kadmin/ history	Generado aleatoriamente por el sistema		
	krbtgt<*System domain name*>	Generado aleatoriamente por el sistema		
Usuario de LDAP	admin	Ninguna	Administrador de FusionInsight Manager. El grupo principal es **compcommon**, que no tiene el permiso de grupo pero tiene el permiso del rol **Manager_administrator**.	El usuario LDAP no puede iniciar sesión en el sistema y la contraseña no se puede cambiar.
	backup		El grupo primario es **compcommon**.	
	backup/ manager		El grupo primario es **compcommon**.	
	oms		El grupo primario es **compcommon**.	

Tipo de usuario	Usuario predeterminado	Contraseña inicial	Descripción	Método de cambio de contraseña
	oms/ manager		El grupo primario es **compcommon**.	
	clientregister		El grupo primario es **compcommon**.	
	zookeeper		El grupo primario es **hadoop**.	
	zookeeper/ hadoop.<*System domain name*>		El grupo primario es **hadoop**.	
	zkcli		El grupo primario es **hadoop**.	
	zkcli/ hadoop.<*System domain name*>		El grupo primario es **hadoop**.	
	flume		El grupo primario es **hadoop**.	
	flume_server		El grupo primario es **hadoop**.	
	hdfs		El grupo primario es **hadoop**.	
	hdfs/ hadoop.<*System domain name*>		El grupo primario es **hadoop**.	
	mapred		El grupo primario es **hadoop**.	
	mapred/ hadoop.<*System domain name*>		El grupo primario es **hadoop**.	
	mr_zk		El grupo primario es **hadoop**.	
	mr_zk/ hadoop.<*System domain name*>		El grupo primario es **hadoop**.	

Tipo de usuario	Usuario predeterminado	Contraseña inicial	Descripción	Método de cambio de contraseña
	hue		El grupo primario es **supergroup**.	
	hive		El grupo primario es **hive**.	
	hive/hadoop.<*System domain name*>		El grupo primario es **hive**.	
	hive1		El grupo primario es **hive1**.	
	hive1/hadoop.<*System domain name*>		El grupo primario es **hive1**.	
	hive2		El grupo primario es **hive2**.	
	hive2/hadoop.<*System domain name*>		El grupo primario es **hive2**.	
	hive3		El grupo primario es **hive3**.	
	hive3/hadoop.<*System domain name*>		El grupo primario es **hive3**.	
	hive4		El grupo primario es **hive4**.	
	hive4/hadoop.<*System domain name*>		El grupo primario es **hive4**.	
	hbase		El grupo primario es **hadoop**.	
	hbase/hadoop.<*System domain name*>		El grupo primario es **hadoop**.	

Tipo de usuario	Usuario predeterminado	Contraseña inicial	Descripción	Método de cambio de contraseña
	thrift		El grupo primario es **hadoop**.	
	thrift/hadoop.<*System domain name*>		El grupo primario es **hadoop**.	
	oozie		El grupo primario es **hadoop**.	
	hbase/zkclient.<*System domain name*>		El grupo primario es **hadoop**.	
	loader		El grupo primario es **hadoop**.	
	loader/hadoop.<*System domain name*>		El grupo primario es **hadoop**.	
	spark2x		El grupo primario es **hadoop**.	
	spark2x/hadoop.<*System domain name*>		El grupo primario es **hadoop**.	
	spark_zk		El grupo primario es **hadoop**.	
	spark2x1		El grupo primario es **hadoop**.	
	spark2x1/hadoop.<*System domain name*>		El grupo primario es **hadoop**.	
	spark2x2		El grupo primario es **hadoop**.	
	spark2x2/hadoop.<*System domain name*<		El grupo primario es **hadoop**.	

Tipo de usuario	Usuario predeterminado	Contraseña inicial	Descripción	Método de cambio de contraseña
	spark2x3		El grupo primario es **hadoop**.	
	spark2x3/hadoop.<*System domain name*>		El grupo primario es **hadoop**.	
	spark2x4		El grupo primario es **hadoop**.	
	spark2x4/hadoop.<*System domain name*>		El grupo primario es **hadoop**.	
	kafka		El grupo primario es **kafkaadmin**.	
	kafka/hadoop.<*System domain name*>		El grupo primario es **kafkaadmin**.	
	storm		El grupo primario es **stormadmin**.	
	storm/hadoop.<*System domain name*>		El grupo primario es **stormadmin**.	
	storm_zk		El grupo primario es **storm**.	
	storm_zk/hadoop.<*System domain name*>		El grupo primario es **storm**.	
	kms/hadoop		El grupo primario es **kmsadmin**.	
	knox		El grupo primario es **compcommon**.	
	executor		El grupo primario es **compcommon**.	
	rangeradmin		El grupo primario es **supergroup**.	

Tipo de usuario	Usuario predeterminado	Contraseña inicial	Descripción	Método de cambio de contraseña
	rangeradmin / hadoop.<*System domain name*>		El grupo primario es **supergroup**.	
	rangerusersync		El grupo primario es **supergroup**.	
	rangertagsync		El grupo primario es **supergroup**.	
	rangerauditor		El grupo primario es **compcommon**.	

NOTA

Inicie sesión en FusionInsight Manager, seleccione **System** > **Permission** > **Domain and Mutual Trust** y compruebe el valor de **Local Domain**. En la tabla anterior, todas las letras del nombre de dominio del sistema contenidas en el nombre de usuario del usuario interno del sistema son letras minúsculas.

Por ejemplo, si **Local Domain** se establece en **9427068F-6EFA-4833-B43E-60CB641E5B6C.COM**, el nombre de usuario del usuario de inicio HDFS predeterminado es **hdfs/hadoop.9427068f-6efa-4833-b43e-60cb641e5b6c.com**.

Usuarios de la base de datos

Los usuarios de la base de datos del sistema incluyen usuarios de la base de datos de OMS y usuarios de la base de datos de DBService.

Tipo de base de datos	Usuario predeterminado	Contraseña inicial	Descripción	Método de cambio de contraseña
Base de datos de OMS	ommdba	dbChangeMe@123456	Administrador de base de datos de OMS que realiza operaciones de mantenimiento, como crear, iniciar y detener.	Para obtener más información, consulte **Cambio de la contraseña del administrador de la base de datos de OMS**.
	omm	ChangeMe@123456	Usuario para acceder a los datos de la base de datos de OMS	Para obtener más información, consulte **Cambio de la contraseña del usuario de acceso a datos de la base de datos de OMS**.

Tipo de base de datos	Usuario predeterminado	Contraseña inicial	Descripción	Método de cambio de contraseña
Base de datos de DBService	omm	dbserverAdmin@123	Administrador de la base de datos de GaussDB en el componente de DBService	• Para versiones anteriores a MRS 3.1.2, consulte **Cambio de la contraseña de un usuario de base de datos de componentes**. • La contraseña inicial no se puede cambiar en MRS 3.1.2 o posterior.
	compdbuser	Contraseña aleatoria	MRS 3.1.2 o posterior: Administrador de la base de datos de GaussDB en el componente de DBService. Se utiliza en escenarios O&M de servicio. Si la contraseña de esta cuenta ha caducado, debe restablecer la contraseña en su primer inicio de sesión.	Para obtener más información, consulte **Cambio de la contraseña para usuario compdbuser de la base de datos de DBService**.

Tipo de base de datos	Usuario predeterminado	Contraseña inicial	Descripción	Método de cambio de contraseña
	hive	• Versiones anteriores a MRS 3.1.2: HiveUser@ • MRS 3.1.2 o posterior: contrase	Usuario para que Hive se conecte al **hivemeta** de base de datos de DBService.	• Para versiones anteriores a MRS 3.1.2, consulte **Cambio de la contraseña de un usuario de base de datos de componentes**. • Para MRS 3.1.2 o posterior, consulte **Restablecimiento de la contraseña de usuario de la base de datos de componentes**.

Tipo de base de datos	Usuario predeterminado	Contraseña inicial	Descripción	Método de cambio de contraseña
		ña alea toria		

Tipo de base de datos	Usuario predeterminado	Contraseña inicial	Descripción	Método de cambio de contraseña
	hive1	• Versiones anteriores a MRS 3.1.2: HiveUser@ • MRS 3.1.2 o posterior: contrase	Usuario para que Hive1 se conecte al **hivemeta1** de base de datos de DBService.	

Tipo de base de datos	Usuario predeterminado	Contraseña inicial	Descripción	Método de cambio de contraseña
		ña aleatoria		

Tipo de base de datos	Usuario predeterminado	Contraseña inicial	Descripción	Método de cambio de contraseña
	hive2	• Versiones anteriores a MRS 3.1.2: HiveUser@ • MRS 3.1.2 o posterior: contrase	Usuario para que Hive2 se conecte al **hivemeta2** de base de datos de DBService.	

Tipo de base de datos	Usuario predeterminado	Contraseña inicial	Descripción	Método de cambio de contraseña
		ña aleatoria		

Tipo de base de datos	Usuario predeterminado	Contraseña inicial	Descripción	Método de cambio de contraseña
	hive3	• Versiones anteriores a MRS 3.1.2: HiveUser@ • MRS 3.1.2 o posterior: contrase	Usuario para que Hive3 se conecte al **hivemeta3** de base de datos de DBService.	

Tipo de base de datos	Usuario predeterminado	Contraseña inicial	Descripción	Método de cambio de contraseña
		ña aleatoria		

Tipo de base de datos	Usuario predeterminado	Contraseña inicial	Descripción	Método de cambio de contraseña
	hive4	• Versiones anteriores a MRS 3.1.2: HiveUser@ • MRS 3.1.2 o posterior: contrase	Usuario para que Hive4 se conecte al **hivemeta4** de base de datos de DBService.	

Tipo de base de datos	Usuario predeterminado	Contraseña inicial	Descripción	Método de cambio de contraseña
		ña aleatoria		

Tipo de base de datos	Usuario predeterminado	Contraseña inicial	Descripción	Método de cambio de contraseña
	hive*NN*	• Versiones anteriores a MRS 3.1.2: HiveUser@ • MRS 3.1.2 o posterior: contrase	Usuario para que **Hive-*N*** se conecte a la base de datos de DBService **hive*N*meta** cuando se instalan varios servicios. Por ejemplo, el usuario para que **Hive-1** se conecte a la base de datos de DBService de **hive1meta** es **hive11**.	

Tipo de base de datos	Usuario predeterminado	Contraseña inicial	Descripción	Método de cambio de contraseña
		ña alea toria		

Tipo de base de datos	Usuario predeterminado	Contraseña inicial	Descripción	Método de cambio de contraseña
	hue	• Versiones anteriores a MRS 3.1.2: HueUser@123 • MRS 3.1.2 o posterior: cont	Usuario para que Hue se conecte al **hue** de base de datos de DBService.	

Tipo de base de datos	Usuario predeterminado	Contraseña inicial	Descripción	Método de cambio de contraseña
		raseñaaleatoria		

Tipo de base de datos	Usuario predeterminado	Contraseña inicial	Descripción	Método de cambio de contraseña
	sqoop	● Versiones anteriores a MRS 3.1.2: SqoopUser@ ● MRS 3.1.2 o posterior: contra	Usuario para que el cargador se conecte al **sqoop** de base de datos de DBService.	

Tipo de base de datos	Usuario predeterminado	Contraseña inicial	Descripción	Método de cambio de contraseña
		señalea toria		

Tipo de base de datos	Usuario predeterminado	Contraseña inicial	Descripción	Método de cambio de contraseña
	sqoop*N*	• Versiones anteriores a MRS 3.1.2: SqoopUser@ • MRS 3.1.2 o posterior: contra	Usuario para que **Loader-***N* se conecte a la base de datos de DBService **sqoop***N* cuando se instalan varios servicios. Por ejemplo, el usuario para que **Loader-1** se conecte a la base de datos de DBService **sqoop1** es **sqoop1**.	

Tipo de base de datos	Usuario predeterminado	Contraseña inicial	Descripción	Método de cambio de contraseña
		señalea toria		

Tipo de base de datos	Usuario predeterminado	Contraseña inicial	Descripción	Método de cambio de contraseña
	oozie	• Versiones anteriores a MRS 3.1.2: OozieUser@ • MRS 3.1.2 o posterior: contras	Usuario para que Oozie se conecte al **oozie** de base de datos de DBService.	

Tipo de base de datos	Usuario predeterminado	Contraseña inicial	Descripción	Método de cambio de contraseña
		eñaaleatoria		

Tipo de base de datos	Usuario predeterminado	Contraseña inicial	Descripción	Método de cambio de contraseña
	oozie*N*	● Versiones anteriores a MRS 3.1.2: OozieUser@ ● MRS 3.1.2 o posterior: contras	Usuario para que **Oozie-***N* se conecte a la base de datos de DBService **oozie***N* cuando se instalan varios servicios. Por ejemplo, el usuario para que **Oozie-1** se conecte a la base de datos de DBService **oozie1** es **oozie1**.	

Tipo de base de datos	Usuario predeterminado	Contraseña inicial	Descripción	Método de cambio de contraseña
		eñaaleatoria		

Tipo de base de datos	Usuario predeterminado	Contraseña inicial	Descripción	Método de cambio de contraseña
	rangeradmin	• Versiones anteriores a MRS 3.1.2: OozieUser@ • MRS 3.1.2 o posterior: contras	Usuario para que Ranger se conecte a la base de datos de DBService.	

Tipo de base de datos	Usuario predeterminado	Contraseña inicial	Descripción	Método de cambio de contraseña
		eñaaleatoria		
	kafkaui	Contraseña aleatoria	Usuario de Kafka UI para conectarse a la base de datos de DBService. Este usuario solo existe en MRS 3.1.2 o posterior.	
	flink	Contraseña aleatoria	Usuario para que Flink se conecte a la base de datos de DBService. Este usuario solo existe en MRS 3.1.2 o posterior.	

7.11.1.6 Información de permisos predeterminados

Rol

Rol predeterminado	Descripción
Manager_administrator	Administrador de Manager que tiene todos los permisos para Manager. Los administradores del Manager pueden crear tenants de primer nivel, crear y modificar grupos de usuarios y especificar permisos de usuario.
Manager_operator	Operador de Manager que tiene todos los permisos en las páginas de pestañas **Homepage**, **Cluster**, **Hosts** y **O&M**.
Manager_auditor	Auditor de Manager que tiene todos los permisos en la página de pestaña **Audit**. Los auditores del Manager pueden ver y gestionar los registros de auditoría del sistema del Manager.

Rol predeterminado	Descripción
Manager_viewer	Visor de Manager que tiene permiso para ver información sobre **Homepage**, **Cluster**, **Hosts**, **Alarm**, **Events** y **System > Permission**.
Manager_tenant	Administrador de tenant de Manager. Este rol puede crear y gestionar subtenants para los tenants que no son hojas a los que pertenece el usuario actual. Tiene el permiso para ver alarmas y eventos en **O&M > Alarm**.
System_administrator	Administrador del sistema, este rol tiene derechos de administrador del sistema de administrador y todos los derechos de administrador de servicios.
default	Este rol es el rol predeterminado creado para el tenant **default**. Tiene los permisos de gestión en el componente Yarn y la cola predeterminada. El rol predeterminado del tenant predeterminado que no es el primer clúster que se instala es **c**<*cluster ID*>**_default**.
Manager_administrator_180	Grupo de administradores del sistema del FusionInsight Manager. Grupo de usuarios interno del sistema, que se utiliza solo entre componentes.
Manager_auditor_181	Grupo de auditor de sistema de FusionInsight Manager. Grupo de usuarios interno del sistema, que se utiliza solo entre componentes.
Manager_operator_182	Grupo de operadores del sistema de FusionInsight Manager. Grupo de usuarios interno del sistema, que se utiliza solo entre componentes.
Manager_viewer_183	Grupo de visor del sistema FusionInsight Manager. Grupo de usuarios interno del sistema, que se utiliza solo entre componentes.
System_administrator_186	Grupo de administradores del sistema. Grupo de usuarios interno del sistema, que se utiliza solo entre componentes.
Manager_tenant_187	Grupo de usuarios del sistema de tenant. Grupo de usuarios interno del sistema, que se utiliza solo entre componentes.
default_1000	Este grupo se crea para tenant. Grupo de usuarios interno del sistema, que se utiliza solo entre componentes.

Grupo de usuario

Tipo	Grupo de usuarios predeterminado	Descripción
Grupo de usuarios de sistema operativo	hadoop	Los usuarios agregados a este grupo tienen permiso para enviar todas las tareas de cola de Yarn.
	hadoopmanager	Los usuarios agregados a este grupo de usuarios pueden tener los derechos de administrador de O&M de HDFS y Yarn. El administrador de O&M de HDFS puede acceder al WebUI de NameNode y realizar el cambio de activo a espera manualmente. El administrador de O&M de Yarn puede acceder a la WebUI de ResourceManager, operar NodeManager nodos, actualizar colas y establecer etiquetas de nodo, pero no puede enviar tareas.
	hetuadmin	Grupo de administradores de HetuEngine. Los usuarios de este grupo tienen permiso para realizar operaciones en HSConsole.
	hive	Grupo de usuarios común. Los usuarios de Hive deben pertenecer a este grupo de usuarios.
	iotdbgroup	Los usuarios agregados a este grupo de usuarios tienen los derechos de administrador del componente IoTDB.
	kafka	Grupo de usuarios comunes de Kafka. Un usuario de este grupo solo puede acceder a un topic cuando un usuario del grupo kafkaadmin otorga el permiso de lectura y escritura del topic al usuario.
	kafkaadmin	Grupo de administradores de Kafka. Los usuarios de este grupo tienen los derechos para crear, eliminar, autorizar, leer y escribir todos los topics.
	kafkasuperuser	Grupo de usuarios de lectura/escritura de topic de Kafka. Los usuarios agregados a este grupo tienen los permisos de lectura y escritura en todos los topics.
	cdladmin	Grupo de administradores de CDL. Solo los usuarios de este grupo pueden acceder a las API de CDL.
	cdl	Grupo de usuarios comunes de CDL. Los usuarios de este grupo pueden crear y consultar trabajos de CDL.
	storm	Los usuarios que se agregan al grupo de usuarios de storm pueden enviar topologías y gestionar sus propias topologías.
	stormadmin	Los usuarios que se agregan al grupo de usuarios de stormadmin pueden tener los derechos de administrador de storm y pueden enviar topologías y gestionar todas las topologías.
	supergroup	Los usuarios agregados a este grupo de usuarios tienen los derechos de administrador de HBase, HDFS y Yarn y pueden usar Hive.

Tipo	Grupo de usuarios predeterminado	Descripción
	yarnviewgroup	Indica el grupo de usuarios de sólo lectura de la tarea de Yarn. Los usuarios de este grupo de usuarios pueden tener el permiso de vista en las tareas de Yarn y MapReduce.
	check_sec_ldap	Realice una prueba interna en el LDAP activo para ver si funciona correctamente. Este grupo de usuarios se genera aleatoriamente en una prueba y se elimina automáticamente una vez completada la prueba. Grupo de usuarios interno del sistema, que se utiliza solo entre componentes.
	compcommon	Grupo interno del sistema para acceder a los recursos del sistema del clúster. Todos los usuarios del sistema y los usuarios en ejecución del sistema se agregan a este grupo de usuarios de forma predeterminada.
Grupo de usuarios de sistema operativo	wheel	Grupo principal del usuario interno de ejecución de FusionInsight omm.
	ficommon	Grupo común del sistema que corresponde a **compcommon** para acceder a los archivos de recursos comunes del clúster almacenados en el sistema operativo.

NOTA

Si el clúster actual no es el clúster que se instala por primera vez en FusionInsight Manager, el nombre de grupo de usuarios predeterminado de todos los componentes excepto el Manager del clúster es **c**<*cluster ID*>_ *default user group name*, por ejemplo, **c2_hadoop**.

Usuario

Para obtener más información, consulte **Lista de cuentas de usuario**.

Parámetros de seguridad de usuario relacionados con el servicio

- **HDFS**

  El parámetro **dfs.permissions.superusergroup** especifica el grupo de administradores con el permiso más alto en el HDFS. El valor predeterminado es **supergroup**.

- **Spark2x**

  El parámetro **spark.admin.acls** especifica la lista de administradores de Spark2x. Los miembros de la lista están autorizados a gestionar todas las tareas de Spark. Los usuarios no agregados en la lista no pueden gestionar todas las tareas de Spark. El valor predeterminado es **admin**.

7.11.1.7 Funciones de seguridad de FusionInsight Manager

Puede consultar y establecer datos de derechos de usuario a través de los siguientes módulos de FusionInsight Manager:

- Gestión de usuarios: Los usuarios pueden ser agregados, eliminados, modificados, consultados, enlazados a grupos de usuarios y asignados con roles.

  Para obtener más información, consulte **Gestión de usuarios**.
- Gestión de grupos de usuarios: los grupos de usuarios se pueden agregar, eliminar, modificar, consultar y enlazar a roles.

  Para obtener más información, consulte **Gestión de grupos de usuarios**.
- Gestión de roles: los roles se pueden agregar, eliminar, modificar, consultar y asignar con los derechos de acceso a recursos de uno o varios componentes.

  Para obtener más información, consulte **Gestión de roles**.
- Gestión de tenant: Tenants pueden agregarse, eliminarse, modificarse, consultarse y enlazarse a recursos de componentes. FusionInsight genera un rol para cada tenant para facilitar la gestión. Si a un tenant se le asignan los derechos de algunos recursos, su rol correspondiente también tiene estos derechos.

  Para obtener más información, consulte **Recursos para tenant**.

7.11.2 Gestión de cuentas

7.11.2.1 Ajustes de seguridad de la cuenta

7.11.2.1.1 Desbloqueo de usuarios LDAP y cuentas de gestión

Escenario

Si el usuario LDAP **cn=pg_search_dn,ou=Users,dc=hadoop,dc=com** y las cuentas de gestión LDAP **cn=krbkdc,ou=Users,dc=hadoop,dc=com** y **cn=krbadmin,ou=Users,dc=hadoop,dc=com** están bloqueadas, el administrador debe desbloquear estas cuentas.

NOTA

Si introduce una contraseña incorrecta para el usuario LDAP o la cuenta de gestión durante cinco veces consecutivas, se bloqueará el usuario LDAP o la cuenta de gestión. La cuenta se desbloquea automáticamente después de 5 minutos.

Procedimiento

Paso 1 Inicie sesión en el nodo de gestión activo como usuario **omm**.

Paso 2 Ejecute el siguiente comando para ir al directorio relacionado:

cd ${BIGDATA_HOME}/om-server/om/ldapserver/ldapserver/local/script

Paso 3 Ejecute el siguiente comando para desbloquear el usuario LDAP o la cuenta de gestión:

./ldapserver_unlockUsers.sh *USER_NAME*

En el comando, *USER_NAME* indica el nombre del usuario que se va a desbloquear.

Por ejemplo, para desbloquear la gestión de LDAP **account cn=krbkdc,ou=Users,dc=hadoop,dc=com**, ejecute el siguiente comando:

./ldapserver_unlockUsers.sh krbkdc

Después de ejecutar el script, introduzca la contraseña del usuario **krbkdc** después de **ROOT_DN_PASSWORD**. Si se muestra la siguiente información, la cuenta se desbloquea correctamente.

```
Unlock user krbkdc successfully.
```

----Fin

7.11.2.1.2 Desbloquear usuarios internos del sistema

Escenario

Si el servicio es anormal, el usuario interno del sistema puede estar bloqueado. Desbloquee al usuario inmediatamente o el clúster no se puede ejecutar correctamente. Para ver la lista de usuarios internos del sistema, consulte **Lista de cuentas de usuario** de. El usuario interno del sistema no se puede desbloquear con FusionInsight Manager.

Prerrequisitos

Obtenga la contraseña predeterminada del administrador LDAP **cn=root,dc=hadoop,dc=com** haciendo referencia a **Lista de cuentas de usuario**.

Procedimiento

Paso 1 Utilice el siguiente método para confirmar si el nombre de usuario interno del sistema está bloqueado:

1. Método de obtención de número de puerto de OLdap:
   a. Inicie sesión en FusionInsight Manager y seleccione **System** > **OMS** > **oldap** > **Modify Configuration**.
   b. El valor del parámetro **LDAP Listening Port** es **oldap port**.
2. Método de obtención de nombres de dominio:
   a. Inicie sesión en FusionInsight Manager, seleccione **System** > **Permission** > **Domain and Mutual Trust**.
   b. El valor del parámetro **Local Domain** es el nombre de dominio.

      Por ejemplo, el nombre de dominio del sistema actual es **9427068F-6EFA-4833-B43E-60CB641E5B6C.COM**.
3. Ejecute el siguiente comando en cada nodo del clúster como usuario **omm** para consultar el número de errores de autenticación de contraseña:

   ldapsearch -H ldaps://*OMS Floating IP Address***:***OLdap port* **-LLL -x -D cn=root,dc=hadoop,dc=com -b krbPrincipalName=***Internal system username@Domain name***,cn=***Domain name***,cn=krbcontainer,dc=hadoop,dc=com -w** *Password of LDAP administrator* **-e ppolicy | grep krbLoginFailedCount**

   Por ejemplo, ejecute el siguiente comando para comprobar el número de errores de autenticación de contraseña para usuario **oms/manager**:

   ldapsearch -H ldaps://10.5.146.118:21750 -LLL -x -D cn=root,dc=hadoop,dc=com -b krbPrincipalName=oms/manager@9427068F-6EFA-4833-

B43E-60CB641E5B6C.COM,cn=9427068F-6EFA-4833-B43E-60CB641E5B6C.COM,cn=krbcontainer,dc=hadoop,dc=com -w *Password of user cn=root,dc=hadoop,dc=com* **-e ppolicy | grep krbLoginFailedCount**

```
krbLoginFailedCount: 5
```

4. Inicie sesión en FusionInsight Manager, seleccione **System** > **Permission** > **Security Policy** > **Password Policy**.
5. Compruebe el valor del parámetro **Password Retries**. Si el valor es menor o igual que el valor de **krbLoginFailedCount**, el usuario está bloqueado.

   NOTA

   También puede comprobar si los usuarios internos están bloqueados mediante la visualización de los registros de operaciones.

Paso 2 Inicie sesión en el nodo de gestión activo como usuario **omm** y ejecute el siguiente comando para desbloquear el usuario:

sh ${BIGDATA_HOME}/om-server/om/share/om/acs/config/unlockuser.sh --userName *Internal system username*

Ejemplo: **sh ${BIGDATA_HOME}/om-server/om/share/om/acs/config/unlockuser.sh --userName oms/manager**

----Fin

7.11.2.1.3 Activación y desactivación de la verificación de permisos en componentes de clúster

Escenario

HDFS y ZooKeeper verifican el permiso de los usuarios que intentan acceder a los servicios en clústeres normales y de seguridad de forma predeterminada. Los usuarios sin permiso relacionado no pueden acceder a los recursos de HDFS y ZooKeeper. Cuando el clúster se despliega en modo normal, HBase y YARN no verifican el permiso de los usuarios que intentan acceder a los servicios de forma predeterminada. Todos los usuarios pueden acceder a recursos en HBase y YARN.

Según los requisitos de servicio reales, los administradores pueden habilitar la verificación de permisos en HBase y YARN o deshabilitar la verificación de permisos en HDFS y ZooKeeper en clústeres normales.

Impacto en el sistema

Después de las operaciones de habilitación y deshabilitación, la configuración del servicio caducará. Es necesario reiniciar el servicio correspondiente para que la configuración surta efecto.

Habilitación de la verificación de permisos en HBase

Paso 1 Inicie sesión en FusionInsight Manager.

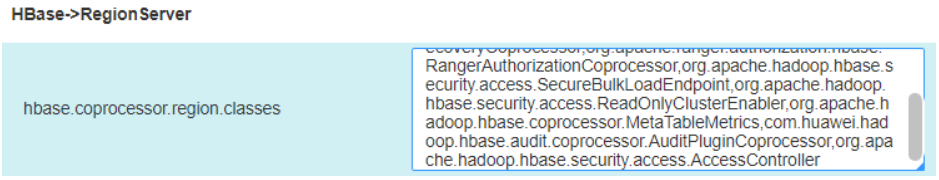
Paso 2 Haga clic en **Cluster**, haga clic en el nombre del clúster deseado, elija **Services** > **Ranger**, y haga clic en **Configurations**.

Paso 3 Haga clic en **All Configurations**.

Paso 4 Busque los parámetros **hbase.coprocessor.region.classes**, **hbase.coprocessor.master.classes** y **hbase.coprocessor.regionserver.classes**.

Agregue el parámetro de coprocesador **org.apache.hadoop.hbase.security.access.AccessController** al final de los valores de los parámetros anteriores, y use un (,) de coma para separar los valores de los coprocesadores originales. El parámetro **hbase.coprocessor.region.classes** se utiliza como ejemplo.

Figura 7-61 hbase.coprocessor.region.classes



Paso 5 Haga clic en **Save**, haga clic en **OK** y espere a que se muestre el mensaje "Operation successful".

----Fin

Desactivación de la verificación de permisos en HBase

NOTA

Después de deshabilitar la verificación de permisos de HBase, se conservarán los datos de permisos existentes. Si desea eliminar información de permisos, deshabilitar la verificación de permisos, introduzca HBase shell y elimine la tabla **hbase:acl**.

Paso 1 Inicie sesión en FusionInsight Manager.

Paso 2 Haga clic en **Cluster**, haga clic en el nombre del clúster deseado, elija **Services** > **HBase**, y haga clic en **Configurations**.

Paso 3 Haga clic en **All Configurations**.

Paso 4 Busque los parámetros **hbase.coprocessor.region.classes**, **hbase.coprocessor.master.classes** y **hbase.coprocessor.regionserver.classes**.

Elimine el parámetro del coprocesador **org.apache.hadoop.hbase.security.access.AccessController**.

Paso 5 Haga clic en **Save**, haga clic en **OK** y espere a que se muestre el mensaje "Operation successful".

----Fin

Desactivación de la verificación de permisos en HDFS

Paso 1 Inicie sesión en FusionInsight Manager.

Paso 2 Haga clic en **Cluster**, haga clic en el nombre del clúster deseado, elija **Services** > **HDFS**, y haga clic en **Configurations**.

Paso 3 Haga clic en **All Configurations**.

Paso 4 Busque los parámetros **dfs.namenode.acls.enabled** y **dfs.permissions.enabled**.

- **dfs.namenode.acls.enabled** indica si se debe habilitar HDFS ACL. El valor predeterminado es **true**, que indica que la ACL está habilitada. Cambie el valor a **false**.
- **dfs.permissions.enabled** indica si se debe habilitar la comprobación de permisos para HDFS. El valor predeterminado es **true**, que indica que la comprobación de permisos está activada. Cambie el valor a **false**. Después de la modificación, el propietario, el grupo de propietarios y el permiso de los directorios y archivos en HDFS permanecen sin cambios.

Paso 5 Haga clic en **Save**, haga clic en **OK** y espere a que se muestre el mensaje "Operation successful".

----Fin

Activación de la verificación de permisos en YARN

Paso 1 Inicie sesión en FusionInsight Manager.

Paso 2 Haga clic en **Cluster**, haga clic en el nombre del clúster deseado, elija **Services** > **Yarn**, y haga clic en **Configurations**.

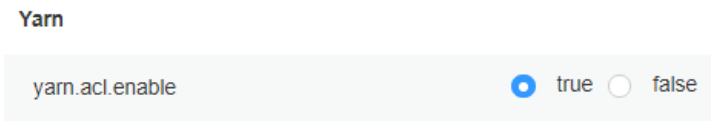
Paso 3 Haga clic en **All Configurations**.

Paso 4 Busque parámetro **yarn.acl.enable**.

yarn.acl.enable indica si se debe habilitar la comprobación de permisos para YARN.

- En clústeres normales, el valor se establece en **false** de forma predeterminada para deshabilitar la comprobación de permisos. Para habilitar la comprobación de permisos, cambie el valor a **true**.
- En los clústeres de seguridad, el valor se establece en **true** de forma predeterminada para habilitar la autenticación.

Figura 7-62 Establecer el parámetro yarn.acl.enable



Paso 5 Haga clic en **Save**, haga clic en **OK** y espere a que se muestre el mensaje "Operation successful".

----Fin

Deshabilitar la verificación de permisos en ZooKeeper

Paso 1 Inicie sesión en FusionInsight Manager.

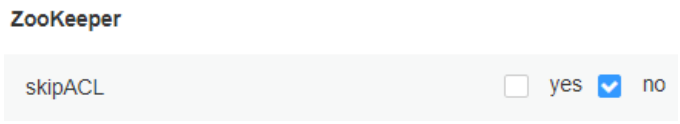
Paso 2 Haga clic en **Cluster**, haga clic en el nombre del clúster deseado, elija **Services** > **ZooKeeper**, y haga clic en **Configurations**.

Paso 3 Haga clic en **All Configurations**.

Paso 4 Busque parámetro **skipACL**.

skipACL indica si se omite la comprobación de permisos del ZooKeeper. El valor predeterminado es **no**, que indica que la comprobación de permisos está activada. Cambie el valor a **yes**.

Figura 7-63 Configuración del parámetro skipACL



Paso 5 Haga clic en **Save**, haga clic en **OK** y espere a que se muestre el mensaje "Operation successful".

----Fin

7.11.2.1.4 Inicio de sesión en un nodo que no es del clúster mediante un usuario del clúster en modo normal

Escenario

Cuando el clúster se instala en modo normal, los clientes de componentes no admiten la autenticación de seguridad y no pueden utilizar el comando **kinit**. Por lo tanto, los nodos fuera del clúster no pueden usar usuarios del clúster de forma predeterminada. Esto puede dar como resultado un error de autenticación de usuario cuando uno de estos nodos accede a un servidor de componentes.

El administrador del nodo puede configurar un usuario que tiene el mismo nombre que el de un usuario para un nodo fuera del clúster, permitir que el usuario inicie sesión en el nodo mediante el protocolo SSH, y conectarse a los servidores de los componentes del clúster mediante el uso del usuario que inicia sesión en el sistema operativo.

Prerrequisitos

- Los nodos fuera del clúster pueden conectarse al plano de servicio del clúster.
- El servicio KrbServer del clúster se está ejecutando correctamente.
- Ha obtenido la contraseña del usuario **root** del nodo fuera del clúster.
- Se ha planificado y agregado un usuario humano-máquina al clúster, y se ha obtenido el archivo de credenciales de autenticación. Para más detalles, consulte **Creación de un usuario** y **Exportación de un archivo de credenciales de autenticación**.

Procedimiento

Paso 1 Inicie sesión en el nodo donde se agregará un usuario como usuario **root**.

Paso 2 Ejecute el siguiente comando:

rpm -qa | grep pam and **rpm -qa| grep krb5-client**

Se muestran los siguientes paquetes RPM:

```
pam_krb5-32bit-2.3.1-47.12.1
pam-modules-32bit-11-1.22.1
yast2-pam-2.17.3-0.5.211
pam-32bit-1.1.5-0.10.17
pam_mount-32bit-0.47-13.16.1
pam-config-0.79-2.5.58
pam_krb5-2.3.1-47.12.1
pam-doc-1.1.5-0.10.17
pam-modules-11-1.22.1
pam_mount-0.47-13.16.1
pam_ldap-184-147.20
```



```
pam-1.1.5-0.10.17
krb5-client-1.6.3
```

Paso 3 Compruebe si los paquetes RPM de la lista están instalados en el sistema operativo.

- En caso afirmativo, vaya a **Paso 5**.
- Si no, vaya a **Paso 4**.

Paso 4 Obtenga los paquetes RPM faltantes de la imagen del sistema operativo, cargue los archivos al directorio actual y ejecute el siguiente comando para instalar el paquete RPM:

rpm -ivh *.rpm

NOTA

Los paquetes RPM que se van a instalar pueden conllevar riesgos de seguridad. Los riesgos que puede conllevar la instalación de estos paquetes RPM deben tenerse en cuenta durante el endurecimiento del sistema operativo.

Una vez instalados los paquetes RPM, vaya a **Paso 5**.

Paso 5 Ejecute el siguiente comando para configurar la autenticación Kerberos en PAM:

pam-config --add --krb5

NOTA

Si necesita cancelar la autenticación de Kerberos y el inicio de sesión del usuario del sistema en un nodo que no sea del clúster, ejecute el comando **pam-config --delete --krb5** como usuario **root**.

Paso 6 Descomprima el archivo de credenciales de autenticación para obtener **krb5.conf** y use WinSCP para cargar este archivo de configuración en el directorio **/etc** en el nodo fuera del clúster, y ejecute el siguiente comando para configurar permisos relacionados para permitir que otros usuarios accedan al archivo, como permiso **604**:

chmod 604 /etc/krb5.conf

Paso 7 Ejecute el siguiente comando en la sesión de conexión como usuario **root** para agregar el usuario del sistema operativo correspondiente al usuario hombre-máquina y especifique **root** como grupo principal.

La contraseña del usuario del sistema operativo es la misma que la contraseña inicial cuando se crea el usuario humano-máquina en Manager.

useradd *User name* **-m -d /home/admin_test -g root -s /bin/bash**

Por ejemplo, si el nombre del usuario humano-máquina es **admin_test**, ejecute el siguiente comando:

useradd admin_test -m -d /home/admin_test -g root -s /bin/bash

NOTA

Cuando se utiliza el usuario del sistema operativo recién agregado para iniciar sesión en el nodo mediante el protocolo SSH por primera vez, el sistema indica que la contraseña ha caducado después de introducir la contraseña del usuario. y el sistema le indica que la contraseña debe cambiarse después de que vuelva a introducir la contraseña de usuario. Debe introducir una nueva contraseña que cumpla con los requisitos de complejidad de contraseña tanto del sistema operativo del nodo como del clúster.

----Fin

7.11.2.2 Cambio de la contraseña de un usuario del sistema

7.11.2.2.1 Cambio de la contraseña para el usuario admin

Escenario

El usuario **admin** es la cuenta de administrador del sistema del FusionInsight Manager. Se recomienda cambiar periódicamente la contraseña del FusionInsight Manager para mejorar la seguridad del sistema.

Procedimiento

Paso 1 Inicie sesión en FusionInsight Manager.

Se requiere usuario **admin** para iniciar sesión.

Paso 2 Mueva el cursor a **Hello, admin** en la esquina superior derecha de la página.

En el menú que se muestra, haga clic en **Change Password**.

Paso 3 Establezca **Old Password**, **New Password** y **Confirm Password** y haga clic en **OK**.

La contraseña debe cumplir los siguientes requisitos de complejidad:

- Contiene de 8 a 64 caracteres.
- Contiene al menos cuatro tipos de los siguientes: letras mayúsculas, minúsculas, números, espacios y caracteres especiales (~`!?,.;-_'(){}[]/<>@#$%^&*+|\=).
- No puede ser el mismo que el nombre de usuario o el nombre de usuario escrito al revés.
- No puede ser una contraseña común fácil de descifrar.
- No puede ser la misma que la contraseña utilizada en las últimas *N* veces. *N* indica el valor de la **Repetition Rule** en **Configuración de políticas de contraseñas**.

----Fin

7.11.2.2.2 Cambio de la contraseña de un usuario de sistema operativo

Escenario

Durante la instalación del FusionInsight Manager, el sistema crea automáticamente usuario **omm** y **ommdba** en cada nodo del clúster. Cambie periódicamente las contraseñas de inicio de sesión de los usuarios del sistema operativo **omm** y **ommdba** del nodo del clúster para mejorar la seguridad del sistema O&M.

Las contraseñas de los usuarios **omm** y **ommdba** de los nodos pueden ser diferentes.

Prerrequisitos

- Usted ha obtenido la dirección IP del nodo donde se van a cambiar las contraseñas de los usuarios **omm** y **ommdba**.
- Usted ha obtenido la contraseña del usuario **root** antes de cambiar las contraseñas de los usuarios **omm** y **ommdba**.

Cambio de la contraseña de un usuario de sistema operativo

Paso 1 Inicie sesión en el nodo donde se va a cambiar la contraseña como usuario **root**.

Paso 2 Ejecute el siguiente comando para cambiar la contraseña de usuario:

passwd *ommdba*

El resultado del comando en Red Hat es el siguiente:

```
Changing password for user ommdba.
New password:
```

Paso 3 Ingrese una contraseña nueva. La política para cambiar la contraseña de un usuario del sistema operativo varía según el sistema operativo que se utilice realmente.

```
Retype New Password:
Password changed.
```

----Fin

7.11.2.3 Cambio de la contraseña de un usuario interno del sistema

7.11.2.3.1 Cambio de la contraseña para el administrador de Kerberos

Escenario

Se recomienda que el administrador cambie periódicamente la contraseña del administrador de Kerberos **kadmin** para mejorar la seguridad del sistema O&M.

Si se cambia la contraseña de usuario, también se cambia la contraseña de administrador de OMS Kerberos.

Prerrequisitos

Ha instalado el cliente en cualquier nodo del clúster y ha obtenido la dirección IP del nodo.

Procedimiento

Paso 1 Inicie sesión en el nodo donde el cliente está instalado como usuario **root**.

Paso 2 Ejecute el siguiente comando para ir al directorio del cliente, por ejemplo **/opt/hadoopclient**:

cd /opt/hadoopclient

Paso 3 Ejecute el siguiente comando para establecer variables de entorno:

source bigdata_env

Paso 4 Ejecute el siguiente comando para cambiar la contraseña de **kadmin/admin**. El cambio de contraseña tiene efecto en todos los servidores. Mantenga la contraseña segura porque no se puede recuperar una vez que se pierde.

kpasswd kadmin/admin

La contraseña debe cumplir los siguientes requisitos de complejidad:

- Contiene al menos 8 caracteres.

- Contiene al menos cuatro tipos de los siguientes: letras mayúsculas, minúsculas, números, espacios y caracteres especiales (~`!?,.;-_'(){}[]/<>@#$%^&*+|\=).
- No puede ser el mismo que el nombre de usuario o el nombre de usuario escrito al revés.
- No puede ser una contraseña común fácil de descifrar, por ejemplo, **Admin@12345**.
- No puede ser la misma que la contraseña utilizada en las últimas *N* veces. *N* indica el valor de la **Repetition Rule** en **Configuración de políticas de contraseñas**.

----Fin

7.11.2.3.2 Cambio de la contraseña para el administrador de OMS Kerberos

Escenario

Se recomienda que el administrador cambie periódicamente la contraseña del administrador OMS Kerberos **kadmin** para mejorar la seguridad del sistema O&M.

Si se cambia la contraseña de usuario, también se cambia la contraseña de administrador de Kerberos.

Procedimiento

Paso 1 Inicie sesión en cualquier nodo de gestión en el clúster como usuario **omm**.

Paso 2 Ejecute el siguiente comando para ir al directorio relacionado:

cd ${BIGDATA_HOME}/om-server/om/meta-0.0.1-SNAPSHOT/kerberos/scripts

Paso 3 Ejecute el siguiente comando para establecer variables de entorno:

source component_env

Paso 4 Ejecute el siguiente comando para cambiar la contraseña de **kadmin/admin**. Esta operación tiene efecto para todos los servidores. Mantenga la contraseña segura porque no se puede recuperar una vez que se pierde.

kpasswd kadmin/admin

La contraseña debe cumplir los siguientes requisitos de complejidad:

- Contiene al menos 8 caracteres.
- Contiene al menos cuatro tipos de los siguientes: letras mayúsculas, minúsculas, números y caracteres especiales (~`!?,.;-_'(){}[]/<>@#$%^&*+|\=).
- No puede ser el mismo que el nombre de usuario o el nombre de usuario escrito al revés.
- No puede ser una contraseña común fácil de descifrar., por ejemplo, **Admin@12345**.
- No puede ser la misma que la contraseña utilizada en las últimas *N* veces. *N* indica el valor de la **Repetition Rule** en **Configuración de políticas de contraseñas**.

----Fin

7.11.2.3.3 Cambio de las contraseñas del administrador LDAP y del usuario LDAP (incluido OMS LDAP)

NOTA

Esta sección solo se aplica a MRS 3.1.0. Para versiones posteriores, consulte **Modificación de los parámetros de configuración del servicio OMS**.

Escenario

Se recomienda que el administrador cambie periódicamente las contraseñas del administrador LDAP **cn=root,dc=hadoop,dc=com** y del usuario LDAP **cn=pg_search_dn,ou=Users,dc=hadoop,dc=com** para mejorar la seguridad del sistema O&M.

Si se cambian las contraseñas, también se cambia la contraseña del administrador o usuario OMS LDAP.

NOTA

Si el clúster se actualiza de una versión anterior a una versión más reciente, la contraseña del administrador LDAP heredará la política de contraseñas del clúster antiguo. Para garantizar la seguridad del sistema, se recomienda cambiar la contraseña después de la actualización del clúster.

Impacto en el sistema

- Cambiar la contraseña de usuario del servicio LdapServer es una operación de alto riesgo y requiere reiniciar los servicios KrbServer y LdapServer. Si se reinicia KrbServer, es posible que no se pueda consultar a los usuarios ejecutando el comando **id** en los nodos del clúster temporalmente. Por lo tanto, tenga cuidado al reiniciar KrbServer.
- Después de cambiar la contraseña del usuario LDAP **cn=pg_search_dn,ou=Users,dc=hadoop,dc=com**, el usuario puede ser bloqueado en el componente LDAP. Por lo tanto, se recomienda desbloquear al usuario después de cambiar la contraseña. Para obtener más información sobre cómo desbloquear el usuario, consulte **Desbloqueo de usuarios LDAP y cuentas de gestión**.

Prerrequisitos

Antes de cambiar la contraseña del usuario LDAP **cn=pg_search_dn,ou=Users,dc=hadoop,dc=com**, asegúrese de que el usuario no está bloqueado ejecutando el siguiente comando en el nodo de gestión activo del clúster:

NOTA

Para consultar el número de puerto OLdap, realice los siguientes pasos:

1. Inicie sesión en FusionInsight Manager y seleccione **System** > **OMS** > **oldap** > **Modify Configuration**:
2. El valor de **LDAP Service Listening Port** es el puerto OLDAP.

ldapsearch -H ldaps://*Floating IP address of OMS:OLDAP port***-LLL -x -D cn=pg_search_dn,ou=Users,dc=hadoop,dc=com -W -b cn=pg_search_dn,ou=Users,dc=hadoop,dc=com -e ppolicy**

Introduzca la contraseña del usuario LDAP **pg_search_dn**. Si se muestra la siguiente información, el usuario está bloquea. En este caso, desbloquee el usuario. Para obtener más información, consulte **Desbloqueo de usuarios LDAP y cuentas de gestión**.

NOTA

La contraseña del usuario LDAP **pg_search_dn** es generada aleatoriamente por el sistema. Puede obtener la contraseña del archivo **/etc/sssd/sssd.conf or /etc/ldap.conf** del nodo activo.

```
ldap_bind: Invalid credentials (49); Account locked
```

Procedimiento

Paso 1 Inicie sesión en FusionInsight Manager, haga clic en **Cluster**, haga clic en el nombre del clúster deseado y elija **Service** > **LdapServer**.

Paso 2 Elija **More** > **Change Database Password**. En el cuadro de diálogo que se muestra, introduzca la contraseña del usuario de inicio de sesión actual y haga clic en **OK**.

Paso 3 En el cuadro de diálogo **Change Password**, seleccione el usuario cuya contraseña se va a modificar en el cuadro desplegable **User Information**.

Paso 4 Introduzca la contraseña antigua en el cuadro de texto **Old Password** e introduzca la nueva contraseña en los cuadros de texto **New Password** y **Confirm Password**.

La contraseña debe cumplir los siguientes requisitos de complejidad:

- Contiene de 16 a 32 caracteres.
- Contiene al menos tres tipos de los siguientes: letras mayúsculas, minúsculas, números, espacios y caracteres especiales (`~!@#$%^&*()-_=+|[{}];,<.>/?).
- No puede ser el mismo que el nombre de usuario o el nombre de usuario escrito al revés.
- No puede ser la misma que la contraseña actual.

Paso 5 Seleccione **I have read the information and understood the impact** y haga clic en **OK** para confirmar la modificación y reiniciar el servicio.

----Fin

7.11.2.3.4 Cambio de la contraseña del administrador LDAP

NOTA

Esta sección solo se aplica a MRS 3.1.0. Para versiones posteriores, consulte **Modificación de los parámetros de configuración del servicio OMS**.

Escenario

Se recomienda que el administrador cambie periódicamente las contraseñas de las cuentas de administrador LDAP **cn=krbkdc,ou=Users,dc=hadoop,dc=com** y **cn=krbadmin,ou=Users,dc=hadoop,dc=com** para mejorar la seguridad del sistema O&M.

Impacto en el sistema

- Debe reiniciar el servicio KrbServer después de cambiar la contraseña.
- Después de cambiar la contraseña, compruebe si las cuentas de administrador LDAP **cn=krbkdc,ou=Users,dc=hadoop,dc=com** y **cn=krbadmin,ou=Users,dc=hadoop,dc=com** están bloqueadas, ejecute el siguiente comando en el nodo de gestión activa del clúster para comprobar si **krbkdc** está bloqueado (el método para el usuario **krbadmin** es similar):

NOTA

Método de obtención de número de puerto de OLdap:

1. Inicie sesión en FusionInsight Manager y seleccione **System** > **OMS** > **oldap** > **Modify Configuration**:
2. El valor del parámetro **LDAP Listening Port** es **oldap port**.

ldapsearch -H ldaps://*OMS_FLOAT_ IP address:OLdap port* **-LLL -x -D cn=krbkdc,ou=Users,dc=hadoop,dc=com -W -b cn=krbkdc,ou=Users,dc=hadoop,dc=com -e ppolicy**

Introduzca la contraseña de la cuenta de administrador LDAP **krbkdc**. Si se muestra el siguiente mensaje, la cuenta está bloqueada. Para obtener más información sobre cómo desbloquear la cuenta, consulte **Desbloqueo de usuarios LDAP y cuentas de gestión**.

```
ldap_bind: Invalid credentials (49); Account locked
```

Prerrequisitos

Ha obtenido la dirección IP del nodo de gestión.

Procedimiento

Paso 1 Inicie sesión en el nodo de gestión activo como usuario **omm** con la dirección IP del nodo de gestión activo.

Paso 2 Ejecute el siguiente comando para ir al directorio relacionado:

cd ${BIGDATA_HOME}/om-server/om/meta-0.0.1-SNAPSHOT/kerberos/scripts

Paso 3 Ejecute el siguiente comando para cambiar la contraseña de la cuenta de administrador LDAP:

./okerberos_modpwd.sh

Ingrese la contraseña antigua y luego ingrese una nueva contraseña dos veces.

La contraseña debe cumplir los siguientes requisitos de complejidad:

- Contiene de 16 a 32 caracteres.
- Contiene al menos tres tipos de los siguientes: letras mayúsculas, minúsculas, números, espacios y caracteres especiales (`~!@#$%^&*()-_=+|[{}];,<.>/?).
- No puede ser la misma que la contraseña actual.

Si se muestra la siguiente información, se cambia la contraseña.

```
Modify kerberos server password successfully.
```

Paso 4 Inicie sesión en FusionInsight Manager, haga clic en **Cluster**, haga clic en el nombre del clúster deseado y elija **Services** > **KrbServer**. En la página mostrada, elija **More** >**Restart Service**.

Ingrese la contraseña y no seleccione **Restart upper-layer services**. Haga clic en **OK** para reiniciar el servicio KrbServer.

----Fin

7.11.2.3.5 Cambio de la contraseña de un usuario en ejecución de componentes

Escenario

Se aconseja al administrador cambiar periódicamente la contraseña de cada componente que ejecuta el usuario para mejorar la seguridad del sistema O&M.

Los usuarios en ejecución de componentes pueden clasificarse en los dos tipos siguientes dependiendo de si sus contraseñas iniciales son generadas aleatoriamente por el sistema:

- Si la contraseña inicial de un componente que ejecuta el usuario es generada aleatoriamente por el sistema, el usuario es del tipo máquina-máquina.
- Si el sistema no genera aleatoriamente la contraseña inicial de un usuario que ejecuta un componente, el usuario es del tipo hombre-máquina.

Impacto en el sistema

Si el sistema genera aleatoriamente la contraseña inicial, es necesario reiniciar el clúster para que el cambio de contraseña surta efecto. Los servicios no están disponibles durante el reinicio.

Prerrequisitos

Ha instalado el cliente en cualquier nodo del clúster y ha obtenido la dirección IP del nodo.

Procedimiento

Paso 1 Inicie sesión en el nodo donde se instala el cliente como usuario de instalación del cliente

Paso 2 Ejecute el siguiente comando para cambiar al directorio del cliente, por ejemplo, /opt/client:

cd /opt/client

Paso 3 Ejecute el siguiente comando para establecer variables de entorno:

source bigdata_env

Paso 4 Ejecute el siguiente comando e introduzca la contraseña del usuario **kadmin/admin** para iniciar sesión en la consola **kadmin**:

kadmin -p kadmin/admin

NOTA

La contraseña predeterminada del usuario **kadmin/admin** es **Admin@123**. La contraseña caducará en su primer inicio de sesión. Cambie la contraseña como se le solicite. Mantenga la contraseña segura porque no se puede recuperar una vez que se pierde.

Paso 5 Ejecute el siguiente comando para cambiar la contraseña de un usuario que ejecuta un componente interno.

cpw *Internal system username*

Ejemplo: **cpw hdfs**

Usuario **hdfs** es un ejemplo. Sustitúyalo con el nombre de usuario real.

La contraseña debe cumplir los siguientes requisitos de complejidad:

- Contiene al menos 8 caracteres.
- Contiene al menos cuatro tipos de los siguientes: letras mayúsculas, minúsculas, números, espacios y caracteres especiales (~`!?,.;-_'(){}[]/<>@#$%^&*+|\=).
- No puede ser el mismo que el nombre de usuario o el nombre de usuario escrito al revés.
- No puede ser una contraseña común fácil de descifrar, por ejemplo, **Admin@12345**.
- No puede ser la misma que la contraseña utilizada en los últimos *N* veces. *N* indica el valor de **Number of Historical Passwords** configuradas en **Configuración de políticas de contraseñas**. Esta política se aplica solo a las cuentas hombre-máquina.

NOTA

Ejecute el siguiente comando para comprobar la información del usuario:

getprinc *Internal system username*

Ejemplo: **getprinc hdfs**

Paso 6 Determine el tipo de usuario cuya contraseña debe cambiarse.

- Si el usuario es un usuario máquina-máquina, vaya a **Paso 7**.
- Si el usuario es un usuario hombre-máquina, la contraseña se cambia con éxito y no se requiere ninguna acción adicional.

Paso 7 Inicie sesión en FusionInsight Manager.

Paso 8 Haga clic en **Cluster**, haga clic en el nombre del clúster deseado y elija **More** > **Restart**.

Paso 9 En la ventana mostrada, ingrese la contraseña del usuario actual de inicio de sesión y haga clic en **OK**.

Paso 10 En el cuadro de diálogo de confirmación de reinicio que se muestra, haga clic en **OK**.

Paso 11 Espere a que se muestre el mensaje "Operation successful".

----Fin

7.11.2.4 Cambiar la contraseña de un usuario de base de datos

7.11.2.4.1 Cambio de la contraseña del administrador de la base de datos de OMS

Escenario

Se recomienda que el administrador cambie periódicamente la contraseña del administrador de la base de datos OMS para mejorar la seguridad del sistema O&M.

Procedimiento

Paso 1 Inicie sesión en el nodo de gestión activo como usuario **root**.

NOTA

La contraseña del usuario **ommdba** no se puede cambiar en el nodo de gestión en espera. De lo contrario, es posible que el clúster no funcione correctamente. Cambie la contraseña solo en el nodo de gestión activo.

Paso 2 Ejecute el siguiente comando para cambiar a otro usuario:

su - omm

Paso 3 Ejecute el siguiente comando para ir al directorio relacionado:

cd $OMS_RUN_PATH/tools

Paso 4 Ejecute el siguiente comando para cambiar la contraseña de usuario **ommdba**:

mod_db_passwd ommdba

Paso 5 Ingrese la contraseña antigua del usuario **ommdba** e ingrese una nueva contraseña dos veces.

La contraseña debe cumplir los siguientes requisitos de complejidad:

- Contiene de 16 a 32 caracteres.
- Contiene al menos tres tipos de los siguientes: letras mayúsculas, minúsculas, números y caracteres especiales (~`!@#$%^&*()-+_=\|[{}];,<.>/?).
- No puede ser el mismo que el nombre de usuario o el nombre de usuario escrito al revés.
- No puede ser lo mismo que las últimas 20 contraseñas históricas.

Si se muestra la siguiente información, se cambia la contraseña.

```
Congratulations, update [ommdba] password successfully.
```

----Fin

7.11.2.4.2 Cambio de la contraseña del usuario de acceso a datos de la base de datos de OMS

Escenario

Se recomienda que el administrador cambie periódicamente la contraseña del usuario que accede a la base de datos OMS para mejorar la seguridad del sistema O&M.

Impacto en el sistema

Es necesario reiniciar el servicio OMS para que la nueva contraseña surta efecto. El servicio no está disponible durante el reinicio.

Procedimiento

Paso 1 En FusionInsight Manager, seleccione **System** > **OMS** > **gaussDB** > **Change Password**.

Paso 2 Busque la fila donde se encuentra usuario **omm** y haga clic en **Change Password** en la columna **Operation**.

Paso 3 En la ventana mostrada, ingrese la contraseña del usuario actual de inicio de sesión y haga clic en **OK**.

Paso 4 Introduzca las contraseñas antiguas y nuevas según se le solicite.

La contraseña debe cumplir los siguientes requisitos de complejidad:

- Debe contener entre 8 y 32 caracteres.
- Contiene al menos tres tipos de los siguientes: letras mayúsculas, minúsculas, números y caracteres especiales (~`!@#$%^&*()-+_=\|[{}];,<.>/?).
- No puede ser el mismo que el nombre de usuario o el nombre de usuario escrito al revés.
- No puede ser lo mismo que las últimas 20 contraseñas históricas.

Paso 5 Haga clic en **OK**. Espere hasta que el sistema muestre un mensaje que indique que la operación se ha realizado correctamente.

Paso 6 Busque la fila donde se encuentra usuario **omm** y haga clic en **Restart OMS Service** en la columna **Operation**.

Paso 7 En la ventana mostrada, ingrese la contraseña del usuario actual de inicio de sesión y haga clic en **OK**.

Paso 8 En el cuadro de diálogo de confirmación de reinicio que se muestra, haga clic en **OK** para reiniciar el servicio OMS.

----Fin

7.11.2.4.3 Cambio de la contraseña de un usuario de base de datos de componentes

Escenario

Se recomienda que el administrador cambie periódicamente la contraseña para cada usuario de la base de datos de componentes para mejorar la seguridad del sistema O&M.

NOTA

Esta sección solo se aplica a MRS 3.1.0. Para las versiones posteriores a MRS 3.1.0, consulte **Restablecimiento de la contraseña de usuario de la base de datos de componentes**.

Impacto en el sistema

Es necesario reiniciar los servicios para que la nueva contraseña entre en vigor. Los servicios no están disponibles durante el reinicio.

Procedimiento

Paso 1 En el Administrador de FusionInsight, haga clic en **Cluster**, haga clic en el nombre del clúster deseado y haga clic en **Services**.

Paso 2 Haga clic en el nombre del servicio cuya contraseña de usuario de base de datos se va a restablecer. En la página **Dashboard** que se muestra, haga clic en **Stop Service**.

En el cuadro de diálogo que se muestra, introduzca la contraseña del usuario de inicio de sesión actual y haga clic en **OK**.

Después de confirmar el impacto de detener el servicio, espere hasta que se detenga el servicio.

Paso 3 Haga clic en el servicio cuya contraseña de usuario de la base de datos se va a cambiar y elija **More** > **Change Database Password**. En la página mostrada, introduzca la contraseña del usuario de inicio de sesión actual y haga clic en **OK**.

Paso 4 Introduzca las contraseñas antiguas y nuevas según se le solicite.

La contraseña debe cumplir los siguientes requisitos de complejidad:

- Debe contener entre 8 y 32 caracteres.
- Contiene al menos tres tipos de los siguientes: letras mayúsculas, minúsculas, números y caracteres especiales (~`!@#$%^&*()-+_=\|[{}];",<.>/?).

- No puede ser el mismo que el nombre de usuario o el nombre de usuario escrito al revés.
- No puede ser lo mismo que las últimas 20 contraseñas históricas.

Paso 5 Seleccione **I have read the information and understand the impact** y haga clic en **OK**.

Paso 6 Una vez cambiada la contraseña, elija **More** >**Restart Service**. En el cuadro de diálogo que se muestra, introduzca la contraseña del usuario de inicio de sesión actual, haga clic en **OK** y seleccione **Restart the upper-layer services**. Haga clic en **OK** para reiniciar los servicios.

----Fin

7.11.2.4.4 Restablecimiento de la contraseña de usuario de la base de datos de componentes

Escenario

Las contraseñas predeterminadas para los componentes del clúster MRS para conectarse a la base de datos DBService son aleatorias. Se recomienda restablecer periódicamente las contraseñas de los usuarios de la base de datos de componentes para mejorar la seguridad del sistema O&M.

NOTA

Esta sección solo se aplica a MRS 3.1.2 o posterior. Para versiones anteriores a MRS 3.1.2, consulte **Cambio de la contraseña de un usuario de base de datos de componentes**.

Impacto en el sistema

Para restablecer las contraseñas, debe detener y reiniciar los servicios, durante los cuales los servicios no están disponibles.

Procedimiento

Paso 1 En FusionInsight Manager, haga clic en **Cluster**, haga clic en el nombre del clúster deseado y haga clic en **Services**.

Paso 2 Haga clic en el nombre del servicio cuya contraseña de usuario de base de datos se va a restablecer, por ejemplo, **Kafka** y haga clic en **Stop Service** en la página **Dashboard**.

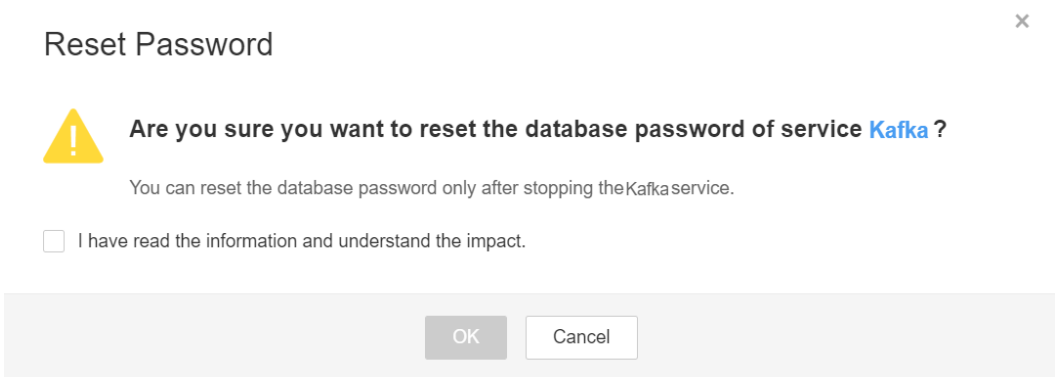
En el cuadro de diálogo que se muestra, introduzca la contraseña del usuario de inicio de sesión actual y haga clic en **OK**.

Después de confirmar el impacto de detener el servicio, espere hasta que se detenga el servicio.

Paso 3 En la página **Dashboard**, seleccione **More** > **Reset Database Password**.

En el cuadro de diálogo que se muestra, introduzca la contraseña del usuario de inicio de sesión actual y haga clic en **OK**.

Seleccione "I have read the information and understand the impact", y haga clic en **OK**.



Paso 4 Una vez restablecida la contraseña, haga clic en **Start Service** en la página **Dashboard**.

Paso 5 En el cuadro de diálogo que se muestra, haga clic en **OK** y espere hasta que se inicie el servicio.

----Fin

7.11.2.4.5 Cambio de la contraseña para usuario compdbuser de la base de datos de DBService

Escenario

Se recomienda que el administrador cambie periódicamente la contraseña del administrador de la base de datos OMS para mejorar la seguridad del sistema O&M.

Procedimiento

Paso 1 Log in to FusionInsight Manager, choose **Cluster** > **Services** > **DBService**, click **Instance**, y vea la dirección IP del nodo DBService activo.

Paso 2 Inicie sesión en el nodo DBService activo como usuario **root**.

NOTA

La contraseña del usuario **compuserdb** no se puede cambiar en el nodo DBService en espera. Cambie la contraseña solo en el nodo de gestión activo.

Paso 3 Cambie al directorio **$DBSERVER_HOME** y configure las variables de entorno:

su - omm

cd $DBSERVER_HOME

source .dbservice_profile

Paso 4 Ejecute el siguiente comando para cambiar la contraseña del usuario **compdbuser** como usuario **omm** de la base de datos de DBService:

gsql -U omm -W omm*Password of user omm of the DBService database* **-d postgres -p 20051 -c "alter user compdbuser identified by '***New password***' valid until '***Expiration time***';"**

NOTA

- La nueva contraseña debe cumplir los siguientes requisitos de complejidad:
  - Contiene de 16 a 32 caracteres.
  - Contiene al menos tres tipos de los siguientes: letras mayúsculas, minúsculas, números y caracteres especiales (~`!@#$%^&*()-+_=\|[{}];:",<.>/?).
  - No puede ser el mismo que el nombre de usuario o el nombre de usuario escrito al revés.
  - No puede ser lo mismo que las últimas 20 contraseñas históricas.
- El formato de tiempo de caducidad es xxxx-xx-xx, por ejemplo **2020-10-31**.

Si se muestra la siguiente información, la modificación se realiza correctamente:

```
ALTER ROLE
```

----Fin

7.11.2.5 Cambiar o restablecer la contraseña para el usuario admin de Manager

Usuario **admin** es la cuenta de administrador del sistema de Manager. Se recomienda cambiar periódicamente la contraseña de Manager para mejorar la seguridad del sistema.

Si la contraseña se ha perdido, restablezca la contraseña haciendo referencia a **Restablecimiento de la contraseña para el usuario admin**.

Cambio de la contraseña para el usuario admin

Puede cambiar la contraseña del usuario **admin** en Manager sólo para clústeres con autenticación de Kerberos activada y clústeres con autenticación de Kerberos desactivada pero la función EIP activada.

Paso 1 Inicie sesión en FusionInsight Manager.

Se requiere usuario **admin** para iniciar sesión.

Paso 2 Mueva el cursor sobre **Hello, admin** en la esquina superior derecha de la página.

En el menú desplegable de la cuenta de usuario, seleccione **Change Password**.

Paso 3 Establezca **Old Password**, **New Password** y **Confirm Password** y haga clic en **OK**.

----Fin

Restablecimiento de la contraseña para el usuario admin

Paso 1 Inicie sesión en el nodo **Master1**.

Paso 2 (Opcional) Para cambiar la contraseña como usuario **omm**, ejecute el siguiente comando para cambiar el usuario:

sudo su - omm

Paso 3 Ejecute el siguiente comando para cambiar al directorio del cliente, por ejemplo, **/opt/Bigdata/client**:

cd /opt/Bigdata/client

Paso 4 Ejecute el siguiente comando para configurar las variables de entorno:

source bigdata_env

Paso 5 Ejecute el siguiente comando para iniciar sesión en la consola como usuario **kadmin/admin**:

kadmin -p kadmin/admin

NOTA

La contraseña predeterminada del **kadmin/admin** de usuario es **Admin@123**, que caducará en su primer inicio de sesión. Cambie la contraseña según se le indique y mantenga segura la nueva contraseña.

Paso 6 Ejecute el siguiente comando para restablecer la contraseña del usuario **admin**:

cpw admin

----Fin

7.11.3 Gestión de certificado

7.11.3.1 Sustitución del certificado de CA

Escenario

El certificado de CA de se utiliza para encriptación de datos durante la comunicación entre el cliente y el servidor de un componente para garantizar la seguridad de la comunicación. Puede reemplazar el certificado de CA en FusionInsight Manager para garantizar la seguridad del producto. Esta operación es aplicable a los siguientes escenarios:

- Después de instalar el clúster por primera vez, importe un certificado de empresa.
- Si el certificado de empresa ha caducado o es necesario reforzar la seguridad, reemplácelo por un nuevo certificado.

Después de reemplazar el certificado de CA, los certificados utilizados por HDFS, YARN, MapReduce, HBase, Loader, HueOozie, Hive, Tomcat, CAS, HTTPD, y LDAP en se actualizarán automáticamente.

El archivo de certificado y el archivo de clave se pueden aplicar desde el centro de certificados de empresa o generar por el usuario del clúster.

NOTA

- Solo los certificados de CA que se pueden emitir y en formato **X.509** se pueden importar en FusionInsight.
- FusionInsight requiere que el formato de codificación del sistema operativo sea **en_US.UTF-8** o **POSIX**. De lo contrario, la función de certificado será anormal.
- Si existe un nodo defectuoso aislado en el clúster actual, no se reemplazará el certificado de CA del nodo. Después de desaislar el nodo, debe volver a instalar los servicios que se ejecutan en el nodo para asegurarse de que el nodo y el clúster utilizan el mismo certificado de CA.

Impacto en el sistema

El sistema de debe reiniciarse durante el reemplazo y no se puede acceder ni proporcionar servicios.

Prerrequisitos

- Ha obtenido los archivos que se van a importar al clúster de, incluidos el archivo de certificado de CA (*.crt), el archivo de clave (*.key) y el archivo (password.property) que guarda la contraseña del archivo de clave. El nombre del certificado y el nombre de la clave admiten letras y dígitos.
- Ha preparado una contraseña para acceder al archivo de clave.

  Para evitar posibles riesgos de seguridad, la contraseña debe cumplir los siguientes requisitos de complejidad:

  – Contiene al menos 8 caracteres.

  – Contiene al menos cuatro tipos de los siguientes: letras mayúsculas, minúsculas, números y caracteres especiales (~`!?,.;-_'(){}[]/<>@#$%^&*+|\=).
- Cuando solicite un certificado desde el centro de certificados, proporcione la contraseña para acceder al archivo de clave y solicite los archivos de certificado en formatos CRT, CER, CERT y PEM y los archivos de clave en formatos KEY y PEM. El certificado aplicado debe tener la función de emisión.

Procedimiento

Paso 1 Inicie sesión en cualquier nodo de gestión en el clúster como usuario **omm**.

Paso 2 Seleccione un método para generar archivos de certificado y archivos de clave.

- Si el certificado es generado por el centro de certificados, guarde el archivo de certificado y el archivo de clave en el directorio de usuario **omm** en el nodo de gestión.

  NOTA

  Si el archivo de certificado obtenido no tiene el formato **.crt** y el archivo de clave no tiene el formato **.key** ejecute los siguientes comandos para cambiar los formatos de archivo:

  mv *Certificate name.Certificate formatCertificate name***.crt**

  mv *Key name.Key format Key name***.key**

  Por ejemplo, ejecute los siguientes comandos para nombrar el archivo de certificado **ca.crt** y el archivo de clave **ca.key**:

  mv server.cer ca.crt

  mv server_key.pem ca.key
- Si el usuario del clúster genera el certificado, ejecute los siguientes comandos para generar el archivo de certificado y el archivo de clave en el directorio de usuario **omm** en el nodo de gestión:

  a. Generar el archivo clave.

  Ejecute el siguiente comando para comprobar si la versión de OpenSSL es 1.1.1 o posterior:

  /usr/bin/openssl version

  - Si es así, ejecute el siguiente comando:

    openssl genrsa -out *Key name***.key -aes256 3072**
  - Si no, ejecute el siguiente comando:

    openssl genrsa -out *Key name***.key -aes256 3072 -sha256**

  Por ejemplo, para generar el archivo de clave **ca.key**, ejecute el siguiente comando:

  openssl genrsa -out ca.key -aes256 3072 -sha256

  Ingrese la contraseña dos veces como se le indique y presione **Enter**.


```
Enter pass phrase for ca.key:
Verifying - Enter pass phrase for ca.key:
```

b. Generar el archivo de certificado.

openssl req -new -x509 -days 1825 -key *Key name***.key -out** *Certificate name***.crt -subj "/C=cn/ST=guangdong/L=shenzhen/O=huawei/OU=huawei/CN=huawei" -sha256**

Por ejemplo, para generar el archivo de certificado **ca.crt**, ejecute el siguiente comando:

openssl req -new -x509 -days 1825 -key ca.key -out ca.crt -subj "/C=cn/ST=guangdong/L=shenzhen/O=huawei/OU=huawei/CN=huawei" -sha256

Ingrese la contraseña del archivo de clave como se le solicite y presione **Enter**.

```
Enter pass phrase for ca.key:
```

Paso 3 Ejecute el siguiente comando en el directorio de usuario **omm** en el nodo de gestión para guardar la contraseña para acceder al archivo de clave.

sh ${BIGDATA_HOME}/om-server/om/sbin/genPwFile.sh

Ingrese la contraseña dos veces como se le indique y presione **Enter**. Una vez encriptada, la contraseña se guarda en **password.property**.

```
Please input key password:
Please Confirm password:
```

NOTA

- El archivo **password.property** generado en un nodo sólo es aplicable en el clúster al que pertenece el nodo actual.
- En escenarios de DR activo/en espera, el script **genPwFile.sh** debe ejecutarse en los nodos de clúster activo y DR, y se debe ingresar la misma contraseña para los dos clústeres.

Paso 4 Comprima los tres archivos en formato **.tar** y guárdelos en el equipo local.

tar -cvf *Package name Certificate name* **.crt** *Key name* **.key password.property**

Por ejemplo, **tar -cvf test.tar ca.crt ca.key password.property**

NOTA

En escenarios de recuperación ante desastres activos/en espera, ejecute este comando en cada nodo del clúster.

Paso 5 Inicie sesión en FusionInsight Manager y elija **System** > **Certificate**.

Paso 6 En el área **Upload Certificate**, haga clic en el botón de selección de archivos. En la ventana de selección de archivos, seleccione los paquetes de archivos de certificado **.tar** obtenidos y ábralos y haga clic en **Upload**. El sistema importa automáticamente el certificado.

Paso 7 Después de importar el certificado, el sistema le pedirá que sincronice la configuración del clúster y reinicie el servicio web para que el nuevo certificado surta efecto. Después de completar estas operaciones, haga clic en **OK**.

Paso 8 En el cuadro de diálogo que se muestra, escriba la contraseña y haga clic en **OK** para sincronizar automáticamente la configuración del clúster y reiniciar el servicio web.

Paso 9 Después de reiniciar el clúster, introduzca la URL para acceder al FusionInsight Manager en el cuadro de dirección del navegador y compruebe si la interfaz de usuario web del FusionInsight Manager se puede mostrar correctamente.

NOTA

El certificado de empresa ha caducado o se ha reforzado la seguridad. Después de reemplazar el certificado de, reemplace también el certificado local.

Paso 10 Elija **More** > **Restart**. En el cuadro de diálogo que se muestra, introduzca la contraseña del usuario de inicio de sesión actual y haga clic en **OK**.

NOTA

Después de reemplazar el certificado de CA, debe reiniciar el clúster sin conexión para que el certificado surta efecto. No se admite el reinicio continuo.

Paso 11 En el cuadro de diálogo de confirmación de reinicio que se muestra, haga clic en **OK**.

----Fin

7.11.3.2 Sustitución de certificados de HA

Escenario

Los certificados de HA se utilizan para cifrar la comunicación entre los procesos activos/en espera y los procesos de alta disponibilidad para garantizar la seguridad. Reemplace los certificados HA en los nodos de gestión activos y en espera en FusionInsight Manager para garantizar la seguridad del producto. Esta operación es aplicable a los siguientes escenarios:

- Después de instalar el clúster por primera vez, importe un certificado de empresa.
- Si el certificado de empresa ha caducado o es necesario reforzar la seguridad, reemplácelo por un nuevo certificado.

NOTA

MRS pero no es aplicable a escenarios en los que no están instalados los nodos de gestión activos y en espera.

El archivo de certificado y el archivo de clave se pueden aplicar desde el centro de certificados de empresa o generar por el usuario del clúster.

Impacto en el sistema

FusionInsight Manager debe reiniciarse durante la sustitución y no se puede acceder ni proporcionar servicios.

Prerrequisitos

- Ha obtenido el archivo raíz **root-ca.crt** y el archivo de clave **root-ca.pem** del certificado que se va a reemplazar.
- Ha preparado una contraseña, por ejemplo, **Userpwd@123**, para acceder al archivo de clave.

  Para evitar posibles riesgos de seguridad, la contraseña debe cumplir los siguientes requisitos de complejidad:

  – Contiene al menos 8 caracteres.

  – Contiene al menos cuatro tipos de los siguientes: letras mayúsculas, minúsculas, números y caracteres especiales (~`!?,.;-_'(){}[]/<>@#$%^&*+|\=).

- Cuando solicite un certificado desde el centro de certificados, proporcione la contraseña para acceder al archivo de clave y solicite los archivos de certificado en formatos CRT, CER, CERT y PEM y los archivos de clave en formatos KEY y PEM. El certificado aplicado debe tener la función de emisión.

Procedimiento

Paso 1 Inicie sesión en el nodo de gestión activo como usuario **omm** mediante la dirección IP del nodo de gestión activo.

Paso 2 Seleccione un método para generar archivos de certificado y archivos de clave.

- Si el certificado es generado por el centro de certificados, guarde el archivo de certificado y el archivo de clave en el directorio **${OMS_RUN_PATH}/workspace0/ha/local/cert** en los nodos de gestión activo y en espera.

  NOTA

  Si el archivo de certificado obtenido no tiene el formato **.crt** y el archivo de clave no tiene el formato **.pem**, ejecute los siguientes comandos para cambiar los formatos de archivo:

  mv *Certificate name.Certificate format***root-ca.crt**

  mv *Key name.Key format* **root-ca.pem**

  Por ejemplo, ejecute los siguientes comandos para nombrar el archivo de certificado **root-ca.crt** y el archivo de clave **root-ca.pem**:

  mv server.cer root-ca.crt

  mv server_key.key root-ca.pem

- Si el usuario del clúster genera el certificado, ejecute el siguiente comando para generar **root-ca.crt** y **root-ca.pem** en el directorio **${OMS_RUN_PATH}/workspace0/ha/local/cert**:

  sh ${OMS_RUN_PATH}/workspace/ha/module/hacom/script/gen-cert.sh --root-ca --country=CN --state=*state* **--city=***city* **--company=***company* **--organize=***organize* **--common-name=***commonname* **--email=***Cluster user email address*

  NOTA

  El período de validez del archivo de certificado generado es de 10 años. Cuando el archivo de certificado del sistema está a punto de caducar, el sistema genera la alarma "ALM-12055 El archivo de certificado está a punto de caducar".

  Por ejemplo, ejecute el siguiente comando:

  sh ${OMS_RUN_PATH}/workspace/ha/module/hacom/script/gen-cert.sh --root-ca --country=CN --state=guangdong --city=shenzhen --company=huawei --organize=IT --common-name=HADOOP.COM --email=abc@*xxx*.com

  Ingrese la contraseña como se le solicite y presione **Enter**.

  ```
  Enter pass phrase for /opt/huawei/Bigdata/om-server/OMS/workspace/ha/local/cert/root-ca.pem:
  ```

  El comando se ejecuta si se muestra la siguiente información:

  ```
  Generate root-ca pair success.
  ```

Paso 3 En el nodo de gestión activo, ejecute el siguiente comando como usuario **omm** para copiar **root-ca.crt** y **root-ca.pem** al directorio **${BIGDATA_HOME}/om-server/om/security/certHA**:

cp -arp ${OMS_RUN_PATH}/workspace0/ha/local/cert/root-ca.* ${BIGDATA_HOME}/om-server/om/security/certHA

Paso 4 Copie **root-ca.crt** y **root-ca.pem** generadas en el nodo de gestión activo en el directorio **${BIGDATA_HOME}/om-server/om/security/certHA** del nodo de gestión en espera como usuario **omm**.

scp ${OMS_RUN_PATH}/workspace0/ha/local/cert/root-ca.* omm@***IP address of the standby management node*:**${BIGDATA_HOME}/om-server/om/security/certHA

Paso 5 Ejecute el siguiente comando para generar un certificado HA y realizar el reemplazo automático:

sh ${BIGDATA_HOME}/om-server/om/sbin/replacehaSSLCert.sh

Ingrese la contraseña como se le solicite y presione **Enter**.

```
Please input ha ssl cert password:
```

El certificado DBService HA se reemplaza correctamente si se muestra la siguiente información:

```
[INFO] Succeed to replace ha ssl cert.
```

NOTA

Si el usuario desea actualizar el paquete para cifrar la contraseña HA, agregue el parámetro **-u**.

Paso 6 Ejecute el siguiente comando para reiniciar el OMS:

sh ${BIGDATA_HOME}/om-server/om/sbin/restart-oms.sh

Se muestra la siguiente información:

```
start HA successfully.
```

Paso 7 Inicie sesión en el nodo de gestión en espera como usuario **omm** mediante la dirección IP del nodo de gestión en espera.

Ejecute **sh ${BIGDATA_HOME}/om-server/om/sbin/status-oms.sh** para comprobar si **HAAllResOK** del nodo de gestión es **Normal** y si FusionInsight Manager puede iniciar sesión de nuevo. En caso afirmativo, la operación es exitosa.

----Fin

7.11.4 Mejoras de seguridad

7.11.4.1 Políticas de endurecimiento

Endurecimiento de Tomcat

Tomcat se endurece de la siguiente manera basado en software de código abierto durante la instalación y uso del software del FusionInsight Manager:

- La versión de Tomcat se actualiza a la versión oficial.
- Los permisos en los directorios bajo aplicaciones se establecen en **500** y se admite el permiso de escritura en algunos directorios.
- El paquete de instalación de Tomcat se elimina automáticamente después de instalar el software del sistema.
- La función de despliegue automático está deshabilitada para proyectos en directorios de aplicaciones. Solo se despliegan los proyectos **web**, **cas** y **client**.

- Algunos métodos de **http** no utilizados están deshabilitados, evitando ataques mediante el uso de los métodos **http**.
- El puerto de shutdown predeterminado y el comando del servidor de Tomcat se cambian para evitar que los piratas informáticos cierren el servidor y ataquen servidores y aplicaciones.
- Para garantizar la seguridad, se cambia el valor de **maxHttpHeaderSize**, lo que permite a los administradores del servidor controlar las solicitudes anormales de los clientes.
- El archivo de descripción de la versión de Tomcat se modifica después de instalar Tomcat.
- Para evitar la divulgación de información de Tomcat, los atributos del servidor de Connector se modifican para que los atacantes no puedan obtener información sobre el servidor.
- Los permisos en los archivos y directorios de Tomcat, como los archivos de configuración, archivos ejecutables, directorios de registro y carpetas temporales, están bajo control.
- El reciclaje de facade de sesión está desactivado para evitar fugas de solicitudes.
- LegacyCookieProcessor se utiliza como CookieProcessor para evitar la filtración de datos sensibles en las cookies.

Endurecimiento de LDAP

LDAP se endurece de la siguiente manera después de instalar un clúster:

- En el archivo de configuración LDAP, la contraseña de la cuenta de administrador se cifra mediante SHA. Después de actualizar el OpenLDAP a 2.4.39 o posterior, los datos se sincronizan automáticamente entre los nodos LDAP activo y en espera mediante el mecanismo externo SASL, que impide la divulgación de la contraseña.
- El servicio LDAP del clúster admite el protocolo SSLv3 de forma predeterminada, que se puede utilizar de forma segura. Cuando OpenLDAP se actualiza a 2.4.39 o posterior, LDAP utiliza automáticamente TLS1.0 o posterior para evitar riesgos de seguridad desconocidos.

Endurecimiento de JDK

- Si el proceso del cliente utiliza el algoritmo de encriptación AES256, se requiere un endurecimiento de seguridad de JDK. Las operaciones son las siguientes:

  Obtenga el paquete Java Cryptography Extension (JCE) cuya versión coincida con la de JDK. El paquete JCE contiene **local_policy.jar** y **US_export_policy.jar**. Copie los archivos JAR en el directorio siguiente y reemplace los archivos en el directorio.

  – Linux: *JDK installation directory*/**jre/lib/security**

  – Windows: *JDK installation directory***jre\lib\security**

  NOTA

  Acceda a la comunidad Open JDK de código abierto para obtener el archivo JCE.

- Si el proceso cliente utiliza el algoritmo de encriptación SM4, el paquete JAR necesita ser actualizado.

  Obtenga **SMS4JA.jar** en el directorio *client installation directory*/**JDK/jdk/jre/lib/ext/** y copie el paquete JAR en el directorio siguiente:

  – Linux: *JDK installation directory*/**jre/lib/ext/**

– Windows: *JDK installation directory***jre\lib\ext**

7.11.4.2 Configuración de una dirección IP de confianza para acceder a LDAP

Escenario

De forma predeterminada, cualquier dirección IP puede acceder al servicio LDAP desplegado en OMS y clúster. Para habilitar el acceso al servicio LDAP solo mediante direcciones IP de confianza, puede configurar la política INPUT en la lista de filtrado de iptables.

Impacto en el sistema

Después de la configuración, no se puede acceder al servicio LDAP mediante direcciones IP que no estén configuradas. Antes de la expansión, las direcciones IP agregadas deben configurarse como direcciones IP de confianza.

Prerrequisitos

- Ha recopilado las direcciones IP del plano de gestión y las direcciones IP del plano de servicio de todos los nodos del clúster y todas las direcciones IP flotantes.
- Ha obtenido la cuenta de usuario **root** para todos los nodos del clúster.

Procedimiento

Configuración de direcciones IP de confianza para el servicio LDAP en el OMS

Paso 1 Inicie sesión en FusionInsight Manager.

Paso 2 Elija **System** > **OMS** y elija **oldap** > **Modify Configuration** para ver el número de puerto de OMS LDAP, es decir, el valor de **LDAP Listening Port**. El número de puerto predeterminado es **21750**.

Paso 3 Inicie sesión en el nodo de gestión activo como usuario **root** usando la dirección IP del nodo de gestión activo.

Paso 4 Ejecute el siguiente comando para comprobar la política INPUT en la lista de filtrado de iptables:

iptables -L

Por ejemplo, si no se configura ninguna regla, la política INPUT se muestra de la siguiente manera:

```
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
```

Paso 5 Ejecute el siguiente comando para configurar todas las direcciones IP utilizadas por el clúster como direcciones IP de confianza. Cada dirección IP necesita ser agregada independientemente.

iptables -A INPUT -s *Trusted IP address* **-p tcp --dport** *Port number* **-j ACCEPT**

Por ejemplo, para configurar **10.0.0.1** como una dirección IP de confianza y habilitarlo para acceder al puerto **21750** debe ejecutar el siguiente comando:

iptables -A INPUT -s 10.0.0.1 -p tcp --dport 21750 -j ACCEPT

Paso 6 Ejecute el siguiente comando para configurar todas las direcciones IP como direcciones IP no confiables. Las direcciones IP de confianza no se verán afectadas por esta regla.

iptables -A INPUT -p tcp --dport *Port number* **-j DROP**

Por ejemplo, para deshabilitar todas las direcciones IP para acceder a **21750** del puerto, ejecute el siguiente comando:

iptables -A INPUT -p tcp --dport 21750 -j DROP

Paso 7 Ejecute el siguiente comando para ver la política INPUT modificada en la lista de filtrado de iptables:

iptables -L

Por ejemplo, después de configurar una dirección IP de confianza, la política INPUT se muestra de la siguiente manera:

```
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  10.0.0.1            anywhere            tcp dpt:21750
DROP       tcp  --  anywhere            anywhere            tcp dpt:21750
```

Paso 8 Ejecute el siguiente comando para ver las reglas y los números de regla en la lista de filtrado de iptables:

iptables -L -n --line-number

```
Chain INPUT (policy ACCEPT)
num target     prot opt source               destination
1   DROP       tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:21750
```

Paso 9 Ejecute el siguiente comando para eliminar la regla deseada de la lista de filtrado de iptables según los requisitos del sitio:

iptables -D INPUT *Number of the rule to be deleted*

Por ejemplo, para eliminar la regla 1, ejecute el siguiente comando:

iptables -D INPUT 1

Paso 10 Inicie sesión en el nodo de gestión en espera como usuario **root** utilizando la dirección IP en espera. Repita **Paso 4** a **Paso 9**.

Configuración de direcciones IP de confianza para el servicio LDAP en el clúster

Paso 11 Inicie sesión en FusionInsight Manager.

Paso 12 Haga clic en **Cluster**, haga clic en el nombre del clúster deseado y elija **Service** > **LdapServer**. En la página mostrada, haga clic en **Instance** para ver los nodos donde se encuentran los servicios LDAP.

Paso 13 Vaya a la página **Configurations** y vea el número de puerto LDAP del clúster, es decir, el valor de **LDAP_SERVER_PORT**. El valor predeterminado es **21780**.

Paso 14 Inicie sesión en el nodo LDAP como usuario **root** utilizando la dirección IP del servicio LDAP.

Paso 15 Ejecute el siguiente comando para ver la política INPUT en la lista de filtrado de iptables:

iptables -L

Por ejemplo, si no se configura ninguna regla, la política INPUT se muestra de la siguiente manera:


```
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
```

Paso 16 Ejecute el siguiente comando para configurar todas las direcciones IP utilizadas por el clúster como direcciones IP de confianza. Cada dirección IP necesita ser agregada independientemente.

iptables -A INPUT -s *Trusted IP address* **-p tcp --dport** *Port number* **-j ACCEPT**

Por ejemplo, para configurar **10.0.0.1** como una dirección IP de confianza y habilitarlo para acceder al puerto **21780** debe ejecutar el siguiente comando:

iptables -A INPUT -s 10.0.0.1 -p tcp --dport 21780 -j ACCEPT

Paso 17 Ejecute el siguiente comando para configurar todas las direcciones IP como direcciones IP no confiables. Las direcciones IP de confianza no se verán afectadas por esta regla.

iptables -A INPUT -p tcp --dport *Port number* **-j DROP**

Por ejemplo, para deshabilitar todas las direcciones IP para acceder a **21780** del puerto, ejecute el siguiente comando:

iptables -A INPUT -p tcp --dport 21780 -j DROP

Paso 18 Ejecute el siguiente comando para ver la política INPUT modificada en la lista de filtrado de iptables:

iptables -L

Por ejemplo, después de configurar una dirección IP de confianza, la política INPUT se muestra de la siguiente manera:

```
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  10.0.0.1             anywhere            tcp dpt:21780
DROP       tcp  --  anywhere             anywhere            tcp dpt:21780
```

Paso 19 Ejecute el siguiente comando para ver las reglas y los números de regla en la lista de filtrado de iptables:

iptables -L -n --line-number

```
Chain INPUT (policy ACCEPT)
num target     prot opt source               destination
1   DROP       tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:21780
```

Paso 20 Ejecute el siguiente comando para eliminar la regla deseada de la lista de filtrado de iptables según los requisitos del sitio:

iptables -D INPUT *Number of the rule to be deleted*

Por ejemplo, para eliminar la regla 1, ejecute el siguiente comando:

iptables -D INPUT 1

Paso 21 Inicie sesión en el nodo LDAP como usuario **root** usando la dirección IP de otro servicio LDAP, y repita **Paso 15** a **Paso 20**.

----Fin

7.11.4.3 Encriptación de HFile y WAL

Encriptación de HFile y WAL

AVISO

- Establecer el modo de encriptación de HFile y WAL a SMS4 o AES tiene un gran impacto en el sistema y causará pérdida de datos en caso de cualquier mal funcionamiento. Por lo tanto, esta operación no se recomienda.
- La importación de datos por lotes mediante Bulkload no admite la encriptación de datos.

HFile y Write ahead log (WAL) en HBase no están cifrados de forma predeterminada. Para cifrarlos, realice las siguientes operaciones.

Paso 1 En cualquier nodo de HBase, ejecute los siguientes comandos para crear un archivo de clave como usuario **omm**:

sh ${BIGDATA_HOME}/FusionInsight_HD_xxx/install/FusionInsight-HBase-xxx/hbase/bin/hbase-encrypt.sh *<path>/hbase.jks <type> <length> <alias>*

- */<path>/hbase.jks* indica la ruta para almacenar el archivo JKS generado.
- *<type>* indica el tipo de encriptación, que puede ser SMS4 o AES.
- *<length>* indica la longitud de la clave. SMS4 soporta 16-bit y AES soporta 128-bit.
- *<alias>* indica el alias del archivo de clave. Cuando cree el archivo de clave por primera vez, conserve el valor predeterminado **omm**.

Por ejemplo, para generar una clave de encriptación SMS4, ejecute el siguiente comando:

sh ${BIGDATA_HOME}/FusionInsight_HD_xxx**/install/FusionInsight-HBase-xxx/hbase/bin/hbase-encrypt.sh /home/hbase/conf/hbase.jks SMS4 16 omm**

Para generar una clave de encriptación AES, ejecute el siguiente comando:

sh ${BIGDATA_HOME}/FusionInsight_HD_xxx**/install/FusionInsight-HBase-xxx/hbase/bin/hbase-encrypt.sh /home/hbase/conf/hbase.jks AES 128 omm**

NOTA

- Para asegurarse de que las operaciones se pueden realizar correctamente, el directorio **<path>/hbase.jks** debe crearse por adelantado y el usuario de la operación del clúster debe tener el permiso **rw** de este directorio.
- Después de ejecutar el comando, introduzca el mismo *<password>* cuatro veces. La contraseña cifrada en el **Paso 3** es la misma que la contraseña en este paso.

Paso 2 Distribuya los archivos de clave generados en el mismo directorio en todos los nodos del clúster y asigne permisos de lectura y escritura al usuario **omm**.

NOTA

- Los administradores deben seleccionar un procedimiento seguro para distribuir claves en función de los requisitos de seguridad de la empresa.
- Si se pierden los archivos clave de algunos nodos, repita el paso para copiar los archivos clave de otros nodos.

Paso 3 En FusionInsight Manager, establezca **hbase.crypto.keyprovider.parameters.encryptedtext** en la contraseña cifrada. Establezca **hbase.crypto.keyprovider.parameters.uri** en la ruta y el nombre del archivo de clave.

- El formato de **hbase.crypto.keyprovider.parameters.uri** es **jceks://** *<key_Path_Name>*.

  <key_Path_Name> indica la ruta del archivo de clave. Por ejemplo, si la ruta del archivo de clave es **/home/hbase/conf/hbase.jks**, establezca este parámetro en **jceks:///home/hbase/conf/hbase.jks**.

- El formato de **hbase.crypto.keyprovider.parameters.encryptedtext** es *<encrypted_password>*.

  <encrypted_password> indica la contraseña cifrada generada durante la creación del archivo de clave. El valor del parámetro se muestra en texto cifrado. Ejecute el siguiente comando como usuario **omm** para obtener la contraseña cifrada relacionada en los nodos donde está instalado el servicio HBase:

  sh ${BIGDATA_HOME}/FusionInsight_HD_xxx**/install/FusionInsight-HBase-xxx/hbase/bin/hbase-encrypt.sh**

  NOTA

  Después de ejecutar el comando, debe escribir **<password>**. La contraseña es la misma que la introducida en **Paso 1**.

Paso 4 En FusionInsight Manager, establezca **hbase.crypto.key.algorithm** en **SMS4** o **AES** para usar SMS4 o AES para la encriptación de HFile.

Paso 5 En FusionInsight Manager, establezca **hbase.crypto.wal.algorithm** en **SMS4** o **AES** para usar SMS4 o AES para la encriptación WAL.

Paso 6 En FusionInsight Manager, establezca **hbase.regionserver.wal.encryption** en **true**.

Paso 7 Guarde los ajustes y reinicie el servicio HBase para que los ajustes surtan efecto.

Paso 8 Cree una tabla de HBase a través de CLI o código y configure el modo de encriptación para habilitar la encriptación. **<type>** indica el tipo de encriptación y **d** indica la familia de columnas.

- Cuando cree una tabla de HBase a través de CLI, establezca el modo de encriptación en SMS4 o AES para la familia de columnas.

  create *'<table name>', {NAME => 'd',* ***ENCRYPTION => '****<type>****'****}*

- Cuando cree una tabla de HBase con código, establezca el modo de encriptación en SMS4 o AES agregando la siguiente información al código:

```
public void testCreateTable()
{
    String tableName = "user";
    Configuration conf = getConfiguration();
    HTableDescriptor htd = new
HTableDescriptor(TableName.valueOf(tableName));
    HColumnDescriptor hcd = new HColumnDescriptor("d");
    //Set the encryption mode to SMS4 or AES.
    hcd.setEncryptionType("<type>");
    htd.addFamily(hcd);
    HBaseAdmin admin = null;
    try
    {
        admin = new HBaseAdmin(conf);
        if(!admin.tableExists(tableName))
        {
            admin.createTable(htd);
        }
```



```
    }
    catch (IOException e)
    {
        e.printStackTrace();
    }
    finally
    {
        if(admin != null)
        {
            try
            {
                admin.close();
            }
            catch (IOException e)
            {
                e.printStackTrace();
            }
        }
    }
}
```

Paso 9 Para comprobar si la configuración de encriptación se realiza correctamente, consulte **Verificación de la configuración de cifrado**.

Paso 10 Si ha configurado la encriptación SMS4 o AES mediante **Paso 1** a **Paso 7**, pero no establece el parámetro de encriptación relacionado al crear la tabla en **Paso 8**, los datos insertados no se cifran.

En este caso, puede realizar los siguientes pasos para cifrar los datos insertados:

1. Ejecute el comando **flush** para que la tabla importe los datos de la memoria al HFile.

   flush'*<table_name>*'

2. Ejecute los siguientes comandos para modificar las propiedades de la tabla:

   disable'*<table_name>*'

   alter'*<table_name>*'**,NAME=>**'*<column_name>*'**,ENCRYPTION =>** '*<type>*'

   enable'*<table_name>*'

3. Inserte un nuevo registro de datos y limpie la tabla.

   NOTA

   Se debe insertar un nuevo registro de datos para que el HFile genere un nuevo HFile y los datos no cifrados insertados previamente se reescriban y encripten.

   put'*<table_name>*'**,'id2','f1:c1','value22222222222222222222222222222222**'

   flush'*<table_name>*'

4. Realice el siguiente paso para volver a escribir el archivo HFile:

   major_compact'*<table_name>*'

   AVISO

   Durante este paso, la tabla HBase está deshabilitada y no puede proporcionar servicios. Tenga cuidado cuando realice este paso.

5. Puede realizar **Paso 6** para comprobar si la configuración de encriptación es correcta.

----Fin

Verificación de la configuración de cifrado

> NOTA
>
> Esta operación sólo se puede realizar cuando los datos de prueba se pueden escribir en una tabla vacía.

Paso 1 Inicie sesión en el nodo donde está instalado el cliente como usuario de instalación del cliente. Cambie al directorio de instalación del cliente.

cd /opt/client

Paso 2 Ejecute el siguiente comando para establecer variables de entorno:

source bigdata_env

Paso 3 Ejecute el siguiente comando para autenticar al usuario actual si se ha habilitado la autenticación Kerberos para el clúster de seguridad actual. El usuario actual debe tener el permiso para leer y escribir tablas de HBase y el permiso de operación de HDFS.

kinit *Component service user*

Ejecute el siguiente comando para establecer el nombre de usuario de Hadoop si la autenticación de Kerberos no está habilitada para el clúster normal actual:

export HADOOP_USER_NAME=hbase

Paso 4 Ejecute el siguiente comando para iniciar sesión en el cliente de HBase:

hbase shell

Ejecute el siguiente comando para insertar un nuevo registro de datos y vaciar la tabla para generar un archivo HFile:

put*'<table_name>'*,**'id2','***d***:c1','value22222222222222222222222222222222'**

flush*'<table_name>'*

> NOTA
>
> - *<table_name>* indica la tabla configurada con encriptación SMS4 o AES. Para obtener más información sobre cómo configurar la encriptación SMS4 o AES, visite **Paso 8**.
> - *d* indica la familia de columnas configurada con encriptación SMS4 o AES. Para obtener más información sobre cómo configurar la encriptación SMS4 o AES, visite **Paso 8**.

Paso 5 Presione **Ctrl+C** para salir del cliente de HBase.

Paso 6 Ejecute el siguiente comando para ver el directorio donde se almacena el archivo HFile generado en **Paso 4**:

hdfs dfs -ls

El formato de directorio de archivo es de **/hbase/data/***<namespace_name>*/*<table_name>*/*<region_name>*/*<columnfamily_name>*/*<HFile_name>*.

> NOTA
>
> Si *<namespace_name>* no se especifica durante la creación de la tabla de HBase, **default** se utiliza de forma predeterminada.

Ejemplo:


```
/hbase/data/default/create_table/dd61b81b1ba1aad6513b9bdcfd8f871c/d/
aa6fe387b27443afaba40f5b584c1fa7
```

Paso 7 Ejecute el siguiente comando para ver el contenido de HFile:

hbase hfile -f <*HFile path*> **-p**

NOTA

<*HFile path*> indica el directorio donde se encuentra el archivo HFile.

El mensaje de error "com.huawei.hadoop.hbase.io.crypto.CryptoRuntimeException" se mostrará en la salida del comando. Sin embargo, el **HBase shell** todavía puede leer los datos de la tabla, lo que indica que la configuración de encriptación se realizó correctamente.

----Fin

Modificación de un archivo de clave

AVISO

La modificación de un archivo de clave tiene un gran impacto en el sistema y causará la pérdida de datos en caso de cualquier mal funcionamiento. Por lo tanto, esta operación no se recomienda.

Durante la operación de **Encriptación de HFile y WAL**, se debe generar el archivo de clave relacionado y se debe establecer su contraseña para garantizar la seguridad del sistema. Después de un período de ejecución, puede reemplazar el archivo de clave con uno nuevo para cifrar HFile y WAL.

Paso 1 Ejecute el siguiente comando para generar un nuevo archivo de clave como usuario **omm**:

sh ${BIGDATA_HOME}/FusionInsight_HD_xxx/install/FusionInsight-HBase-xxx/hbase/bin/hbase-encrypt.sh <*path*>*/hbase.jks* <*type*> <*length*> <*alias-new*>

- <*path*>*/hbase.jks*: indica la ruta para almacenar el archivo **hbase.jks** generado. La ruta de acceso y el nombre del archivo deben ser coherentes con los del archivo clave generado en **Encriptación de HFile y WAL**.
- <*alias-new*>: indica el alias del archivo de clave. El alias debe ser diferente con el del archivo de clave anterior.
- <*type*>: indica el tipo de encriptación, que puede ser SMS4 o AES.
- <*length*> indica la longitud de la clave. SMS4 soporta 16-bit y AES soporta 128-bit.

Por ejemplo, para generar una clave de encriptación SMS4, ejecute el siguiente comando:

sh ${BIGDATA_HOME}/FusionInsight_HD_xxx**/install/FusionInsight-HBase-xxx/hbase/bin/hbase-encrypt.sh /home/hbase/conf/hbase.jks SMS4 16 omm_new**

Para generar una clave de encriptación AES, ejecute el siguiente comando:

sh ${BIGDATA_HOME}/FusionInsight_HD_xxx**/install/FusionInsight-HBase-xxx/hbase/bin/hbase-encrypt.sh /home/hbase/conf/hbase.jks AES 128 omm_new**

NOTA

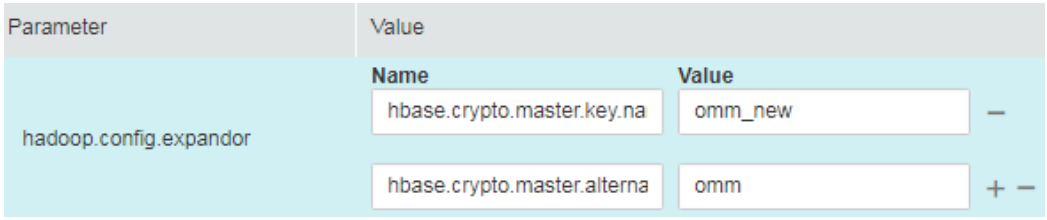
- Para asegurarse de que las operaciones se pueden realizar correctamente, el directorio **<path>/hbase.jks** debe crearse por adelantado y el usuario de la operación del clúster debe tener el permiso **rw** de este directorio.
- Después de ejecutar el comando, debe ingresar el mismo *<password>* tres veces. Esta contraseña es la contraseña del archivo de clave. Puede utilizar la contraseña del archivo antiguo sin ningún riesgo de seguridad.

Paso 2 Distribuya los archivos de clave generados en el mismo directorio en todos los nodos del clúster y asigne permisos de lectura y escritura al usuario **omm**.

NOTA

Los administradores deben seleccionar un procedimiento seguro para distribuir claves en función de los requisitos de seguridad de la empresa.

Paso 3 En la página de configuración del servicio de HBase de FusionInsight Manager, agregue elementos de configuración personalizados, establezca **hbase.crypto.master.key.name** en **omm_new**, establezca **hbase.crypto.master.alternate.key.name** en **omm** y guarde la configuración.

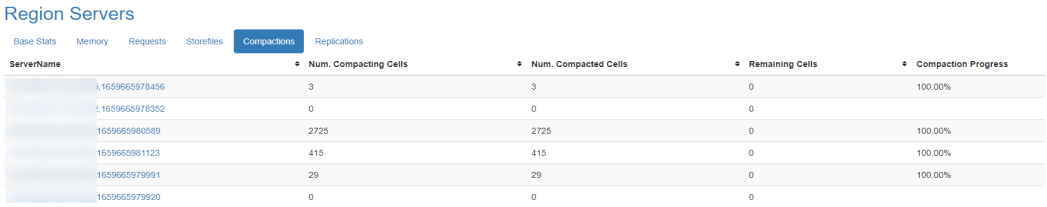


Paso 4 Reinicie el servicio HBase para que la configuración surta efecto.

Paso 5 En el shell de HBase, ejecute el comando **major compact** para generar el archivo HFile basado en el nuevo algoritmo de encriptación.

major_compact *'<table_name>'*

Paso 6 Puede ver el progreso compacto más importante desde la página web de HMaster.



Paso 7 Cuando todos los elementos en **Compaction Progress** lleguen a **100%** y los de **Remaining KVs** sean **0**, ejecute el siguiente comando como usuario **omm** para destruir el archivo de clave anterior:

sh ${BIGDATA_HOME}/FusionInsight_HD_xxx/install/FusionInsight-HBase-xxx/hbase/bin/hbase-encrypt.sh *<path>/hbase.jks <alias-old>*

- *<path>/hbase.jks*: indica la ruta para almacenar el archivo **hbase.jks** generado. La ruta de acceso y el nombre del archivo deben ser coherentes con los del archivo clave generado en **Encriptación de HFile y WAL**.
- *<alias-old>*: indica el alias del archivo de clave antiguo que se va a eliminar.

Por ejemplo:

sh ${BIGDATA_HOME}/FusionInsight_HD_xxx**/install/FusionInsight-HBase-xxx/hbase/bin/hbase-encrypt.sh /home/hbase/conf/hbase.jks omm**

NOTA

Para asegurarse de que las operaciones se pueden realizar correctamente, el directorio **<path>/hbase.jks** debe crearse por adelantado y el usuario de la operación del clúster debe tener el permiso **rw** de este directorio.

Paso 8 Repita **Paso 2** y distribuya de nuevo los archivos de clave actualizados.

Paso 9 Elimine el elemento de configuración autodefinida de HBase **hbase.crypto.master.alternate.key.name** agregado en **Paso 3** desde FusionInsight Manager.

Paso 10 Repita **Paso 4** para que la configuración surta efecto.

----Fin

7.11.4.4 Configuración de parámetros de seguridad de Hadoop

Configuración del cifrado del canal de seguridad

Los canales entre componentes no están cifrados de forma predeterminada. Puede establecer los siguientes parámetros para configurar la encriptación del canal de seguridad.

Acceso a la página para establecer parámetros: en FusionInsight Manager, haga clic en **Cluster**, haga clic en el nombre del clúster deseado, haga clic en **Services** y haga clic en el servicio de destino. En la página mostrada, haga clic en **Configuration** y haga clic en **All Configurations**. Introduzca un nombre de parámetro en el cuadro de búsqueda.

NOTA

Reinicie los servicios correspondientes para que la modificación surta efecto después de modificar los parámetros de configuración.

Tabla 7-84 Descripción de parámetros

Servicio	Parámetro	Descripción	Valor predeterminado
HBase	hbase.rpc.protection	Indica si los canales HBase, incluidos los canales de llamada a procedimiento remoto (RPC) para que los clientes HBase accedan al servidor HBase y los canales RPC entre HMaster y RegionServer están cifrados. Si este parámetro se establece en **privacy**, los canales se cifran y se habilitan las funciones de autenticación, integridad y privacidad. Si este parámetro se establece en **integrity**, los canales no se cifran y solo se habilitan las funciones de autenticación e integridad. Si este parámetro se establece en **authentication**, los canales no se cifran, solo se autentican los paquetes y no se requiere integridad ni privacidad. **NOTA** El modo de privacidad cifra el contenido transmitido, incluida la información sensible, como los tokens de usuario, para garantizar la seguridad del contenido transmitido. Sin embargo, este modo tiene un gran impacto en el rendimiento. En comparación con los otros dos modos, este modo reduce el rendimiento de lectura/escritura en aproximadamente un 60%. Modifique la configuración según los requisitos de seguridad de la empresa. Los elementos de configuración del cliente y del servidor deben ser los mismos.	-
HDFS	dfs.encrypt.data.transfer	Indica si los canales de transferencia de datos de HDFS y los canales para que los clientes accedan a HDFS están cifrados. Los canales de transferencia de datos de HDFS incluyen los canales de transferencia de datos entre DataNodes y los canales de transferencia de datos (DT) para que los clientes accedan a DataNodes. El valor **true** indica que los canales están cifrados. Los canales no están cifrados por defecto.	false

Servicio	Parámetro	Descripción	Valor predeterminado
HDFS	dfs.encrypt.data.transfer.algorithm	Indica si los canales de transferencia de datos de HDFS y los canales para que los clientes accedan a HDFS están cifrados. Este parámetro solo es válido cuando **dfs.encrypt.data.transfer** está establecido en **true**. El valor por defecto es **3des**, que indica que el algoritmo 3DES se utiliza para cifrar datos. El valor también se puede establecer en **rc4**. Sin embargo, para evitar riesgos de seguridad, no se recomienda establecer el parámetro en este valor.	3des
HDFS	hadoop.rpc.protection	Indica si los canales RPC de cada módulo en Hadoop están cifrados. Los canales incluyen: ● Canales RPC para que los clientes accedan a HDFS ● Canales RPC entre módulos en HDFS, por ejemplo, entre DataNode y NameNode ● Canales RPC para que los clientes accedan a YARN ● Canales RPC entre NodeManager y ResourceManager ● Canales RPC para Spark para acceder a YARN y HDFS ● Canales RPC para MapReduce para acceder a YARN y HDFS ● Canales RPC para que HBase acceda a HDFS El valor predeterminado es **privacy**, que indica la transmisión cifrada. El valor **authentication** indica que la transmisión no está cifrada. **NOTA** Puede establecer este parámetro en la página de configuración de componentes de HDFS. El ajuste del parámetro es válido globalmente, es decir, el ajuste de si el canal RPC está cifrado tiene efecto en todos los módulos en Hadoop.	● Modo de seguridad: **privacy** ● Modo normal: **authentication**

Configuración del número máximo de conexiones web simultáneas

Para garantizar la confiabilidad del servidor web, se rechazan nuevas conexiones cuando el número de conexiones de usuario alcanza un umbral específico. Esto evita los ataques DDOS y la falta de disponibilidad del servicio causados por demasiados usuarios que acceden al servidor web al mismo tiempo.

Acceso a la página para establecer parámetros: en FusionInsight Manager, haga clic en **Cluster**, haga clic en el nombre del clúster deseado, haga clic en **Services** y haga clic en el servicio de destino. En la página mostrada, haga clic en **Configuration** y haga clic en **All Configurations**. Introduzca un nombre de parámetro en el cuadro de búsqueda.

Tabla 7-85 Descripción de parámetros

Servicio	Parámetro	Descripción	Valor predeterminado
HDFS/Yarn	hadoop.http.server.MaxRequests	Especifica el número máximo de conexiones web simultáneas de cada componente.	2000
Spark2x	spark.connection.maxRequest	Especifica el número máximo de conexiones de solicitud de JobHistory.	5000

7.11.4.5 Configuración de una lista blanca de direcciones IP para la modificación permitida por HBase

Si la función de replicación está habilitada para los clústeres de HBase, se agrega un mecanismo de protección para la modificación de datos en el clúster HBase en espera para garantizar la coherencia de los datos entre los clústeres activo y en espera. Al recibir una solicitud RPC para la modificación de datos, el clúster de HBase en espera comprueba el permiso del usuario que envía la solicitud (solo los usuarios de gestión de HBase tienen el permiso de modificación). A continuación, comprueba la validez de la dirección IP de origen de la solicitud. Solo se aceptan solicitudes de modificación de direcciones IP de la lista blanca. El elemento **hbase.replication.allowedIPs** configura la lista blanca de direcciones IP.

Inicie sesión en el FusionInsight Manager y elija **Cluster** > **Services** > **HBase**. Haga clic en **Configurations** e introduzca el nombre del parámetro en el cuadro de búsqueda.

Tabla 7-86 Descripción de parámetro

Parámetro	Descripción	Valor predeterminado
hbase.replication.allowedIPs	Permite el procesamiento de solicitudes de replicación solo desde direcciones IP configuradas. Soporta patrones de expresiones regulares separadas por comas. Cada patrón puede ser cualquiera de los siguientes: ● Patrón de Regex Ejemplo: 10.18.40.*, 10.18.*, 10.18.40.11 ● Patrón de rango (El rango solo se puede especificar en el último octeto) Ejemplo: 10.18.40.[10-20] Si este elemento está vacío (valor predeterminado), la lista blanca contiene solo la dirección IP del RegionServer del clúster, lo que indica que solo se aceptan solicitudes de modificación del RegionServer del clúster HBase en espera.	N/A

7.11.4.6 Actualización de una clave para un clúster

Escenario

Cuando se instala un clúster, el sistema genera automáticamente una clave de encriptación para que la información de seguridad en el clúster (como todas las contraseñas de usuario de base de datos y contraseñas de acceso a archivos clave) puede almacenarse en modo de encriptación. Una vez instalado el clúster, si se revela accidentalmente la clave original o se requiere una nueva clave, puede actualizarla manualmente.

Impacto en el sistema

- Después de actualizar una clave de clúster, se genera una nueva clave aleatoriamente en el clúster. Esta clave se utiliza para cifrar y descifrar los datos recién almacenados. La clave antigua no se elimina, y se utiliza para descifrar datos cifrados utilizando la clave antigua. Después de modificar la información de seguridad, por ejemplo, se cambia una contraseña de usuario de base de datos, la nueva contraseña se cifra usando la nueva clave.
- Cuando se actualiza una clave para un clúster, se debe detener el clúster y no se puede acceder a él.

Prerrequisitos

- Ha obtenido las direcciones IP de los nodos de gestión activo y en espera.
- Ha detenido las aplicaciones de servicio de capa superior que dependen del clúster.

Procedimiento

Paso 1 Inicie sesión en FusionInsight Manager.

Paso 2 Elija **Cluster** > *Name of the desired cluster* y haga clic en **Stop**. En el cuadro de diálogo que se muestra, escriba la contraseña del usuario actual

y haga clic en **OK**. Espere un momento hasta que se muestre un mensaje que indique que la operación se ha realizado correctamente.

Paso 3 Inicie sesión en el nodo de gestión activo como usuario **omm**.

Paso 4 Ejecute el siguiente comando para deshabilitar el cierre de sesión al finalizar el tiempo de espera:

TMOUT=0

NOTA

Una vez completadas las operaciones de esta sección, ejecute el comando **TMOUT=***Timeout interval* para restaurar el intervalo de tiempo de espera de manera oportuna. Por ejemplo, **TMOUT=600** indica que un usuario ha cerrado sesión si el usuario no realiza ninguna operación en 600 segundos.

Paso 5 Ejecute el siguiente comando para ir al directorio relacionado:

cd ${BIGDATA_HOME}/om-server/om/tools

Paso 6 Ejecute el siguiente comando para actualizar la clave de clúster:

sh updateRootKey.sh

Escriba **y** como se le solicite.

```
The root key update is a critical operation.
Do you want to continue?(y/n):
```

Si se muestra la siguiente información, la clave se actualiza correctamente.

```
Step 4-1: The key save path is obtained successfully.
...
Step 4-4: The root key is sent successfully.
```

Paso 7 En FusionInsight Manager, haga clic en **Cluster**, haga clic en el nombre del clúster deseado y haga clic en **Start**.

En el cuadro de diálogo que se muestra, haga clic en **OK**. Espere hasta que se muestre un mensaje que indique que el inicio se ha realizado correctamente.

----Fin

7.11.4.7 Endurecimiento del LDAP

Configuración de la política de firewall de LDAP

En el clúster que adopta la red de doble plano, el LDAP se despliega en el plano de servicio. Para garantizar la seguridad de los datos de LDAP, se recomienda configurar la política de firewall en el clúster para deshabilitar los puertos de LDAP relevantes.

Paso 1 Inicie sesión en FusionInsight Manager.

Paso 2 Haga clic en **Cluster**, haga clic en el nombre del clúster deseado, elija **Services** > **LdapServer** y haga clic en **Configurations**.

Paso 3 Comprueba el valor de **LDAP_SERVER_PORT**, que es el puerto de servicio de LdapServer.

Paso 4 Para garantizar la seguridad de los datos, configure la política de firewall para todo el clúster para deshabilitar el puerto LdapServer según el entorno de firewall del cliente.

----Fin

Habilitación de la salida del registro de auditoría de LDAP

Los usuarios pueden establecer el nivel de salida del registro de auditoría del servicio LDAP y los registros de auditoría de salida en un directorio específico, por ejemplo, **/var/log/messages**. La salida de los registros se puede utilizar para comprobar las actividades del usuario y los comandos de operación.

NOTA

Si la función de salida del registro de auditoría de LDAP está habilitada, se generan registros masivos que afectan al rendimiento del clúster. Tenga cuidado al habilitar esta función.

Paso 1 Inicie sesión en cualquier nodo de LdapServer.

Paso 2 Ejecute el siguiente comando para editar el archivo **slapd.conf.consumer** y establezca el valor de **loglevel** en **256** (puede ejecutar el comando **man slapd.conf** en el sistema operativo para ver la definición del nivel de registro).

cd ${BIGDATA_HOME}/FusionInsight_BASE_xxx**/install/FusionInsight-ldapserver-2.7.0/ldapserver/local/template**

vi slapd.conf.consumer

```
...
pidfile         [PID_FILE_SLAPD_PID]
argsfile        [PID_FILE_SLAPD_ARGS]
loglevel   256
...
```

Paso 3 Inicie sesión en FusionInsight Manager, haga clic en **Cluster**, haga clic en el nombre del clúster deseado, elija **Services** > **LdapServer**. En la página mostrada, elija **More** >**Restart Service**. Ingrese la contraseña de administrador y reinicie el servicio.

----Fin

7.11.4.8 Configuración del cifrado de datos de Kafka durante la transmisión

Escenario

Los datos entre el cliente de Kafka y el broker se transmiten en texto sin formato. El cliente Kafka puede desplegarse en una red no confiable, exponiendo los datos de transmisión a riesgos de fuga y manipulación indebida.

Procedimiento

El canal entre componentes no está cifrado de forma predeterminada. Puede establecer los siguientes parámetros para habilitar la encriptación del canal de seguridad.

Acceso a la página para establecer parámetros: en FusionInsight Manager, haga clic en **Cluster**, haga clic en el nombre del clúster deseado y elija **Services** > **Kafka**. En la página mostrada, haga clic en **Configuration** y haga clic en **All Configurations**. Introduzca un nombre de parámetro en el cuadro de búsqueda.

NOTA

Después de la configuración, reinicie el servicio correspondiente para que los ajustes surtan efecto.

Tabla 7-87 describe los parámetros relacionados con la encriptación de transmisión en el servidor Kafka.

Tabla 7-87 Parámetros relevantes para la encriptación de datos de Kafka durante la transmisión

Parámetro	Descripción	Valor predeterminado
ssl.mode.enable	Indica si se habilita el protocolo Secure Sockets Layer (SSL). Si este parámetro se establece en **true**, los servicios relevantes para el protocolo SSL se inician durante el inicio del broker.	false
security.inter.broker.protocol	Indica el protocolo de comunicación entre brokers. El protocolo de comunicación puede ser PLAINTEXT, SSL, SASL_PLAINTEXT o SASL_SSL.	SASL_PLAINTEXT

El protocolo SSL se puede configurar para que el servidor o cliente encripte la transmisión y la comunicación solo después de que **ssl.mode.enable** se establezca en **true** y el broker habilita los protocolos **SSL** y **SASL_SSL**.

7.11.4.9 Configuración del cifrado de datos de HDFS durante la transmisión

Configuración del cifrado de canal de seguridad de HDFS

El canal entre componentes no está cifrado de forma predeterminada. Puede establecer parámetros para habilitar la encriptación de canales de seguridad.

Ruta de navegación para establecer parámetros: en FusionInsight Manager, elija **Cluster** > *Name of the desired cluster* > **Services** > **HDFS** > **Configurations**. En la página mostrada, haga clic en la pestaña **All Configurations**. Introduzca un nombre de parámetro en el cuadro de búsqueda.

NOTA

Después de la configuración, reinicie el servicio correspondiente para que los ajustes surtan efecto.

Tabla 7-88 Parámetros

Elemento de configuración	Descripción	Valor predeterminado
hadoop.rpc.protection	**AVISO** ● La configuración solo se aplica después de reiniciar el servicio. No se admite el reinicio continuo. ● Después de la configuración, debe descargar el archivo de configuración del cliente de nuevo. De lo contrario, HDFS no puede proporcionar los servicios de lectura y escritura. ● Después de la configuración, debe reiniciar el executor. De lo contrario, las funciones de gestión de tareas y de gestión de archivos de la consola no estarán disponibles. Indica si los canales RPC de cada módulo en Hadoop están cifrados. Los canales incluyen: ● Canales RPC para que los clientes accedan a HDFS ● Canales RPC entre módulos en HDFS, por ejemplo, entre DataNode y NameNode ● Canales RPC para que los clientes accedan a Yarn ● Canales RPC entre NodeManager y ResourceManager ● Canales RPC para Spark para acceder a Yarn y HDFS ● Canales RPC para MapReduce para acceder a Yarn y HDFS ● Canales RPC para que HBase acceda a HDFS **NOTA** La configuración tiene efecto globalmente, es decir, el atributo de encriptación del canal RPC de cada módulo en el Hadoop tiene efecto.	● Modo de seguridad: privacidad ● Modo normal: autenticación **NOTA** ● **authentication**: indica que solo se requiere autenticación. ● **integrity**: indica que es necesario realizar la verificación de autenticación y consistencia. ● **privacy**: indica que es necesario realizar la autenticación, la comprobación de coherencia y la encriptación.

Elemento de configuración	Descripción	Valor predeterminado
dfs.encrypt.data.transfer	Indica si los canales de transferencia de datos de HDFS y los canales para que los clientes accedan a HDFS están cifrados. Los canales de transferencia de datos de HDFS incluyen los canales de transferencia de datos entre DataNodes y los canales de transferencia de datos (DT) para que los clientes accedan a DataNodes. El valor **true** indica que los canales están cifrados. Los canales no están cifrados por defecto. **NOTA** ● Este parámetro solo es válido cuando **hadoop.rpc.protection** está establecido en **privacy**. ● Si se transmite una gran cantidad de datos de servicio, la activación de la encriptación por defecto afecta gravemente el rendimiento del sistema. ● Si se configura la encriptación de transmisión de datos para un clúster en el clúster de confianza, se debe configurar la misma encriptación de transmisión de datos para el clúster del mismo nivel.	false
dfs.encrypt.data.transfer.algorithm	Indica el algoritmo para cifrar los canales de transferencia de datos de HDFS y los canales para que los clientes accedan a HDFS. Este parámetro solo es válido cuando **dfs.encrypt.data.transfer** está establecido en **true**. **NOTA** El valor por defecto es **3des**, que indica que el algoritmo 3DES se utiliza para cifrar datos. El valor también se puede establecer en **rc4**. Sin embargo, para evitar riesgos de seguridad, no se recomienda establecer el parámetro en este valor.	3des
dfs.encrypt.data.transfer.cipher.suites	Este parámetro se puede dejar vacío o establecer en **AES/CTR/NoPadding** para especificar el conjunto de encriptación para la encriptación de datos. Si no se especifica este parámetro, el algoritmo de encriptación especificado por **dfs.encrypt.data.transfer.algorithm** se utiliza para la encriptación de datos. El valor predeterminado es **AES/CTR/NoPadding**.	AES/CTR/NoPadding

7.11.4.10 Configuración del cifrado de datos de Spark2x durante la transmisión

Escenario

Esta sección describe cómo configurar el cifrado de los canales de seguridad de Spark2x para mejorar la seguridad.

Procedimiento

Para modificar parámetros, inicie sesión en FusionInsight Manager, haga clic en **Cluster** y elija **Services** > **Spark2x**. En la página mostrada, haga clic en **Configurations** y haga clic en **All Configurations**. Introduzca un nombre de parámetro en el cuadro de búsqueda.

NOTA

Después de la configuración, reinicie el servicio correspondiente para que los ajustes surtan efecto.

Tabla 7-89 Parámetros

Parámetro	Descripción	Valor predeterminado
spark.authenticate	Si se debe habilitar la autenticación de seguridad interna de Spark	Modo de seguridad: **true** Modo normal: **false**
spark.authenticate.enableSaslEncryption	Si se debe habilitar la comunicación cifrada basada en Autenticación simple y capa de seguridad (SASL)	Modo de seguridad: **true** Modo normal: **false**
spark.network.crypto.enabled	Si se debe habilitar el cifrado RPC basado en Estándar de cifrado avanzado (AES)	Modo de seguridad: **true** Modo normal: **false**
spark.network.sasl.serverAlwaysEncrypt	Si se deben deshabilitar las conexiones no cifradas para puertos con autenticación SASL habilitada	false
spark.network.crypto.keyLength	Longitud de la clave de encriptación que se va a generar	256
spark.network.crypto.keyFactoryAlgorithm	Algoritmo utilizado para generar la clave de encriptación	PBKDF2WithHmacSHA1
spark.io.encryption.enabled	Si se debe habilitar el cifrado de E/S de disco local	Modo de seguridad: **true** Modo normal: **false**

Parámetro	Descripción	Valor predeterminado
spark.io.encryption.keygen.algorithm	Algoritmo utilizado para generar la clave de encriptación de E/S	HmacSHA256
spark.io.encryption.keySizeBits	Tamaño de una clave de encriptación de E/S, en bits	256
spark.ssl.ui.enabled	Si se debe habilitar la autenticación Secure Sockets Layer (SSL) para la conexión de interfaz de usuario web	Modo de seguridad: **true** Modo normal: **false**

7.11.4.11 Configuración de ZooKeeper SSL

Escenario

De forma predeterminada, la transmisión de encriptación de canal SSL está deshabilitada entre el cliente ZooKeeper y el servidor y entre instancias en el servidor. Esta sección describe cómo habilitar la transmisión de encriptación de canal ZooKeeper.

NOTA

Esta función solo está disponible para clústeres MRS de la versión 3.1.2 o posterior.

Impacto en el sistema

- Cuando la transmisión de encriptación de canal SSL está habilitada en el servidor ZooKeeper, el rendimiento se deteriora.
- Cuando la transmisión de encriptación de canal SSL está habilitada en el servidor ZooKeeper, es necesario reiniciar el ZooKeeper y los componentes dependientes de la capa superior. Durante el reinicio, los servicios no están disponibles.
- Para habilitar la transmisión de encriptación de canal SSL en el servidor ZooKeeper, debe descargar el cliente de nuevo.
- Si la transmisión de encriptación de canal SSL está habilitada para ZooKeeper, no se admite el reinicio continuo.

Procedimiento

Paso 1 Inicie sesión en FusionInsight Manager, haga clic en **Cluster** y elija **Services** > **ZooKeeper**. En la página mostrada, haga clic en **Configurations** y haga clic en **All Configurations**.

Paso 2 Introduzca el nombre del parámetro en el cuadro de búsqueda y cambie el valor de la siguiente manera:

Tabla 7-90 Elemento de configuración de seguridad

Parámetro	Descripción	Valor predeterminado	Valor nuevo
ssl.enabled	Si se debe habilitar encriptación de comunicación SSL.	false	true

Paso 3 Una vez completada la modificación, haga clic en **Save** y, a continuación, haga clic en **OK**.

Paso 4 Haga clic en **Cluster** y elija **Services** > **ZooKeeper**. En la página Servicio ZooKeeper, elija **More** > **Restart Service**, introduzca la contraseña de autenticación y confirme el impacto de la operación en la página **Restart Service**.

Puede seleccionar **Restart upper-layer services**. Durante el reinicio de todos los componentes afectados, los servicios no estarán disponibles. Tenga cuidado al realizar esta operación.

Paso 5 Haga clic en **OK** y espere hasta que los servicios se reinicien correctamente.

Paso 6 Elija **Cluster** > **Active/Standby Cluster DR** para comprobar si la DR activa/en espera está configurada para el clúster actual.

- En caso afirmativo, vaya a **Paso 7**.
- En caso negativo, no se requiere ninguna otra acción.

Paso 7 La configuración **ssl.enabled** del servicio ZooKeeper en el clúster activo debe ser la misma que en el clúster de DR. Modifique el parámetro **ssl.enabled** en el clúster donde no se realiza ninguna operación haciendo referencia a los pasos anteriores.

Paso 8 Inicie sesión en el nodo OMS activo en el clúster activo como usuario **root** y ejecute los siguientes comandos para reiniciar el proceso de gestión de DR:

su - omm

${BIGDATA_HOME}/om-server/om/share/om/disaster/sbin/restart-disaster.sh

If the following information is displayed, the operation is successful:

```
...
disaster start with process id : 23256
End into restart-disaster.sh
```

Paso 9 Inicie sesión en el nodo OMS activo en el clúster de recuperación ante desastres como usuario **root** y ejecute los siguientes comandos para reiniciar el proceso de gestión de recuperación ante desastres:

su - omm

${BIGDATA_HOME}/om-server/om/share/om/disaster/sbin/restart-disaster.sh

----Fin

7.11.4.12 Cifrado de la comunicación entre el Controller y el Agent

Escenario

Después de instalar un clúster, el Controller y el Agent deben comunicarse entre sí. La autenticación Kerberos se utiliza durante la comunicación. De forma predeterminada, la comunicación no se cifra durante la comunicación en aras del rendimiento del clúster. Los usuarios que tengan requisitos de seguridad exigentes pueden utilizar el método descrito en esta sección para encriptación.

Impacto en el sistema

- El Controller y todos los Agents se reinician automáticamente, lo que interrumpe el FusionInsight Manager.
- El rendimiento de los nodos de gestión se deteriora en clústeres grandes. Se recomienda activar la función de encriptación para clústeres con un máximo de 200 nodos.

Prerrequisitos

Ha obtenido las direcciones IP de los nodos de gestión activo y en espera.

Procedimiento

Paso 1 Inicie sesión en el nodo de gestión activo como usuario **omm**.

Paso 2 Ejecute el siguiente comando para deshabilitar el cierre de sesión al finalizar el tiempo de espera:

TMOUT=0

NOTA

Una vez completadas las operaciones de esta sección, ejecute el comando **TMOUT=***Timeout interval* para restaurar el intervalo de tiempo de espera de manera oportuna. Por ejemplo, la **TMOUT=600** indica que un usuario ha cerrado sesión si el usuario no realiza ninguna operación en 600 segundos.

Paso 3 Ejecute el siguiente comando para ir al directorio relacionado:

cd ${CONTROLLER_HOME}/sbin

Paso 4 Ejecute el siguiente comando para habilitar encriptación de comunicaciones:

./enableRPCEncrypt.sh -t

Ejecute el comando **sh ${BIGDATA_HOME}/om-server/om/sbin/status-oms.sh** para comprobar si **ResHAStatus** del Controller del nodo de gestión activo es **Normal** y si puede iniciar sesión de nuevo en FusionInsight Manager. En caso afirmativo, la activación se realiza correctamente.

Paso 5 Ejecute el siguiente comando para deshabilitar encriptación de comunicaciones cuando sea necesario:

./enableRPCEncrypt.sh -f

Ejecute el comando **sh ${BIGDATA_HOME}/om-server/om/sbin/status-oms.sh** para comprobar si **ResHAStatus** del Controller del nodo de gestión activo es **Normal** y si puede

iniciar sesión de nuevo en FusionInsight Manager. En caso afirmativo, la activación se realiza correctamente.

----Fin

7.11.4.13 Actualización de claves de SSH para el usuario omm

Escenario

Durante la instalación del clúster, el sistema genera automáticamente la clave pública y la clave privada de SSH para que el usuario **omm** establezca la relación de confianza entre los nodos. Después de instalar el clúster, si las claves originales se revelan accidentalmente o se usan nuevas claves, el administrador del sistema puede realizar las siguientes operaciones para cambiar manualmente las claves.

Prerrequisitos

- Se ha detenido el clúster.
- No se realizan otras operaciones de gestión.

Procedimiento

Paso 1 Inicie sesión como usuario **omm** al nodo cuyas claves de SSH necesitan ser reemplazadas.

Si el nodo es un nodo de gestión del Manager, ejecute el siguiente comando en el nodo de gestión activo.

Paso 2 Ejecute el siguiente comando para deshabilitar el cierre de sesión al finalizar el tiempo de espera:

TMOUT=0

NOTA

Una vez completadas las operaciones de esta sección, ejecute el comando **TMOUT=***Timeout interval* para restaurar el intervalo de tiempo de espera de manera oportuna. Por ejemplo, **TMOUT=600** indica que un usuario ha cerrado sesión si el usuario no realiza ninguna operación en 600 segundos.

Paso 3 Ejecute el siguiente comando para generar una clave para el nodo:

- Si el nodo es un nodo de gestión del administrador, ejecute el siguiente comando:

  sh ${CONTROLLER_HOME}/sbin/update-ssh-key.sh
- Si el nodo es un nodo de gestión que no es de Manager, ejecute el siguiente comando:

  sh ${NODE_AGENT_HOME}/bin/update-ssh-key.sh

Si aparece "Succeed to update ssh private key" cuando se ejecuta el comando anterior, la clave SSH se genera correctamente.

Paso 4 Ejecute el siguiente comando para copiar la clave pública del nodo al nodo de gestión activo:

scp ${HOME}/.ssh/id_rsa.pub** *oms_ip*:**${HOME}/.ssh/id_rsa.pub_bak

oms_ip: indica la dirección IP del nodo de gestión activo.

Introduzca la contraseña del usuario **omm** para copiar los archivos.

Paso 5 Inicie sesión en el nodo de gestión activo como usuario **omm**.

Paso 6 Ejecute el siguiente comando para deshabilitar el cierre de sesión en el tiempo de espera del sistema:

TMOUT=0

Paso 7 Ejecute el siguiente comando para ir al directorio relacionado:

cd ${HOME}/.ssh

Paso 8 Ejecute el siguiente comando para agregar nuevas claves públicas:

cat id_rsa.pub_bak >> authorized_keys

Paso 9 Ejecute el siguiente comando para mover el archivo de clave pública temporal, por ejemplo, **/tmp**.

mv -f id_rsa.pub_bak /tmp

Paso 10 Copie el archivo **authorized_keys** del nodo de gestión activo en los otros nodos del clúster:

scp authorized_keys *node_ip*:**/${HOME}/.ssh/authorized_keys**

node_ip: indica la dirección IP de otro nodo del clúster. No se admiten varias direcciones IP.

Paso 11 Ejecute el siguiente comando para confirmar el reemplazo de clave privada sin introducir la contraseña:

ssh *node_ip*

node_ip: indica la dirección IP de otro nodo del clúster. No se admiten varias direcciones IP.

Paso 12 Inicie sesión en FusionInsight Manager. En **Homepage**, busque el clúster deseado y elija > **Start** para iniciar el clúster.

----Fin

7.11.5 Mantenimiento de seguridad

7.11.5.1 Sugerencias de mantenimiento de cuenta

Se recomienda que el administrador realice comprobaciones rutinarias de las cuentas. La comprobación cubre los siguientes elementos:

- Compruebe si las cuentas del sistema operativo, FusionInsight Manager y cada componente son necesarias y si se han eliminado cuentas temporales.
- Compruebe si los permisos de las cuentas son adecuados. Diferentes administradores tienen diferentes derechos.
- Verifique y audite los registros de inicios de sesión y operaciones de todo tipo de cuentas.

7.11.5.2 Sugerencias de mantenimiento de contraseñas

La autenticación de identidad de usuario es una necesidad para acceder al sistema de aplicación. La complejidad y el período de validez de las cuentas de usuario y contraseñas deben cumplir con los requisitos de seguridad de los clientes.

Las sugerencias de mantenimiento de contraseñas son las siguientes:

1. Se debe disponer de personal dedicado para gestionar la contraseña del sistema operativo.
2. Las contraseñas deben cumplir los requisitos de complejidad, como la longitud mínima de la contraseña o los tipos de caracteres.
3. Las contraseñas deben estar cifradas antes de la transferencia. Generalmente, no transfiera contraseñas usando correos electrónicos.
4. Las contraseñas deben estar cifradas en los archivos de configuración.
5. Los usuarios empresariales deben cambiar las contraseñas cuando se entrega el sistema.
6. Las contraseñas deben cambiarse periódicamente.

7.11.5.3 Sugerencias de mantenimiento de registros

Los registros de operaciones ayudan a detectar excepciones como operaciones ilegales e inicios de sesión por parte de usuarios no autorizados. El sistema registra las operaciones importantes en los registros. Puede utilizar registros de operaciones para localizar problemas.

Comprobación de registros regularmente

Verifique los registros del sistema periódicamente y maneje excepciones como operaciones no autorizadas o inicios de sesión de manera oportuna.

Copia de respaldo de registros regularmente

Los registros de auditoría proporcionados por FusionInsight Manager y el clúster registran las actividades y operaciones del usuario. Puede exportar los registros de auditoría en FusionInsight Manager. Si hay demasiados registros de auditoría en el sistema, puede configurar parámetros de volcado para volcar los registros de auditoría en un servidor especificado para asegurarse de que el espacio en disco de los nodos del clúster es suficiente.

Propietario de mantenimiento

Ingenieros de monitorización de redes e ingenieros de mantenimiento de sistemas

7.11.6 Declaración de seguridad

Declaración de uso de JDK

El clúster MRS de es un clúster de big data que proporciona a los usuarios capacidades informáticas y de análisis de datos distribuidos. El JDK integrado de MRS de es OpenJDK, que se utiliza en los siguientes escenarios:

- Funcionamiento y mantenimiento del servicio de la plataforma
- Operaciones de cliente Linux, incluidos envío de servicios y aplicaciones O&M

Descripción del riesgo de JDK

El sistema realiza el control de permisos en el JDK integrado. Solo los usuarios del grupo relacionado de la plataforma FusionInsight pueden acceder al JDK. Además, la plataforma se despliega en la intranet de un cliente. Por lo tanto, el riesgo de seguridad es bajo.

Endurecimiento de JDK

Para obtener más información sobre cómo endurecer el JDK, consulte "Endurecimiento de JDK" en **Políticas de endurecimiento**.

Direcciones IP públicas en Hue

Hue utiliza los casos de prueba de paquetes de terceros, como **ipadrress**, **requests** y **Django** y utiliza las direcciones IP públicas en los comentarios de los casos de prueba. Sin embargo, estas direcciones IP públicas no están involucradas cuando Hue proporciona servicios, y el archivo de configuración de Hue no involucra estas direcciones IP públicas.

8 Guía de operación de MRS Manager (Aplicable a versiones 2.x y anteriores)

8.1 Introducción a MRS Manager

Descripción

MRS gestiona y analiza datos masivos y le ayuda a obtener rápidamente los datos deseados a partir de datos estructurados y no estructurados. La estructura de los componentes de código abierto es compleja. Los procesos de instalación, configuración y gestión requieren mucho tiempo y trabajo. MRS Manager es una plataforma unificada de gestión de clústeres a nivel empresarial y proporciona las siguientes funciones:

- El monitoreo de clústeres le permite ver rápidamente el estado de mantenimiento de hosts y servicios.
- El monitoreo y la personalización de métricas gráficas le permiten obtener rápidamente información clave sobre el sistema.
- Las configuraciones de propiedades de servicio pueden cumplir los requisitos de rendimiento del servicio.
- Con las funciones de instancia de clúster, servicio y rol, puede iniciar o detener servicios y clústeres con un solo clic.

Introducción a la interfaz gráfica de usuario de MRS Manager

MRS Manager proporciona una plataforma de gestión de clústeres unificada, lo que facilita la operación rápida y sencilla para clústeres. Para obtener más información acerca de cómo acceder al MRS Manager, consulte **Acceso a MRS Manager (MRS 2.x o anterior)**.

Tabla 8-1 describe las funciones de cada entrada de operación.

Figura 8-1 MRS Manager

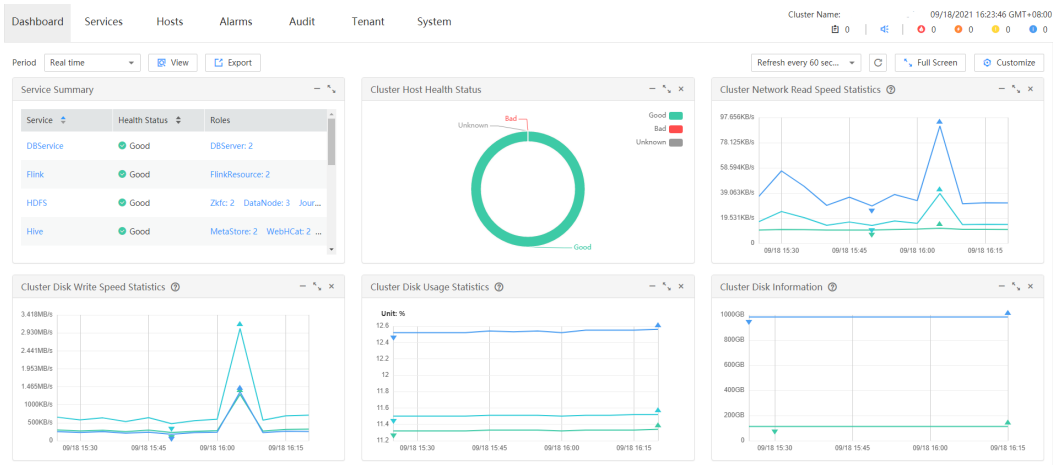


Tabla 8-1 Funciones de cada entrada en la barra de operación

Parámetro	Función
Dashboard	Muestra el estado de todos los servicios, los principales indicadores de monitoreo de cada servicio y el estado del host en gráficos, como gráficos de barras, gráficos de líneas y tablas. Puede personalizar un panel de control para los indicadores clave de monitoreo y arrastrarlo a cualquier posición de la interfaz. La página del panel del sistema admite la actualización automática de datos.
Services	Proporciona la guía de monitoreo, operación y configuración del servicio, que le ayuda a gestionar los servicios de una manera unificada.
Hosts	Proporciona orientación sobre cómo monitorear, operar y configurar hosts, lo que le ayuda a gestionar hosts de manera unificada.
Alarms	Admite la consulta de alarmas y proporciona orientación sobre el manejo de alarmas, lo que le ayuda a identificar y rectificar las fallas del producto y los riesgos potenciales de manera oportuna para garantizar el funcionamiento normal del sistema.
Audit	Permite a los usuarios autorizados consultar y exportar registros de auditoría, lo que le ayuda a ver todas las actividades y operaciones de los usuarios.
Tenant	Proporciona una plataforma unificada de gestión de tenant.
System	Proporciona monitoreo, gestión de configuración de alarmas y gestión de copias de respaldo.

Vaya a la página de pestaña **System** y cambie a otras páginas de función a través de accesos directos. Consulte **Tabla 8-2**.

El siguiente es un ejemplo de redirección rápida a través de accesos directos:

Paso 1 En el Administrador de MRS, haga clic en **System**.

Paso 2 En la página de pestaña **System**, haga clic en un enlace de función. Se muestra la página de función.

Por ejemplo, en el área **Backup and Restoration**, haga clic en **Back Up Data**. Se muestra la página para realizar copias de respaldo de los datos.

Paso 3 Mueva el cursor al borde izquierdo de la ventana del navegador. Se muestra el menú contextual negro **System**. Después de mover el cursor fuera del menú, el menú se contrae.

Paso 4 En el menú contextual que se muestra, puede hacer clic en un enlace de función para ir a la página de función correspondiente.

Por ejemplo, elija **Maintenance > Export Log**. Se muestra la página para exportar registros.

----Fin

Tabla 8-2 Menús de acceso directo en la página de pestaña **System**

Menú	Enlace de función
Copia de respaldo y restauración	Copia de respaldo de datos
	Restablecer datos
Mantenimiento	Registro de exportación
	Registro de auditoría de exportación
	Comprobar estado de salud
Monitoreo y Alarma	Configurar Syslog
	Configurar umbral de alarma
	Configurar SNMP
	Configurar el volcado métrico de monitoreo
	Configurar el Ranking de contribuciones de recursos
Permiso	Gestionar usuario
	Gestionar grupo de usuarios
	Gestionar rol
	Configurar política de contraseñas
	Cambiar la contraseña de la base de datos de OMS
Gestión de recursos	Grupo de servicio estática
Parche	Gestionar parches

Referencia

MapReduce Service (MRS) es un servicio de análisis de datos en la nube pública. Se utiliza para gestionar y analizar conjuntos masivos de datos.

MRS utiliza MRS Manager para gestionar componentes de big data, como componentes en el ecosistema de Hadoop. Por lo tanto, algunos conceptos en la consola de MRS en la nube pública deben ser diferentes de los del MRS Manager. Para obtener más información, consulte **Tabla 8-3**.

Tabla 8-3 Comparación de diferencias

Concepto	MRS de Nube pública	MRS Manager
MapReduce Service	Indica el servicio de nube de análisis de datos en la nube pública, llamado MRS. Este servicio incluye componentes como Hive, Spark, Yarn, HDFS y ZooKeeper.	Proporciona una plataforma de gestión unificada para componentes de big data en clústeres de tenant.

8.2 Comprobación de tareas en ejecución

Escenario

Cuando realiza operaciones en MRS Manager para desencadenar una tarea, se muestran el proceso de ejecución de la tarea y el progreso. Una vez cerrada la ventana de tareas, debe abrir la ventana de tareas mediante la función de gestión de tareas.

MRS Manager reserva las 10 tareas más recientes de forma predeterminada, por ejemplo, reiniciar servicios, sincronizar configuraciones de servicios y realizar comprobaciones de estado.

Procedimiento

Paso 1 En MRS Manager, haga clic en  para abrir la lista de tareas.

Puede ver la siguiente información en la lista de tareas **Name**, **Status**, **Progress**, **Start Time** y **End Time**.

Paso 2 Haga clic en el nombre de la tarea de destino para ver la información detallada sobre la tarea en ejecución.

----Fin

8.3 Gestión de monitoreo

8.3.1 Panel

En MRS Manager, los nodos de un clúster se pueden clasificar en nodos de gestión, nodos de control y nodos de datos. Las tendencias de cambio de las métricas clave de monitoreo de host

en cada tipo de nodo se pueden calcular y mostrar como gráficos de curvas en informes basados en los períodos personalizados. Si un host pertenece a varios tipos de nodo, las estadísticas de métricas se recopilarán repetidamente.

Esta sección proporciona una visión general de los clústeres de MRS y describe cómo ver, personalizar y exportar métricas de monitoreo de nodos en MRS Manager.

Procedimiento

Paso 1 Inicie sesión en MRS Manager. Para obtener más información, consulte **Acceso a MRS Manager (MRS 2.x o anterior)**.

Paso 2 Elija **Dashboard** en MRS Manager.

Paso 3 En **Period**, puede especificar un período para ver los datos de monitoreo. Las opciones son las siguientes:

- Real time
- Last 3 hours
- Last 6 hours
- Last 24 hours
- Last week
- Last month
- Last 3 months
- Last 6 months
- Customize. Si selecciona esta opción, puede personalizar el período de visualización de los datos de monitoreo.

Paso 4 Haga clic en **View** para ver los datos de monitoreo en un período.

- Puede ver **Health Status** y **Roles** de cada servicio en la página **Service Summary** de MRS Manager.
- Haga clic en  encima del gráfico de curvas para ver detalles sobre una métrica.

Paso 5 Personalice un informe de monitoreo.

1. Haga clic en **Customize** y seleccione las métricas de monitorización que se mostrarán en MRS Manager.

   MRS Manager admite un máximo de 14 métricas de monitoreo, pero como máximo 12 métricas de monitoreo personalizadas se pueden mostrar en la página.

   - Cluster Host Health Status
   - Cluster Network Read Speed Statistics
   - Host Network Read Speed Distribution
   - Host Network Write Speed Distribution
   - Cluster Disk Write Speed Statistics
   - Cluster Disk Usage Statistics
   - Cluster Disk Information
   - Host Disk Usage Distribution
   - Cluster Disk Read Speed Statistics

  - Cluster Memory Usage Statistics
  - Host Memory Usage Distribution
  - Cluster Network Write Speed Statistics
  - Host CPU Usage Distribution
  - Cluster CPU Usage Statistics
2. Haga clic en **OK** para guardar las métricas de monitoreo seleccionadas para mostrarlas.

   NOTA

   Haga clic en **Clear** para cancelar todas las métricas de monitoreo seleccionadas en un lote.

Paso 6 Establezca un intervalo de actualización automática o haga clic en para una actualización inmediata.

Se admiten las siguientes opciones de intervalo de actualización:

- Refresh every 60 seconds
- **Refresh every 120 seconds**
- Stop refreshing

NOTA

Si selecciona **Full Screen**, la ventana **Dashboard** se maximizará.

Paso 7 Exportar un informe de monitoreo.

1. Seleccione un período. Las opciones son las siguientes:
   - Real time
   - Last 3 hours
   - Last 6 hours
   - Last 24 hours
   - Last week
   - Last month
   - Last 3 months
   - Last 6 months
   - Customize. Si selecciona esta opción, puede personalizar un período de tiempo para exportar un informe.
2. Haga clic en **Export**. MRS Manager generará un informe sobre las métricas de monitoreo seleccionadas en un período de tiempo especificado. Guarde el informe.

   NOTA

   Para ver los gráficos de curvas de las métricas de monitoreo en un período especificado, haga clic en **View**.

----Fin

8.3.2 Gestión de servicios y monitoreo de hosts

Puede gestionar el siguiente estado e indicadores de todos los servicios (incluidas las instancias de rol) y hosts en MRS Manager:

- Información de estado: incluye el estado de operación, estado, configuración e instancia de rol.
- Información de métricas: incluye métricas clave de monitoreo de servicios.
- Exportación de métrica: permite exportar informes de monitoreo.

NOTA

Establezca un intervalo de actualización automática o haga clic en  para una actualización inmediata.

Se admiten las siguientes opciones de intervalo de actualización:

- Actualizar cada 30 segundos
- Actualizar cada 60 segundos
- Dejar de actualizar

Gestión de monitoreo de servicios

Paso 1 En MRS Manager, haga clic en **Services**.

La lista de servicios incluye **Service**, **Operating Status**, **Health Status**, **Configuration Status**, **Roles** y **Operation** se muestran en la lista de componentes.

- Tabla 8-4 describe el estado de funcionamiento del servicio.

Tabla 8-4 Estado de funcionamiento del servicio

Estado	Descripción
Started	Se ha iniciado el servicio.
Stopped	El servicio está detenido.
Failed to start	Error al iniciar la instancia de rol.
Failed to stop	Error al detener la instancia de rol.
Unknown	Indica el estado inicial del servicio después de reiniciar el sistema en segundo plano.

- Tabla 8-5 describe el estado del servicio.

Tabla 8-5 Estado de salud del servicio

Estado	Descripción
Good	Indica que todas las instancias de rol del servicio se están ejecutando correctamente.
Bad	Indica que el estado de ejecución de al menos una instancia de rol es **Faulty** o que el estado del servicio del que depende el servicio actual es anormal.
Unknown	Indica que todas las instancias de rol del servicio están en estado **Unknown**.

Estado	Descripción
Concerning	Indica que el sistema en segundo plano está reiniciando el servicio.
Partially Healthy	Indica que el estado del servicio del que depende es anormal y que los sistemas externos no pueden invocar las API relacionadas con el servicio anormal.

- Tabla 8-6 describe el estado del servicio.

  Tabla 8-6 Estado de la configuración del servicio

Estado	Descripción
Synchronized	La última configuración entra en vigor.
Expired	La última configuración no tiene efecto después de la modificación del parámetro. Los servicios relacionados deben reiniciarse.
Failed	La comunicación es incorrecta o los datos no se pueden leer o escribir durante la configuración del parámetro. Utilice **Synchronize Configuration** para rectificar la falla.
Configuring	Los parámetros se están configurando.
Unknown	No se puede obtener el estado de configuración actual.

De forma predeterminada, la columna **Service** está ordenada en orden ascendente. Puede hacer clic en el icono junto a **Service**, **Operating Status**, **Health Status** o **Configuration Status** para cambiar el modo de clasificación.

Paso 2 Haga clic en un servicio especificado en la lista para ver su estado y la información de métrica.

Paso 3 Personalice las métricas de monitoreo y exporte información de monitoreo personalizada.

1. En el área **Charts**, haga clic en **Customize** para personalizar las métricas de monitoreo de servicios.
2. En el área **Period**, seleccione una hora del período y haga clic en **View** para ver los datos de supervisión dentro del período de tiempo.
3. Haga clic en **Export** para exportar las métricas mostradas.

----Fin

Gestión de instancias de rol

Paso 1 En MRS Manager, haga clic en **Services** y haga clic en el nombre del servicio de destino en la lista de servicios.

Paso 2 Haga clic en **Instance** para ver el estado del rol.

La lista de instancia de rol contiene el **Role**, **Host Name**, **OM IP Address**, **Business IP Address**, **Rack**, **Operation Status**, **Health Status,** y **Configuration Status** de una instancia.

- Tabla 8-7 muestra el estado de configuración de una instancia de rol.

Tabla 8-7 Estado de instancia de rol

Estado	Descripción
Started	Se ha iniciado la instancia de rol.
Stopped	Se ha detenido la instancia de rol.
Failed to start	Error al iniciar la instancia de rol.
Failed to stop	Error al detener la instancia de rol.
Decommissioning	La instancia de rol se da de baja.
Decommissioned	La instancia de rol se ha dado de baja.
Recommissioning	La instancia de rol se está volviendo a poner en servicio.
Unknown	Indica el estado inicial de la instancia de rol después de reiniciar el sistema en segundo plano.

- Tabla 8-8 muestra el estado de salud de una instancia de rol.

Tabla 8-8 Estado del estado de la instancia de rol

Estado	Descripción
Good	La instancia de rol se está ejecutando correctamente.
Restoring	El sistema en segundo plano está reiniciando una instancia de rol.
Bad	La instancia de rol es anormal. Por ejemplo, no se puede acceder al puerto si no existe PID.
Unknown	El host donde reside una instancia de rol no se conecta al sistema en segundo plano.
Partially Healthy	La instancia de rol se ejecuta parcialmente correctamente.

- Tabla 8-9 muestra el estado de configuración de una instancia de rol.

Tabla 8-9 Estado de configuración de instancia de rol

Estado	Descripción
Synchronized	La última configuración entra en vigor.
Expired	La última configuración no tiene efecto después de la modificación del parámetro. Los servicios relacionados deben reiniciarse.

Estado	Descripción
Failed	La comunicación es incorrecta o los datos no se pueden leer o escribir durante la configuración del parámetro. Utilice **Synchronize Configuration** para rectificar la falla.
Configuring	Los parámetros se están configurando.
Unknown	No se puede obtener el estado de configuración actual.

De forma predeterminada, la columna **Role** está ordenada en orden ascendente. Puede hacer clic en el icono de ordenación situado junto a **Role**, **Host Name**, **OM IP Address**, **Business IP Address**, **Rack**, **Operating Status**, **Health Status** o **Configuration Status** para cambiar el modo de ordenación.

Puede filtrar todas las instancias del mismo rol en la columna **Role**.

Para establecer criterios de búsqueda en el área de búsqueda de roles, haga clic en **Advanced Search** y haga clic en **Search** para ver la información de roles especificada. Haga clic en **Reset** para borrar los criterios de búsqueda. Se soporta la búsqueda difusa.

Paso 3 Haga clic en la instancia de rol de destino para ver su estado y la información de métrica.

Paso 4 Personalice las métricas de monitoreo y exporte información de monitoreo personalizada.

1. En el área **Charts**, haga clic en **Customize** para personalizar las métricas de monitoreo de servicios.
2. En el área **Period**, seleccione una hora del período y haga clic en **View** para ver los datos de supervisión dentro del período de tiempo.
3. Haga clic en **Export** para exportar las métricas mostradas.

----Fin

Gestión de hosts

Paso 1 En MRS Manager, haga clic en **Hosts** para ver el estado de todos los hosts.

La lista de hosts contiene el nombre del host, la dirección IP de gestión, la dirección IP del servicio, el rack, la velocidad de la red, el estado operativo, el estado de estado, el uso del disco, el uso de la memoria y el uso de la CPU.

- **Tabla 8-10** muestra el estado operativo del host.

Tabla 8-10 Estado de funcionamiento del host

Estado	Descripción
Normal	Los roles de host y servicio en el host se están ejecutando correctamente.
Isolated	El host está aislado y los roles de servicio en el host dejan de ejecutarse.

- Tabla 8-11 describe el estado de salud del host.

  Tabla 8-11 Estado del estado del host

Estado	Descripción
Good	El host puede enviar correctamente los latidos del corazón.
Bad	El host no puede enviar los latidos debido al tiempo de espera.
Unknown	El estado inicial del host es desconocido durante la operación de agregar o eliminar un host.

De forma predeterminada, la columna **Host Name** se ordena por nombre de host en orden ascendente. Puede hacer clic en el icono de ordenación situado junto a **Host Name**, **OM IP Address**, **Business IP Address**, **Rack**, **Network Speed**, **Operating Status**, **Health Status**, **Disk Usage**, **Memory Usage** o **CPU Usage** para cambiar el modo de ordenación.

Para establecer criterios de búsqueda en el área de búsqueda de roles, haga clic en **Advanced Search** y haga clic en **Search** para ver la información de roles especificada. Haga clic en **Reset** para borrar los criterios de búsqueda. Se soporta la búsqueda difusa.

Paso 2 Haga clic en el host de destino en la lista de hosts para ver su estado y la información de métrica.

Paso 3 Personalice las métricas de monitoreo y exporte información de monitoreo personalizada.

1. En el área **Charts**, haga clic en **Customize** para personalizar las métricas de monitoreo de servicios.
2. En el área **Period**, seleccione una hora del período y haga clic en **View** para ver los datos de supervisión dentro del período de tiempo.
3. Haga clic en **Export** para exportar las métricas mostradas.

----Fin

8.3.3 Gestión de la distribución de recursos

En MRS Manager, puede consultar las curvas de valor superior, las curvas de valor inferior o las curvas de datos promedio de las métricas de monitoreo de host y servicio clave, es decir, la información de distribución de recursos. MRS Manager le permite ver los datos de monitoreo de la última hora.

También puede modificar la distribución de recursos en MRS Manager para mostrar las curvas de valores superior e inferior en las figuras de distribución de recursos de servicio y host.

No se registra la distribución de recursos de algunas métricas de monitoreo.

Procedimiento

- Vea la distribución de recursos de las métricas de monitoreo de servicios.
  a. En MRS Manager, haga clic en **Services**.

b. Seleccione el servicio de destino en la lista de servicios.

c. Haga clic en **Resource Distribution**.

Seleccione las métricas clave del servicio desde **Metric**. MRS Manager muestra la distribución de recursos de las métricas en la última hora.

- Vea la distribución de recursos de las métricas de monitoreo de host.

a. Haga clic en **Hosts**.

b. Haga clic en el nombre del host especificado en la lista de hosts.

c. Haga clic en **Resource Distribution**.

Seleccione las métricas clave del host desde **Metrics**. MRS Manager muestra la distribución de recursos de las métricas en la última hora.

- Configure la distribución de recursos.

a. En MRS Manager, haga clic en **System**.

b. Haga clic en **Configuration**, haga clic en **Configure Resource Contribution Ranking** en **Monitoring and Alarm**.

c. Cambie el número de recursos que se mostrarán.

- Establezca **Number of Top Resources** en el número de valores superiores.
- Establezca **Number of Bottom Resources** en el número de valores inferiores.

NOTA

La suma del valor máximo y el valor mínimo de la distribución de recursos no puede ser mayor que 5.

d. Haga clic en **OK** para guardar las configuraciones.

El mensaje "Number of top and bottom resources saved successfully" aparece en la esquina superior derecha de la página.

8.3.4 Configuración del volcado de métricas de monitoreo

Puede configurar los parámetros de interconexión en MRS Manager para guardar los datos de métricas de monitoreo en un servidor FTP especificado mediante el protocolo FTP o SFTP. De esta manera, los clústeres MRS pueden interconectarse con sistemas de terceros. El protocolo FTP no cifra los datos, lo que conlleva riesgos potenciales de seguridad. Por lo tanto, se recomienda el protocolo SFTP.

MRS Manager admite la recopilación de todos los datos de métricas de monitoreo en los clústeres gestionados. El periodo de recogida es de 30 segundos, 60 segundos o 300 segundos. Los datos de métrica de monitoreo se almacenan en diferentes archivos de monitoreo en el servidor FTP por período de recopilación. La regla de nomenclatura del archivo de monitoreo está en el formato "*Cluster name*_**metric**_*Monitoring metric data collection period*_*File saving time***.log**".

Prerrequisitos

El ECS correspondiente al servidor de volcado debe estar en la misma VPC que el nodo de Master del clúster MRS, y el nodo de Master puede acceder a la dirección IP y el puerto especificado del servidor de volcado. El servicio FTP en el servidor de volcado se está ejecutando correctamente.

Procedimiento

Paso 1 En MRS Manager, haga clic en **System**.

Paso 2 Haga clic en **Configuration**, haga clic en **Configure Monitoring Metric Dump** en **Monitoring and Alarm**.

Paso 3 Tabla 8-12 describe los parámetros de volcado.

Tabla 8-12 Parámetros de volcado

Parámetro	Descripción	Obligatorio
Dump Monitoring Metric	Si se debe habilitar la interconexión de datos métricos de monitoreo. ●  : Activado. ●  : Desactivado.	Sí
FTP IP Address	Servidor FTP para almacenar archivos de monitoreo después de que los datos métricos de monitoreo estén interconectados.	Sí
FTP Port	Puerto para conectarse al servidor FTP.	Sí
FTP Username	Nombre de usuario para iniciar sesión en el servidor FTP.	Sí
FTP Password	Contraseña para el inicio de sesión en el servidor FTP.	Sí
Save Path	Ruta de acceso para almacenar archivos de monitoreo en el servidor FTP.	Sí
Dump Interval (s)	Intervalo en el que los archivos de monitoreo se almacenan periódicamente en el servidor FTP, en segundos.	Sí
Dump Mode	Protocolo utilizado para enviar archivos de monitoreo. Las opciones son **FTP** y **SFTP**.	Sí
SFTP Public Key	Clave pública del servidor FTP. Este parámetro solo está disponible cuando **Dump Mode** está establecido en **SFTP**. Se recomienda configurar una clave pública. De lo contrario, es posible que se generen riesgos de seguridad.	No

Paso 4 Haga clic en **OK** para completar la configuración.

----Fin

8.4 Gestión de alarma

8.4.1 Consulta y eliminación manual de una alarma

Escenario

Puede ver y borrar las alarmas en MRS Manager.

Generalmente, el sistema borra automáticamente una alarma cuando se rectifica la falla. Si la falla ha sido rectificado y la alarma no se puede borrar automáticamente, puede borrar la alarma manualmente.

Puede ver las últimas 100,000 alarmas (incluidas las alarmas borradas, borradas manualmente y borradas automáticamente) en MRS Manager. Si el número de alarmas borradas supera los 100,000 y está a punto de alcanzar los 110,000, el sistema descarga automáticamente las 10,000 alarmas borradas más tempranas a **${BIGDATA_HOME}/OMSV100R001C00x8664/workspace/data** en el nodo de gestión activa. Un directorio se genera automáticamente cuando las alarmas se descargan por primera vez.

NOTA

Establezca un intervalo de actualización automática o haga clic en para una actualización inmediata.

Se admiten las siguientes opciones de intervalo de actualización:

- Refresh every 30 seconds
- Refresh every 60 seconds
- Stop refreshing

Procedimiento

Paso 1 En MRS Manager, haga clic en **Alarms** para ver la información de alarma en la lista de alarmas.

- De forma predeterminada, la página de lista de alarmas muestra las últimas 10 alarmas.
- De forma predeterminada, las alarmas se muestran en orden descendente según **Generated**. Puede hacer clic en **Alarm ID**, **Alarm Name**, **Severity**, **Generated**, **Location**, **Operation** para cambiar el modo de visualización.
- Puede filtrar todas las alarmas de la misma gravedad en **Severity**, incluidas las alarmas borradas y no borradas.
- Puede hacer clic en , , o para filtrar las alarmas **Critical**, **Major**, **Minor** o **Warning**.

Paso 2 Haga clic en **Advanced Search**. En el área de búsqueda de alarmas mostrada, establezca criterios de búsqueda y haga clic en **Search** para ver la información sobre las alarmas especificadas. Haga clic en **Reset** para borrar los criterios de búsqueda.

NOTA

Puede configurar **Start Time** y **End Time** para especificar el intervalo de tiempo. Puede buscar las alarmas generadas dentro del rango de tiempo.

Manejar la alarma haciendo referencia a **Alarm Reference**. Si las alarmas en algunos escenarios se generan debido a otros servicios en la nube de los que depende MRS, debe ponerse en contacto con el personal de mantenimiento de los servicios en la nube correspondientes.

Paso 3 Si la alarma necesita ser borrada manualmente después de corregir los errores, haga clic en **Clear Alarm**.

NOTA

Si se han manejado varias alarmas, puede seleccionar una o más alarmas para borrarlas y hacer clic en **Clear Alarm** para borrar las alarmas por lotes. Se puede eliminar un máximo de 300 alarmas en cada lote.

----Fin

8.4.2 Configuración de un umbral de alarma

Escenario

Puede configurar un umbral de alarma para conocer el estado de la métrica. Después de seleccionar **Send Alarm**, el sistema envía un mensaje de alarma cuando los datos monitorizados alcanzan el umbral de alarma. Puede ver la información de la alarma en **Alarms**.

Procedimiento

Paso 1 En MRS Manager, haga clic en **System**.

Paso 2 En **Configuration**, haga clic en **Configure Alarm Threshold** en **Monitoring and Alarm**, seleccione las métricas de supervisión según lo planeado y establezca sus líneas de base.

Paso 3 Haga clic en una métrica, por ejemplo, **CPU Usage** y, a continuación, haga clic en **Create Rule**.

Paso 4 Establezca los parámetros de la regla de la métrica de monitoreo en la página de configuración mostrada.

Tabla 8-13 Parámetros de regla de métrica de monitoreo

Parámetro	Descripción	Valor
Rule Name	Especifica el nombre de la regla.	CPU_MAX (example)
Reference Date	Especifica la fecha en la que se genera el historial de indicadores de referencia.	06/11/2014 (ejemplo)
Threshold Type	Especifica el valor máximo o mínimo de una métrica. Si este parámetro se establece en **Max. Value**, el sistema genera una alarma cuando el valor real de la métrica es mayor que el umbral. Si este parámetro se establece en **Min. Value**, el sistema genera una alarma cuando el valor real de la métrica es menor que el umbral.	● Max. value ● Min. value

Parámetro	Descripción	Valor
Alarm Severity	Severidad de alarma	● Critical ● Major ● Minor ● Warning
Time Range	Especifica el período en el que la regla tiene efecto.	De 00:00 a 23:59 (ejemplo)
Threshold	Especifica el umbral de las métricas de monitoreo de reglas.	80 (ejemplo)
Date	Especifica el tipo de fecha en la que la regla surte efecto.	● Workday ● Weekend ● Other
Add Date	Este parámetro solo es válido cuando **Date** está establecido en **Other**. Es posible seleccionar múltiples fechas.	30/11 (ejemplo)

Paso 5 Haga clic en **OK**. Aparece un mensaje en la esquina superior derecha de la página, indicando que la plantilla se ha guardado correctamente.

Send alarm está seleccionado de forma predeterminada. MRS Manager comprueba si el valor de cada métrica supervisada alcanza el umbral. Si el número de tiempos de comprobación consecutivos es igual al valor de **Trigger Count** y no se alcanza el umbral en estas comprobaciones, el sistema envía una alarma. El valor se puede personalizar. **Check Period (s)** indica el intervalo en el que MRS Manager comprueba las métricas de monitoreo.

Paso 6 Busque la fila que contiene la regla recién agregada y haga clic en **Apply** en la columna **Operation**. En la esquina superior derecha aparece un mensaje que indica que la regla *xx* se ha agregado correctamente. Haga clic en **Cancel** en la columna **Operation**. En la esquina superior derecha aparece un mensaje que indica que la regla *xx* se cancela correctamente.

----Fin

8.4.3 Configuración de los parámetros de la interfaz en dirección norte de Syslog

Escenario

Puede configurar la interfaz en dirección norte para que las alarmas generadas en MRS Manager puedan ser reportadas a su sistema de monitoreo de O&M usando Syslog.

AVISO

Si el protocolo Syslog no está cifrado, los datos pueden ser robados.

Prerrequisitos

El ECS correspondiente al servidor debe estar en la misma VPC que el nodo de Master del clúster de MRS, y el nodo de Master puede acceder a la dirección IP y el puerto especificado del servidor.

Procedimiento

Paso 1 En MRS Manager, haga clic en **System**.

Paso 2 Haga clic en **Configuration**, haga clic en **Configure Syslog** en **Monitoring and Alarm**.

El **Syslog Service** está deshabilitado de forma predeterminada. Haga clic en el conmutador para habilitar el servicio Syslog.

Paso 3 Establezca los parámetros de interconexión enumerados en **Tabla 8-14**.

Tabla 8-14 Parámetros de Syslog

Área	Parámetro	Descripción
Protocolo de Syslog	Service IP Address	Especifica la dirección IP del servidor de interconexión.
	Server Port	Especifica el número de puerto para la interconexión.
	Protocol	Especifica el tipo de protocolo. Las opciones son las siguientes: ● **TCP** ● **UDP**
	Severity	Especifica la gravedad del mensaje notificado. Las opciones son las siguientes: ● **Informational** ● **Emergency** ● **Alert** ● **Critical** ● **Error** ● **Warning** ● **Notice** ● **Debug**
	Facility	Especifica el módulo donde se genera el registro.

Área	Parámetro	Descripción
	Identifier	Especifica el ID del producto. El valor predeterminado es **MRS Manager**.
Report Message	Report Format	Especifica el formato de mensaje del informe de alarma. Para obtener más información, consulte la información de ayuda en la página Web.
	Alarm Status	Especifica el tipo de alarma que se va a notificar. ● **Fault**: indica que el mensaje de alarma Syslog se notifica cuando MRS Manager genera una alarma. ● **Clear**: indica que se notifica un mensaje de alarma Syslog cuando se borra una alarma en MRS Manager. ● **Event**: indica que el mensaje de alarma Syslog se notifica cuando MRS Manager genera un evento.
	Report Alarm Severity	Especifica el nivel de la alarma que se va a informar. El valor puede ser **Suggestion**, **Minor**, **Major** y **Critical**.
Uncleared Alarm Reporting	Periodic Uncleared Alarm Report	Especifica si las alarmas confusas se notifican periódicamente. De forma predeterminada, el interruptor de **Periodic Uncleared Alarm Reporting** está deshabilitado. Puede hacer clic en el interruptor para habilitarlo.

Área	Parámetro	Descripción
	Report Interval (min)	Especifica el intervalo para informar periódicamente de las alarmas no borradas al servicio Syslog remoto. Este parámetro solo es válido cuando el interruptor **Periodic Uncleared Alarm Reporting** está habilitado. La unidad es un minuto. El valor predeterminado es **15**. El valor varía de 5 minutos a un día (1,440 minutos).
Heartbeat Settings	Heartbeat Report	Especifica si se deben informar periódicamente los mensajes de latidos de Syslog. De forma predeterminada, el interruptor de **Periodic Uncleared Alarm Reporting** está deshabilitado. Puede hacer clic en el interruptor para habilitarlo.
	Heartbeat Period (min)	Especifica el intervalo para informar periódicamente los mensajes de latidos del corazón. Este parámetro solo es válido cuando el interruptor **Heartbeat Report** está habilitado. La unidad es un minuto. El valor predeterminado es **15**. El valor varía de 1 a 60.
	Heartbeat Packet	Especifica el contenido del mensaje de latido informado. Este parámetro está habilitado cuando **Heartbeat Report** está habilitado. El valor puede contener un máximo de 256 caracteres, incluidos dígitos, letras, guiones bajos (_), barras verticales (|), dos puntos (:), espacios, comas (,), y puntos (.).

NOTA

Después de que se habilite la función de paquete de latido periódico, los paquetes pueden interrumpirse durante la recuperación automática de alguna tolerancia a errores de clúster (por ejemplo, conmutación de nodos de gestión activo/en espera). En este caso, espere a la recuperación automática.

Paso 4 Haga clic en **OK** para completar la configuración.

----Fin

8.4.4 Configuración de los parámetros de interfaz en dirección norte de SNMP

Escenario

Puede configurar la interfaz norte para que las alarmas y las métricas de monitoreo en MRS Manager se puedan integrar en la plataforma de gestión de red mediante SNMP.

Prerrequisitos

El ECS correspondiente al servidor debe estar en la misma VPC que el nodo de Master del clúster de MRS, y el nodo de Master puede acceder a la dirección IP y el puerto especificado del servidor.

Procedimiento

Paso 1 En MRS Manager, haga clic en **System**.

Paso 2 Haga clic en **Configuration**, haga clic en **Configure SNMP** en **Monitoring and Alarm**.

El **SNMP Service** está deshabilitado de forma predeterminada. Haga clic en el conmutador para habilitar el servicio SNMP.

Paso 3 Establezca los parámetros de interconexión enumerados en **Tabla 8-15**.

Tabla 8-15 Parámetros de Syslog

Parámetro	Descripción
Version	Especifica la versión del SNMP, que puede ser: ● v2c: una versión anterior con baja seguridad ● v3: la última versión de SNMP con mayor seguridad que SNMPv2c Se recomienda la versión SNMP v3.
Local Port	Especifica el puerto local. El valor predeterminado es **20000**. El valor oscila entre **1025** y **65535**.
Read Community Name	Especifica el nombre de la comunidad de sólo lectura. Este parámetro solo es válido cuando **Version** está establecido en **v2c**.
Write Community Name	Especifica el nombre de la comunidad de escritura. Este parámetro solo es válido cuando **Version** está establecido en **v2c**.

Parámetro	Descripción
Security Username	Especifica el nombre de usuario de seguridad de SNMP. Este parámetro solo es válido cuando **Version** está establecido en **v3**.
Authentication Protocol	Especifica el protocolo de autenticación. Se recomienda establecer este parámetro para establecer este parámetro en **SHA**. Este parámetro solo es válido cuando **Version** está establecido en **v3**.
Authentication Password	Especifica la clave de autenticación. Este parámetro solo es válido cuando **Version** está establecido en **v3**.
Confirm Password	Se utiliza para confirmar la clave de autenticación. Este parámetro solo es válido cuando **Version** está establecido en **v3**.
Encryption Protocol	Especifica el protocolo de encriptación. Se recomienda establecer este parámetro en **AES256**. Este parámetro solo es válido cuando **Version** está establecido en **v3**.
Encryption Password	Especifica la clave de encriptación. Este parámetro solo es válido cuando **Version** está establecido en **v3**.
Confirm Password	Se utiliza para confirmar la clave de encriptación. Este parámetro solo es válido cuando **Version** está establecido en **v3**.

NOTA

- El **Authentication Password** y el **Encryption Password** deben contener de 8 a 16 caracteres, incluidos al menos tres tipos de los siguientes caracteres: letras mayúsculas, letras minúsculas, dígitos y caracteres especiales. Las dos contraseñas deben ser diferentes. Las dos contraseñas no pueden ser las mismas que el nombre de usuario de seguridad o el reverso del nombre de usuario de seguridad.
- Por motivos de seguridad, cambie periódicamente la contraseña de autenticación y la contraseña de encriptación cuando se utilice el protocolo SNMP.
- Si se utiliza SNMPv3, un usuario de seguridad se bloqueará después de cinco fallas de autenticación consecutivas en 5 minutos. El usuario se desbloqueará automáticamente 5 minutos más tarde.

Paso 4 Haga clic en **Create Trap Target** en el área **Trap Target**. En el cuadro de diálogo que se muestra, establezca los siguientes parámetros:

- **Target Symbol** especifica el ID de destino de captura, que es el ID del NMS o del host que recibe capturas. El valor consta de 1 a 255 caracteres, incluidas letras o dígitos.
- **Target IP Address** especifica la dirección IP de la captura de destino. Las direcciones IP de clase A, B y C pueden usarse para comunicarse con la dirección IP del plano de gestión del nodo de gestión.
- **Target Port** especifica el puerto que recibe las capturas. El número de puerto debe ser coherente con el extremo del par y oscila entre 0 y 65535.
- **Trap Community Name** solo es válido cuando **Version** está establecido en **v2c**.

Haga clic en **OK**. El cuadro de diálogo **Create Trap Target** está cerrado.

Paso 5 Haga clic en **OK** para completar la configuración.

----Fin

8.5 Referencia de alarma (aplicable a versiones anteriores a MRS 3.x)

8.5.1 ALM-12001 Error de volcado del registro de auditoría (Para MRS 2.*x* o anterior)

Descripción

Los registros de auditoría de clúster deben volcarse en un servidor de terceros debido a la política de copia de respaldo de datos históricos locales. Los registros de auditoría se pueden volcar correctamente si el servidor de volcado cumple las condiciones de configuración. Esta alarma se genera cuando el volcado del registro de auditoría falla porque el espacio en disco del directorio de volcado en el servidor de terceros es insuficiente o un usuario cambia el nombre de usuario, la contraseña o el directorio de volcado del servidor de volcado.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
12001	Menor	Sí

Parámetros

Parámetro	Descripción
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

El sistema solo puede almacenar un máximo de 50 archivos de volcado localmente. Si el error persiste en el servidor de volcado, es posible que se pierda el registro de auditoría local.

Causas posibles

- La conexión de red es anormal.
- El nombre de usuario, contraseña o directorio de volcado del servidor de volcado no cumple las condiciones de configuración.
- El espacio en disco del directorio de volcado es insuficiente.

Procedimiento

Paso 1 Compruebe si el nombre de usuario, la contraseña y el directorio de volcado son correctos.

1. Compruebe en la página de configuración de volcado de MRS Manager para ver si son correctos.
   - En caso afirmativo, vaya a **Paso 3**.
   - Si no, vaya a **Paso 1.2**.
2. Cambie el nombre de usuario, la contraseña o el directorio de volcado y haga clic en **OK**.
3. Espere 2 minutos y compruebe si la alarma está desactivada.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 2**.

Paso 2 Restablezca la regla de volcado.

1. En MRS Manager, seleccione **System** > **Dump Audit Log**.
2. Reinicie las reglas de volcado, establezca los parámetros correctamente y haga clic en **OK**.
3. Espere 2 minutos y compruebe si la alarma está desactivada.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 3**.

Paso 3 Recopilar información de fallas.

1. En MRS Manager, seleccione **System** > **Export Log**.
2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Referencia

N/A

8.5.2 ALM-12002 Recurso de HA anormal (para MRS 2.*x* o anterior)

Descripción

El software de alta disponibilidad (HA) comprueba periódicamente las direcciones IP flotantes de WebService y las bases de datos de Manager. Esta alarma se genera cuando el software de HA detecta que las direcciones IP flotantes de WebService o las bases de datos son anormales.

Esta alarma se borra cuando el software de HA detecta que las direcciones IP flotantes o bases de datos son normales.

Atributo

ID de alarma	Gravedad de alarma	Borrar automáticamente
12002	Grave	Sí

Parámetro

Parámetro	Descripción
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
RESName	Especifica el recurso para el que se genera la alarma.

Impacto en el sistema

Si las direcciones IP flotantes de WebService de Manager son anormales, los usuarios no pueden iniciar sesión ni usar Manager. Si las bases de datos de Manager son anormales, todos los servicios básicos y los procesos de servicio relacionados, como las alarmas y las funciones de monitoreo, se ven afectados.

Causas posibles

- La dirección IP flotante es anormal.
- El estado de la base de datos es anormal.

Procedimiento

Paso 1 Compruebe el estado de la dirección IP flotante del nodo de gestión activo.

1. Vaya a la página de detalles del clúster de MRS. En la lista de alarmas de la página de pestaña de gestión de alarmas, haga clic en la fila que contiene la alarma. En los detalles de la alarma, vea la dirección del host y el nombre del recurso de la alarma.
2. Inicie sesión en el nodo de gestión activo. Ejecute los siguientes comandos para cambiar el usuario:

   sudo su - root

   su - omm
3. Vaya al directorio **${BIGDATA_HOME}/om-0.0.1/sbin/**, ejecute el script **status-oms.sh** para comprobar si la dirección IP flotante del Manager activo es normal. Vea la salida del comando, localice la fila donde **ResName** es **floatip** y compruebe si se muestra la siguiente información.

   Ejemplo:


```
10-10-10-160 floatip Normal Normal Single_active
```

- En caso afirmativo, vaya a **Paso 2**.
- Si no, vaya a **Paso 1.4**.

4. Póngase en contacto con el personal de O&M para comprobar si existe la NIC de IP flotante.
   - En caso afirmativo, vaya a **Paso 2**.
   - Si no, vaya a **Paso 1.5**.
5. Póngase en contacto con el personal de O&M para rectificar la falla de NIC.

   Espere 5 minutos y compruebe si la alarma está desactivada.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 2**.

Paso 2 Compruebe el estado de la base de datos de los nodos de gestión activo y en espera.

1. Inicie sesión en los nodos de gestión activos y en espera, ejecute los comandos **sudo su - root** y **su - ommdba** para cambiar a **ommdba** de usuario y ejecute el comando **gs_ctl query** para comprobar si se muestra la siguiente información en la salida del comando.

   Salida del comando del nodo de gestión activo:

   ```
   Ha state:
   LOCAL_ROLE: Primary
   STATIC_CONNECTIONS: 1
   DB_STATE: Normal
   DETAIL_INFORMATION: user/password invalid
    Senders info:
   No information
    Receiver info:
   No information
   ```

   Salida del comando del nodo de gestión en espera:

   ```
   Ha state:
   LOCAL_ROLE: Standby
   STATIC_CONNECTIONS: 1
   DB_STATE : Normal
   DETAIL_INFORMATION: user/password invalid
    Senders info:
   No information
    Receiver info:
   No information
   ```

   - En caso afirmativo, vaya a **Paso 2.3**.
   - Si no, vaya a **Paso 2.2**.
2. Póngase en contacto con el personal de O&M para comprobar si se produce una falla de red y rectificar la falla.
   - En caso afirmativo, vaya a **Paso 2.3**.
   - Si no, vaya a **Paso 3**.
3. Espere 5 minutos y compruebe si la alarma está desactivada.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 3**.

Paso 3 Recopilar información de fallas.

1. En MRS Manager, seleccione **System** > **Export Log**.
2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Referencia

Ninguna

8.5.3 ALM-12004 Recurso OLdap anormal (Para MRS 2.*x* o anterior)

Descripción

Esta alarma se genera cuando el recurso Ldap en Manager es anormal.

Esta alarma se borra cuando se recupera el recurso Ldap en Manager y se completa el manejo de alarmas.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
12004	Grave	Sí

Parámetro

Parámetro	Descripción
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

Los servicios de autenticación de Manager no están disponibles y no pueden proporcionar funciones de autenticación de seguridad y gestión de usuarios para los servicios web de capa superior. Es posible que los usuarios no puedan iniciar sesión en Manager.

Causas posibles

El proceso LdapServer en Manager es anormal.

Procedimiento

Paso 1 Compruebe si el proceso LdapServer en Manager es normal.

1. Inicie sesión en el nodo de gestión activo.

2. Ejecute **ps -ef | grep slapd** para comprobar si el proceso de recursos LdapServer en el directorio **${BIGDATA_HOME}/om-0.0.1/** del archivo de configuración se está ejecutando correctamente.

   Puede determinar que el recurso es normal de la siguiente manera:

   a. Ejecute **sh ${BIGDATA_HOME}/om-0.0.1/sbin/status-oms.sh** y encuentre que el **ResHAStatus** del proceso OLdap es **Normal**.

   b. Ejecute **ps -ef | grep slapd** y encuentre que el proceso de slapd ocupa el puerto 21750.

   – En caso afirmativo, vaya a **Paso 2**.

   – Si no, vaya a **Paso 3**.

Paso 2 Ejecute **kill -2** *PID of the LdapServer process* y espere 20 segundos. El HA inicia el proceso OLdap automáticamente. Compruebe si el estado del recurso OLdap es normal.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 3**.

Paso 3 Recopilar información de fallas.

1. En MRS Manager, seleccione **System** > **Export Log**.
2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Referencia

Ninguna

8.5.4 ALM-12005 Recursos de OKerberos anormales (Para MRS 2.*x* o anterior)

Descripción

El módulo de alarma monitorea el estado del recurso de Kerberos en Manager. Esta alarma se genera cuando el recurso de Kerberos es anormal.

Esta alarma se borra cuando se completa la gestión de alarmas y se recupera el estado del recurso de Kerberos.

Atributo

ID de alarma	Gravedad de alarma	Borrar automáticamente
12005	Grave	Sí

Parámetros

Parámetro	Descripción
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

Los servicios de autenticación no están disponibles y no pueden proporcionar funciones de autenticación de seguridad para los servicios web de capa superior. Es posible que los usuarios no puedan iniciar sesión en MRS Manager.

Causas posibles

El recurso de OLdap del que depende OKerberos es anormal.

Procedimiento

Paso 1 Compruebe si el recurso OLdap del que depende OKerberos es anormal en Manager.

1. Inicie sesión en el nodo de gestión activo.
2. Ejecute el siguiente comando para comprobar si el recurso de OLdap gestionado por HA es normal:

   sh ${BIGDATA_HOME}/OMSV100R001C00x8664/workspace0/ha/module/hacom/script/status_ha.sh

   El recurso OLdap es normal cuando el recurso OLdap está en el estado **Active_normal** en el nodo activo y en el estado **Standby_normal** en el nodo de espera.

   – En caso afirmativo, vaya a **Paso 3**.

   – Si no, vaya a **Paso 2**.

Paso 2 Resuelva el problema siguiendo las instrucciones en **ALM-12004 Recurso OLdap anormal (Para MRS 2.x o anterior)**. Después de recuperar el estado del recurso de OLdap, compruebe si el recurso de OKerberos es normal.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 3**.

Paso 3 Recopilar información de fallas.

1. En MRS Manager, seleccione **System** > **Export Log**.
2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Referencia

Ninguna

8.5.5 ALM-12006 Falla de nodo (para MRS 2.*x* o anterior)

Descripción

Controller comprueba el estado del NodeAgent cada 30 segundos. Esta alarma se genera cuando Controller no recibe el informe de estado de un NodeAgent tres veces consecutivas.

Esta alarma se borra cuando el Controller puede recibir correctamente el informe de estado del NodeAgent.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
12006	Crítica	Sí

Parámetros

Parámetro	Descripción
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

Los servicios del nodo no están disponibles.

Causas posibles

La red está desconectada o el hardware está defectuoso.

Procedimiento

Paso 1 Compruebe si la red está desconectada o si el hardware está defectuoso.

1. Vaya a la página de detalles del clúster de MRS. En la lista de alarmas de la página de pestaña de gestión de alarmas, haga clic en la fila que contiene la alarma. En los detalles de la alarma, vea la dirección del host de la alarma.
2. Inicie sesión en el nodo de gestión activo.

3. Ejecute el siguiente comando para comprobar si el nodo defectuoso es accesible:

   ping *IP address of the faulty host*

   a. En caso afirmativo, vaya a **Paso 2**.

   b. Si no, vaya a **Paso 1.4**.

4. Póngase en contacto con el personal de O&M para comprobar si la red es defectuosa.
   - En caso afirmativo, vaya a **Paso 2**.
   - Si no, vaya a **Paso 1.6**.

5. Rectifique la falla de la red y compruebe si la alarma está borrada de la lista de alarmas.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 1.6**.

6. Póngase en contacto con el personal de O&M para comprobar si se produce una falla de hardware (por ejemplo, un fallo de CPU o de memoria) en el nodo.
   - En caso afirmativo, vaya a **Paso 1.7**.
   - Si no, vaya a **Paso 2**.

7. Repare los componentes defectuosos y reinicie el nodo. Verifique si la alarma se ha borrado.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 2**.

Paso 2 Recopile información de fallas.

1. En MRS Manager, seleccione **System** > **Export Log**.
2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Referencia

Ninguna

8.5.6 ALM-12007 Falla de proceso (Para MRS 2.*x* o anterior)

Descripción

El módulo de comprobación de estado del proceso comprueba el estado del proceso cada 5 segundos. Esta alarma se genera cuando el módulo de comprobación de estado del proceso detecta que el estado de conexión del proceso es Bad durante tres veces consecutivas.

Esta alarma se borra cuando se puede conectar el proceso.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
12007	Grave	Sí

Parámetros

Parámetro	Descripción
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

El servicio proporcionado por el proceso no está disponible.

Causas posibles

- El proceso de instancia es anormal.
- El espacio en la unidad es insuficiente.

Procedimiento

Paso 1 Compruebe si el proceso de instancia es anormal.

1. Vaya a la página de detalles del clúster de MRS. En la lista de alarmas de la página de pestaña de gestión de alarmas, haga clic en la fila que contiene la alarma. En los detalles de la alarma, vea el nombre del host y el nombre del servicio de la alarma.
2. En la página **Alarms**, compruebe si se ha generado el **ALM-12006 Falla de nodo (para MRS 2.x o anterior)** de alarma.

   En caso afirmativo, vaya a **Paso 1.3**.

   Si no, vaya a **Paso 1.4**.
3. Maneje la alarma siguiendo las instrucciones en **ALM-12006 Falla de nodo (para MRS 2.x o anterior)**.
4. Compruebe si el usuario del directorio de instalación, el grupo de usuarios y el permiso del rol de alarma son correctos. El usuario correcto, el grupo de usuarios y el permiso son **omm**, **ficommon** y **750** respectivamente.
   - En caso afirmativo, vaya a **Paso 1.6**.
   - Si no, vaya a **Paso 1.5**.
5. Ejecute los siguientes comandos para establecer el permiso para **750** y **User:Group** para **omm:ficommon**:

   chmod 750 <*folder_name*>

   chown omm:ficommon <*folder_name*>
6. Espere 5 minutos y compruebe si la ALM-12007 Alarma de falla de proceso está desactivada.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 2.1**.

Paso 2 Compruebe si el espacio en disco es insuficiente.

1. En la página de detalles del clúster MRS, haga clic en la pestaña de gestión de alarmas y compruebe si ALM-12017 Capacidad de disco insuficiente se genera en la lista de alarmas.
   - En caso afirmativo, vaya a **Paso 2.2**.
   - Si no, vaya a **Paso 3**.
2. Maneje la alarma siguiendo las instrucciones en **ALM-12017 Capacidad de disco insuficiente (para MRS 2.x o anterior)**.
3. Espere 5 minutos y compruebe si la alarma de capacidad de disco insuficiente ALM-12017 está desactivada.

   En caso afirmativo, vaya a **Paso 2.4**.

   Si no, vaya a **Paso 3**.
4. Espere 5 minutos y compruebe si la alarma está desactivada.

   En caso afirmativo, no es necesario hacer nada más.

   Si no, vaya a **Paso 3**.

Paso 3 Recopilar información de fallas.

1. En MRS Manager, seleccione **System** > **Export Log**.
2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Referencia

Ninguna

8.5.7 ALM-12010 Interrupción del latido del Manager entre los nodos activo y en espera (para MRS 2.*x* o anterior)

Descripción

Esta alarma se genera cuando el Manager activo no recibe ninguna señal de latido del Manager en espera en 7 segundos.

Esta alarma se borra cuando el Manager activo recibe señales de latidos del Manager en espera.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
12010	Grave	Sí

Parámetros

Parámetro	Descripción
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Local Manager HA Name	Especifica un Manager HA local.
Peer Manager HA Name	Especifica un Manager HA del mismo nivel.

Impacto en el sistema

Cuando el proceso activo de Manager es anormal, no se puede realizar una conmutación por error activa/en espera y los servicios se ven afectados.

Causas posibles

El vínculo entre los servidores de Manager activo y en espera es anormal.

Procedimiento

Paso 1 Compruebe si la red entre los servidores de Manager activo y en espera es normal.

1. Vaya a la página de detalles del clúster de MRS. En la lista de alarmas de la página de pestaña de gestión de alarmas, haga clic en la fila que contiene la alarma. En los detalles de la alarma, vea la dirección del servidor de Manager en espera.
2. Inicie sesión en el nodo de gestión activo.
3. Ejecute el siguiente comando para comprobar si el Manager en espera es accesible:

   ping *heartbeat IP address of the standby Manager*

   – En caso afirmativo, vaya a **Paso 2**.
   – Si no, vaya a **Paso 1.4**.
4. Póngase en contacto con el personal de O&M para comprobar si la red es defectuosa.
   – En caso afirmativo, vaya a **Paso 1.5**.
   – Si no, vaya a **Paso 2**.
5. Rectifique la falla de la red y compruebe si la alarma está borrada de la lista de alarmas.
   – En caso afirmativo, no es necesario hacer nada más.
   – Si no, vaya a **Paso 2**.

Paso 2 Inicie sesión en todos los nodos de master del clúster y ejecute los siguientes comandos para buscar todos los archivos **sed***xxx* y eliminarlos:

find /srv/BigData/ -name "sed*"

find /opt -name "sed*"

Paso 3 Recopile información de fallas.

1. En MRS Manager, seleccione **System** > **Export Log**.
2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Referencia

Ninguna

8.5.8 ALM-12011 Excepción de sincronización de datos de entre los nodos activos y en espera de Manager (Para MRS 2.*x* o anterior)

Descripción

Esta alarma se genera cuando el Manager en espera no puede sincronizar archivos con el Manager activo.

Esta alarma se borra cuando el Manager en espera sincroniza los archivos con el Manager activo.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
12011	Crítica	Sí

Parámetros

Parámetro	Descripción
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Local Manager HA Name	Especifica un Manager HA local.
Peer Manager HA Name	Especifica un Manager HA del mismo nivel.

Impacto en el sistema

Debido a que los archivos de configuración del Manager en espera no se actualizan, algunas configuraciones se perderán después de una conmutación activa/en espera. Es posible que Manager y algunos componentes no se ejecuten correctamente.

Causas posibles

Se interrumpe el vínculo entre los nodos del Manager activo y en espera.

Procedimiento

Paso 1 Compruebe si la red entre los servidores de Manager activo y en espera es normal.

1. Vaya a la página de detalles del clúster de MRS. En la lista de alarmas de la página de pestaña de gestión de alarmas, haga clic en la fila que contiene la alarma. En los detalles de la alarma, vea la dirección del servidor de Manager en espera.
2. Inicie sesión en el nodo de gestión activo. Ejecute el siguiente comando para comprobar si el Manager en espera es accesible:

   ping *IP address of the standby Manager*

   – En caso afirmativo, vaya a **Paso 2**.

   – Si no, vaya a **Paso 1.3**.
3. Póngase en contacto con el personal de O&M para comprobar si la red es defectuosa.

   – En caso afirmativo, vaya a **Paso 1.4**.

   – Si no, vaya a **Paso 2**.
4. Rectifique la falla de la red y compruebe si la alarma está borrada de la lista de alarmas.

   – En caso afirmativo, no es necesario hacer nada más.

   – Si no, vaya a **Paso 2**.

Paso 2 Recopilar información de fallas.

1. En MRS Manager, seleccione **System** > **Export Log**.
2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Referencia

Ninguna

8.5.9 ALM-12012 NTP Servicio anormal (Para MRS 2.*x* o anterior)

Descripción

Esta alarma se genera cuando el servicio NTP en el nodo actual no puede sincronizar el tiempo con el servicio NTP en el nodo OMS activo.

Esta alarma se borra cuando el servicio NTP en el nodo actual sincroniza el tiempo correctamente con el servicio NTP en el nodo OMS activo.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
12012	Grave	Sí

Parámetros

Parámetro	Descripción
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

El tiempo en el nodo es inconsistente con el de otros nodos del clúster. Por lo tanto, algunas aplicaciones de MRS en el nodo pueden no ejecutarse correctamente.

Causas posibles

- El servicio NTP en el nodo actual no puede iniciarse correctamente.
- El nodo actual no puede sincronizar la hora con el servicio NTP en el nodo OMS activo.
- El valor de clave autenticado por el servicio NTP en el nodo actual es incompatible con el del nodo OMS activo.
- El desplazamiento de tiempo entre el nodo y el servicio NTP en el nodo OMS activo es grande.

Procedimiento

Paso 1 Compruebe el servicio NTP en el nodo actual.

1. Compruebe si el proceso ntpd se está ejecutando en el nodo mediante el siguiente método. Inicie sesión en el nodo para el que se genera la alarma y ejecute el comando **sudo su - root** para cambiar a usuario **root**. A continuación, ejecute el siguiente comando para comprobar si la salida del comando contiene el proceso ntpd:

   ps -ef | grep ntpd | grep -v grep

   – En caso afirmativo, vaya a **Paso 2.1**.

   – Si no, vaya a **Paso 1.2**.
2. Ejecute **service ntp start** para iniciar el servicio NTP.
3. Espere 10 minutos y compruebe si la alarma está desactivada.

   – En caso afirmativo, no es necesario hacer nada más.

   – Si no, vaya a **Paso 2.1**.

Paso 2 Compruebe si el nodo actual puede sincronizar la hora correctamente con el servicio NTP en el nodo OMS activo.

1. Compruebe si el nodo puede sincronizar la hora con el servicio NTP en el nodo OMS activo basado en información adicional de la alarma.

   En caso afirmativo, vaya a **Paso 2.2**.

   Si no, vaya a **Paso 3**.

2. Compruebe si la sincronización con el servicio NTP en el nodo OMS activo es defectuosa.

   Inicie sesión en el nodo para el que se genera la alarma, ejecute el comando **sudo su - root** para cambiar a usuario **root** y ejecute el comando **ntpq -np**.

   Si existe un asterisco (*) antes de la dirección IP del servicio NTP en el nodo OMS activo en la salida del comando, la sincronización está en estado normal. La salida de comandos es la siguiente:

   ```
   remote refid st t when poll reach delay offset jitter
   ==============================================================================
   *10.10.10.162 .LOCL. 1 u 1 16 377 0.270 -1.562 0.014
   ```

   Si no hay un asterisco (*) antes de la dirección IP del servicio NTP en el nodo OMS activo, como se muestra en la siguiente salida del comando, y el valor de **refid** es de **.INIT.**, la sincronización es anormal.

   ```
   remote refid st t when poll reach delay offset jitter
   ==============================================================================
   10.10.10.162 .INIT. 1 u 1 16 377 0.270 -1.562 0.014
   ```

   – En caso afirmativo, vaya a **Paso 2.3**.
   – Si no, vaya a **Paso 3**.

3. Rectifique la falla, espere 10 minutos y luego compruebe si la alarma está desactivada.

   Una falla de sincronización de NTP generalmente está relacionado con el firewall del sistema. Si se puede desactivar el firewall, desactívelo y compruebe si se ha rectificado la falla. Si el firewall no se puede deshabilitar, compruebe las políticas de configuración del firewall y asegúrese de que el puerto **UDP 123** está habilitado (necesita seguir las políticas de configuración de firewall específicas de cada sistema).

   – En caso afirmativo, no es necesario hacer nada más.
   – Si no, vaya a **Paso 3**.

Paso 3 Compruebe si el valor de clave autenticado por el servicio NTP en el nodo actual es consistente con el del nodo OMS activo.

Ejecute **cat /etc/ntp.keys** para comprobar si el código de autenticación cuyo índice de valor de clave es 1 es el mismo que el valor del servicio NTP en el nodo OMS activo.

- En caso afirmativo, vaya a **Paso 4.1**.
- Si no, vaya a **Paso 5**.

Paso 4 Compruebe si el desfase de tiempo entre el nodo y el servicio NTP en el nodo OMS activo es grande.

1. Compruebe si el desplazamiento de tiempo es grande en la información adicional de la alarma.

   – En caso afirmativo, vaya a **Paso 4.2**.
   – Si no, vaya a **Paso 5**.

2. En la página **Hosts**, seleccione el host del nodo y elija **More** > **Stop All Roles** para detener todos los servicios del nodo.

   Si el tiempo en el nodo de alarma es posterior al del servicio NTP del nodo OMS activo, ajuste el tiempo del nodo de alarma. Después de ajustar el tiempo, elija **More** > **Start All Roles** para iniciar los servicios en el nodo.

   Si el tiempo en el nodo de alarma es anterior al del servicio NTP del nodo OMS activo, espere hasta que se deba el desplazamiento de tiempo y ajuste el tiempo del nodo de alarma. Después de ajustar el tiempo, elija **More** > **Start All Roles** para iniciar los servicios en el nodo.

NOTA

Si no espera, puede ocurrir la pérdida de datos.

3. Espere 10 minutos y compruebe si la alarma está desactivada.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 5**.

Paso 5 Recopilar información de fallas.

1. En MRS Manager, seleccione **System** > **Export Log**.
2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Referencia

Ninguna

8.5.10 ALM-12014 Partición de dispositivo perdida (Para MRS 2.*x* o anterior)

Descripción

Esta alarma se genera cuando el sistema detecta que se ha perdido una partición en la que se montan los directorios de servicio (porque el dispositivo se quita o se desconecta, o la partición se elimina). El sistema comprueba periódicamente el estado de la partición.

Esta alarma necesita ser borrada manualmente.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
12014	Grave	No

Parámetros

Parámetro	Descripción
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
DirName	Especifica el directorio para el que se genera la alarma.

Parámetro	Descripción
PartitionName	Especifica la partición de dispositivo para la que se genera la alarma.

Impacto en el sistema

Los datos de servicio no se pueden escribir en la partición y el sistema de servicio se ejecuta de forma anormal.

Causas posibles

- Se quita el disco.
- El disco está sin conexión o existe un sector defectuoso en el disco.

Procedimiento

Paso 1 Vaya a la página de detalles del clúster de MRS y elija **Alarms**.

Paso 2 En la lista de alarmas en tiempo real, haga clic en la fila que contiene la alarma.

Paso 3 En el área **Alarm Details**, obtenga los valores de **HostName**, **PartitionName** y **DirName** de **Location**.

Paso 4 Compruebe si el disco correspondiente a **PartitionName** de **HostName** está insertado en la ranura del servidor correcta.

- En caso afirmativo, vaya a **Paso 5**.
- Si no, vaya a **Paso 6**.

Paso 5 Póngase en contacto con los ingenieros de hardware para quitar el disco defectuoso.

Paso 6 Utilice PuTTY para iniciar sesión en el nodo **HostName** donde se reporta una alarma y verifique si hay una línea que contenga **DirName** en el archivo **/etc/fstab**.

- En caso afirmativo, vaya a **Paso 7**.
- Si no, vaya a **Paso 8**.

Paso 7 Ejecute el comando **vi /etc/fstab** para editar el archivo y eliminar la línea que contiene **DirName**.

Paso 8 Póngase en contacto con los ingenieros de hardware para insertar un nuevo disco. Para obtener más información, consulte el documento del producto de hardware del modelo correspondiente. Si el disco defectuoso está en un grupo RAID, configure el grupo RAID. Para obtener más información, consulte los métodos de configuración de la tarjeta controladora de RAID relevante.

Paso 9 Espere de 20 a 30 minutos (el tamaño del disco determina el tiempo de espera) y ejecute el comando **mount** para comprobar si el disco se ha montado en el directorio **DirName**.

- En caso afirmativo, borre la alarma manualmente. No se requiere ninguna operación adicional.
- Si no, vaya a **Paso 10**.

Paso 10 Recopilar información de fallas.

1. En MRS Manager, seleccione **System** > **Export Log**.
2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Referencia

Ninguna

8.5.11 ALM-12015 Sistema de archivos de partición de dispositivo de solo lectura (para MRS 2.*x* o anterior)

Descripción

Esta alarma se genera cuando el sistema detecta que una partición en la que están montados los directorios de servicio entra en el modo de solo lectura (debido a un sector defectuoso o a un sistema de archivos defectuoso). El sistema comprueba periódicamente el estado de la partición.

Esta alarma se borra cuando el sistema detecta que la partición en la que se montan los directorios de servicio sale del modo de solo lectura (debido a que el sistema de archivos se restaura al modo de lectura/escritura, se quita el dispositivo o se formatea el dispositivo).

Atributo

ID de alarma	Gravedad de alarma	Borrar automáticamente
12015	Grave	Sí

Parámetros

Parámetro	Descripción
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
DirName	Especifica el directorio para el que se genera la alarma.
PartitionName	Especifica la partición de dispositivo para la que se genera la alarma.

Impacto en el sistema

Los datos de servicio no se pueden escribir en la partición y el sistema de servicio se ejecuta de forma anormal.

Causas posibles

El disco está defectuoso, por ejemplo, existe un sector defectuoso.

Procedimiento

Paso 1 Vaya a la página de detalles del clúster de MRS y elija **Alarms**.

Paso 2 En la lista de alarmas en tiempo real, haga clic en la fila que contiene la alarma.

Paso 3 En el área **Alarm Details**, obtenga **HostName** y **PartitionName** de **Location**. **HostName** indica el nodo para el que se genera la alarma, y **PartitionName** indica la partición del disco defectuoso.

Paso 4 Póngase en contacto con los ingenieros de hardware para comprobar si el disco está defectuoso. Si el disco está defectuoso, elimínelo del servidor.

Paso 5 Después de quitar el disco, el sistema informa de ALM-12014 Partición perdida. Maneje la alarma siguiendo las instrucciones en **ALM-12014 Partición de dispositivo perdida (Para MRS 2.x o anterior)**. Después de la manipulación, la alarma se borra automáticamente.

----Fin

Referencia

Ninguna

8.5.12 ALM-12016 El uso de CPU supera el umbral (Para MRS 2.*x* o anterior)

Descripción

El sistema comprueba el uso de la CPU cada 30 segundos y compara el resultado de la comprobación con el umbral predeterminado. El uso de la CPU tiene un umbral predeterminado. Esta alarma se genera cuando el uso de la CPU excede el umbral varias veces (configurable, 10 veces por defecto) consecutivamente.

Esta alarma se borra cuando el uso promedio de CPU es menor o igual al 90% del umbral.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
12016	Grave	Sí

Parámetros

Parámetro	Descripción
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger Condition	Genera una alarma cuando el valor real del indicador excede el umbral especificado.

Impacto en el sistema

Los procesos responden lentamente o no funcionan.

Causas posibles

- El umbral de alarma o el número de acierto de alarma está configurado incorrectamente.
- La configuración de la CPU no puede cumplir los requisitos de servicio. El uso de la CPU alcanza el límite superior.

Procedimiento

Paso 1 Compruebe si el umbral de alarma o el número de acierto de alarma están configurados correctamente.

1. Inicie sesión en MRS Manager y cambie el umbral de alarma y el número de aciertos de alarma según el uso de CPU.
2. Elija **System** > **Threshold Configuration** > **Device** > **Host** > **CPU** > **CPU Usage** > **CPU Usage** y cambie el umbral de alarma basado en el uso real de CPU.
3. Elija **System** > **Threshold Configuration** > **Device** > **Host** > **CPU** > **CPU Usage** > **CPU Usage** y cambie **hit number** según el uso real de la CPU.

   NOTA

   Esta opción define la fase de comprobación de alarma. **Interval** indica el período de comprobación de alarma y **hit number** indica el número de veces que el uso de CPU excede el umbral. Se genera una alarma cuando el uso de la CPU excede el umbral varias veces consecutivamente.
4. Espere 2 minutos y compruebe si la alarma se borra automáticamente.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 2**.

Paso 2 Expanda el sistema.

1. Vaya a la página de detalles del clúster de MRS. En la lista de alarmas de la página de pestaña de gestión de alarmas, haga clic en la fila que contiene la alarma. En los detalles de la alarma, vea la dirección del nodo.

2. Inicie sesión en el nodo para el que se genera la alarma.
3. Ejecute **cat /proc/stat | awk 'NR==1'|awk '{for(i=2;i<=NF;i++)j+=$i;print "" 100 - ($5+$6) * 100 / j;}'** para comprobar el uso de la CPU del sistema.
4. Si el uso de la CPU excede el umbral, expanda la capacidad de la CPU.
5. Verifique si la alarma se ha borrado.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 3**.

Paso 3 Recopilar información de fallas.

1. En MRS Manager, seleccione **System** > **Export Log**.
2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Referencia

Ninguna

8.5.13 ALM-12017 Capacidad de disco insuficiente (para MRS 2.*x* o anterior)

Descripción

El sistema comprueba el uso del disco host cada 30 segundos y compara el uso real del disco con el umbral. El uso del disco tiene un umbral predeterminado. Esta alarma se genera si el uso del disco excede el umbral.

Para cambiar el umbral, elija **System** >**Threshold Configuration**.

Esta alarma se borra cuando el uso del disco host es menor o igual que el umbral.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
12017	Grave	Sí

Parámetros

Parámetro	Descripción
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Parámetro	Descripción
PartitionName	Especifica la partición de disco para la que se genera la alarma.
Trigger Condition	Genera una alarma cuando el valor real del indicador excede el umbral especificado.

Impacto en el sistema

Los procesos de servicio no están disponibles.

Causas posibles

La configuración del disco no puede cumplir los requisitos de servicio. El uso del disco alcanza el límite superior.

Procedimiento

Paso 1 Inicie sesión en MRS Manager y compruebe si el umbral es apropiado.

1. El umbral predeterminado es 90%. Puede cambiar el umbral para cumplir con los requisitos de servicio.
   - En caso afirmativo, vaya a **Paso 2**.
   - Si no, vaya a **Paso 1.2**.
2. Elija **System** > **Threshold Configuration** y cambie el umbral de alarma en función del uso real del disco.
3. Espere 2 minutos y compruebe si la alarma está desactivada.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 2**.

Paso 2 Compruebe si el disco es un disco del sistema.

1. Vaya a la página de detalles del clúster de MRS. En la lista de alarmas de la página de pestaña de gestión de alarmas, haga clic en la fila que contiene la alarma. En los detalles de la alarma, vea el nombre del host y la información de la partición del disco.
2. Inicie sesión en el nodo para el que se genera la alarma.
3. Ejecute el comando **df -h** para comprobar el uso de la partición del disco del sistema. Compruebe si el disco está montado en cualquiera de los siguientes directorios utilizando el nombre de partición de disco obtenido en las versiones **Paso 2.1**: **/**, **/boot**, **/home**, **/opt**, **/tmp**, **/var**, **/var/log**, **/boot** y **/srv/BigData**.
   - En caso afirmativo, el disco es un disco del sistema. Entonces vaya a **Paso 3.1**.
   - Si no, el disco no es un disco del sistema. Entonces vaya a **Paso 2.4**.
4. Ejecute el comando **df -h** para comprobar el uso de la partición del disco del sistema. Determine el rol del disco basado en el nombre de la partición de disco obtenido en **Paso 2.1**.
5. Compruebe si el disco es utilizado por HDFS o Yarn.
   - Si es así, expanda la capacidad del disco para el nodo Core. Entonces vaya a **Paso 2.6**.

- Si no, vaya a **Paso 4**.

6. Espere 2 minutos y compruebe si la alarma está desactivada.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 3**.

Paso 3 Compruebe si los archivos grandes están escritos en el disco.

1. Ejecute el comando **find / -xdev -size +500M -exec ls -l {} \;** para ver archivos de más de 500 MB en el nodo. Compruebe si dichos archivos están escritos en el disco.
   - En caso afirmativo, vaya a **Paso 3.2**.
   - Si no, vaya a **Paso 4**.
2. Maneje los archivos grandes y compruebe si la alarma se borra 2 minutos después.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 4**.
3. Amplíe la capacidad del disco.
4. Espere 2 minutos y compruebe si la alarma está desactivada.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 4**.

Paso 4 Recopile información de fallas.

1. En MRS Manager, seleccione **System** > **Export Log**.
2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Referencia

Ninguna

8.5.14 ALM-12018 El uso de memoria supera el umbral (Para MRS 2.*x* o anterior)

Descripción

El sistema comprueba el uso de la memoria cada 30 segundos y compara el uso real de la memoria con el umbral. El uso de memoria tiene un umbral predeterminado. Esta alarma se genera cuando el uso de memoria detectado excede el umbral.

Esta alarma se borra cuando el uso de la memoria del host es menor o igual al 90% del umbral.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
12018	Grave	Sí

Parámetros

Parámetro	Descripción
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger Condition	Genera una alarma cuando el valor real del indicador excede el umbral especificado.

Impacto en el sistema

Los procesos responden lentamente o no funcionan.

Causas posibles

La configuración de la memoria no puede cumplir con los requisitos de servicio. El uso de memoria alcanza el umbral superior.

Procedimiento

Paso 1 Expanda el sistema.

1. Vaya a la página de detalles del clúster de MRS. En la lista de alarmas de la página de pestaña de gestión de alarmas, haga clic en la fila que contiene la alarma. En los detalles de la alarma, vea la dirección del host de la alarma.
2. Inicie sesión en el nodo para el que se genera la alarma.
3. Ejecute **free -m | grep Mem\: | awk '{printf("%s,", ($3-$6-$7) * 100 / $2)}'** para comprobar el uso de la memoria del sistema.
4. Si el uso de memoria excede el umbral, amplíe la capacidad de memoria.
5. Espere 5 minutos y compruebe si la alarma está desactivada.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 2**.

Paso 2 Recopilar información de fallas.

1. En MRS Manager, seleccione **System** > **Export Log**.
2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Referencia

Ninguna

8.5.15 ALM-12027 El uso de PID de host supera el umbral (para MRS 2.*x* o anterior)

Descripción

El sistema comprueba el uso del PID cada 30 segundos y compara el uso real del PID con el umbral predeterminado. Esta alarma se genera cuando el uso del PID excede el umbral.

Esta alarma se borra cuando el uso del PID del host es menor o igual que el umbral.

Atributo

ID de alarma	Gravedad de alarma	Borrar automáticamente
12027	Grave	Sí

Parámetros

Parámetro	Descripción
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger Condition	Genera una alarma cuando el valor real del indicador excede el umbral especificado.

Impacto en el sistema

No hay ningún PID disponible para los nuevos procesos y los procesos de servicio no están disponibles.

Causas posibles

Se están ejecutando demasiados procesos en el nodo. Necesita aumentar el valor de **pid_max**. El sistema no funciona normalmente.

Procedimiento

Paso 1 Aumenta el valor de **pid_max**.

1. En la página de detalles del clúster MRS, haga clic en la alarma de la lista de alarmas en tiempo real. En el área **Alarm Details**, obtenga la dirección IP del host para el que se genera la alarma.

2. Inicie sesión en el nodo para el que se genera la alarma.
3. Ejecute el comando **cat /proc/sys/kernel/pid_max** para comprobar el valor de **pid_max**.
4. Si el uso de PID excede el umbral, ejecute el siguiente comando para duplicar el valor de **pid_max**:

   echo *New pid_max value* **> /proc/sys/kernel/pid_max**

   Ejemplo:

   echo 65536 > /proc/sys/kernel/pid_max

   NOTA

   El valor máximo de **pid_max** es el siguiente:
   - 32-bit OS: **32768**
   - 64-bit OS: **4194304** (22nd power of 2)
5. Espere 5 minutos y compruebe si la alarma está desactivada.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 2**.

Paso 2 Compruebe si el entorno del sistema es anormal.

1. Póngase en contacto con el personal de O&M para comprobar si el sistema operativo es anormal.
   - En caso afirmativo, rectifique la falla del sistema operativo y vaya a **Paso 2.2**.
   - Si no, vaya a **Paso 3**.
2. Espere 5 minutos y compruebe si la alarma está desactivada.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 3**.

Paso 3 Recopilar información de fallas.

1. En MRS Manager, seleccione **System** > **Export Log**.
2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Referencia

Ninguna

8.5.16 ALM-12028 Número de procesos en el Estado D en el host supera el umbral (Para MRS 2.*x* o anterior)

Descripción

El sistema comprueba periódicamente el número de procesos de estado D de usuario **omm** en el host cada 30 segundos y compara el número con el umbral. El número de procesos en el estado D en el host tiene un umbral predeterminado. Esta alarma se genera cuando el número de procesos en el estado D supera el umbral.

Esta alarma se borra cuando el número es menor o igual que el umbral.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
12028	Grave	Sí

Parámetros

Parámetro	Descripción
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger Condition	Genera una alarma cuando el valor real del indicador excede el umbral especificado.

Impacto en el sistema

Se utilizan recursos excesivos del sistema y el proceso de servicio responde lentamente.

Causas posibles

El host responde lentamente a las solicitudes de E/S (E/S de disco y E/S de red) y un proceso está en el estado D.

Procedimiento

Paso 1 Compruebe el proceso que está en el estado D.

1. Vaya a la página de detalles del clúster de MRS. En la lista de alarmas de la página de pestaña de gestión de alarmas, haga clic en la fila que contiene la alarma. En los detalles de la alarma, vea la dirección del host.
2. Inicie sesión en el nodo para el que se genera la alarma.
3. Ejecute los siguientes comandos para cambiar el usuario:

   sudo su - root

   su - omm
4. Ejecute el siguiente comando como usuario **omm** para ver el PID del proceso que está en estado D:

   ps -elf | grep -v "\[thread_checkio\]" | awk 'NR!=1 {print $2, $3, $4}' | grep omm | awk -F' ' '{print $1, $3}' | grep D | awk '{print $2}'
5. Compruebe si la salida del comando está vacía.
   - En caso afirmativo, el proceso de servicio se está ejecutando correctamente. Entonces vaya a **Paso 1.7**.

– Si no, vaya a **Paso 1.6**.

6. Cambie a usuario **root** y ejecute el comando **reboot** para reiniciar el host de alarma.

   Reiniciar el host conlleva ciertos riesgos. Asegúrese de que el proceso de servicio se ejecuta correctamente después del reinicio.

7. Espere 5 minutos y compruebe si la alarma está desactivada.
   – En caso afirmativo, no es necesario hacer nada más.
   – Si no, vaya a **Paso 2**.

Paso 2 Recopilar información de fallas.

1. En MRS Manager, seleccione **System** > **Export Log**.
2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Referencia

Ninguna

8.5.17 ALM-12031 Usuario omm o contraseña está a punto de caducar (Para MRS 2.*x* o anterior)

Descripción

El sistema comienza a las 00:00 todos los días para comprobar si el usuario **omm** y la contraseña están a punto de caducar cada ocho horas. Esta alarma se genera si el usuario o la contraseña están a punto de caducar en 15 días.

La alarma se borra cuando se cambia el período de validez del usuario **omm** o se restablece la contraseña y se completa el manejo de la alarma.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
12031	Menor	Sí

Parámetros

Parámetro	Descripción
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

La relación de confianza de nodo no está disponible y el administrador no puede gestionar los servicios.

Causas posibles

Usuario **omm** o la contraseña están a punto de caducar.

Procedimiento

Paso 1 Compruebe si usuario **omm** y la contraseña del sistema son válidas.

1. Inicie sesión en el nodo defectuoso.
2. Ejecute el siguiente comando para ver la información sobre usuario **omm** y la contraseña:

   chage -l omm
3. Compruebe si el usuario ha caducado según el mensaje del sistema.
   a. Vea el valor de **Password expires** para comprobar si la contraseña está a punto de caducar.
   b. Vea el valor de **Account expires** para comprobar si el usuario está a punto de caducar.

   NOTA

   Si el valor del parámetro es de **never**, el usuario y la contraseña son válidos permanentemente; si el valor es una fecha, compruebe si el usuario y la contraseña están a punto de caducar en un plazo de 15 días.

   – En caso afirmativo, vaya a **Paso 1.4**.
   – Si no, vaya a **Paso 2**.
4. Ejecute el siguiente comando para modificar la configuración del período de validez:
   – Ejecute el siguiente comando para establecer un período de validez para usuario **omm**:

     chage -E *'specified date'* **omm**
   – Ejecute el siguiente comando para establecer el número de días de validez para usuario **omm**:

     chage -M *'number of days'* **omm**
5. Compruebe si la alarma se borra automáticamente en la siguiente comprobación periódica.
   – En caso afirmativo, no es necesario hacer nada más.
   – Si no, vaya a **Paso 2**.

Paso 2 Recopilar información de fallas.

1. En MRS Manager, seleccione **System** > **Export Log**.
2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Referencia

Ninguna

8.5.18 ALM-12032 Usuario ommdba o contraseña está a punto de caducar (Para MRS 2.*x* o anterior)

Descripción

El sistema comienza a las 00:00 todos los días para comprobar si usuario **ommdba** y la contraseña están a punto de caducar cada ocho horas. Esta alarma se genera si el usuario o la contraseña están a punto de caducar en 15 días.

La alarma se borra cuando se cambia el período de validez del usuario **ommdba** o se restablece la contraseña y se completa el manejo de la alarma.

Atributo

ID de alarma	Gravedad de alarma	Borrar automáticamente
12032	Menor	Sí

Parámetros

Parámetro	Descripción
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

No se puede gestionar la base de datos de OMS y no se puede acceder a los datos.

Causas posibles

El usuario **ommdba** o la contraseña están a punto de caducar.

Procedimiento

Paso 1 Compruebe si usuario **ommdba** y la contraseña del sistema son válidas.

1. Inicie sesión en el nodo defectuoso.
2. Ejecute el siguiente comando para ver la información sobre el usuario **ommdba** y la contraseña:

chage -l ommdba

3. Compruebe si el usuario ha caducado según el mensaje del sistema.
   a. Vea el valor de **Password expires** para comprobar si la contraseña está a punto de caducar.
   b. Vea el valor de **Account expires** para comprobar si el usuario está a punto de caducar.

   NOTA

   Si el valor del parámetro es de **never**, el usuario y la contraseña son válidos permanentemente; si el valor es una fecha, compruebe si el usuario y la contraseña están a punto de caducar en un plazo de 15 días.

   – En caso afirmativo, vaya a **Paso 1.4**.
   – Si no, vaya a **Paso 2**.
4. Ejecute el siguiente comando para modificar la configuración del período de validez:
   – Ejecute el siguiente comando para establecer un período de validez para usuario **ommdba**:

     chage -E *'specified date'* **ommdba**
   – Ejecute el siguiente comando para establecer el número de días de validez para usuario **ommdba**:

     chage -M *'number of days'* **ommdba**
5. Compruebe si la alarma se borra automáticamente en la siguiente comprobación periódica.
   – En caso afirmativo, no es necesario hacer nada más.
   – Si no, vaya a **Paso 2**.

Paso 2 Recopilar información de fallas.

1. En MRS Manager, seleccione **System** > **Export Log**.
2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Referencia

Ninguna

8.5.19 ALM-12033 Falla de disco lento (Para MRS 2.*x* o anterior)

Descripción

- En el caso de HDDs, la alarma se activa cuando se cumple alguna de las siguientes condiciones:
  – El sistema ejecuta el comando **iostat** cada 3 segundos y detecta que el valor **svctm** supera los 1000 ms durante 10 períodos consecutivos en 30 segundos.
  – El sistema ejecuta el comando **iostat** cada 3 segundos y detecta que más del 60% de E/S supera los 150 ms en 300 segundos.
- Para las SSD, la alarma se activa cuando se cumple alguna de las siguientes condiciones:
  – El sistema ejecuta el comando **iostat** cada 3 segundos y detecta que el valor **svctm** supera los 1000 ms durante 10 períodos consecutivos en 30 segundos.

– El sistema ejecuta el comando **iostat** cada 3 segundos y detecta que más del 60% de E/S supera los 20 ms en 300 segundos.

Esta alarma se borra automáticamente cuando las condiciones anteriores no se han cumplido durante 15 minutos.

NOTA

El principio de detección de alarma es el siguiente:

En la plataforma Linux, ejecute el comando **iostat -x -t 1** para comprobar si la E/S es defectuosa. Específicamente, marque el valor **svctm** en el cuadro rojo de la siguiente figura.

svctm indica el tiempo de servicio de E/S del disco.

Atributo

ID de alarma	Severidad de la alarma	Borrar automáticamente
12033	Grave	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster o sistema para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
Host Name	Especifica el host para el que se genera la alarma.
DiskName	Especifica el disco para el que se genera la alarma.

Impacto en el sistema

El rendimiento del servicio se deteriora, las capacidades de procesamiento de servicios se vuelven deficientes y es posible que los servicios no estén disponibles.

Causas posibles

El disco está envejecido o tiene sectores defectuosos.

Procedimiento

Comprobar el estado de disco.

Paso 1 En la página de detalles del clúster MRS, haga clic en la alarma de la lista de alarmas en tiempo real. En el área **Alarm Details**, obtenga información sobre el host para el que se genera la alarma e información sobre el disco defectuoso.

Paso 2 Compruebe si el nodo para el que se genera la alarma se encuentra en un entorno de virtualización.

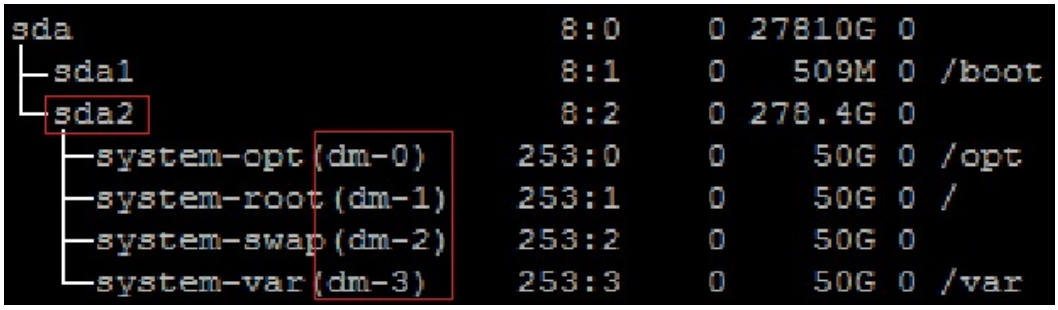
- En caso afirmativo, vaya a **Paso 3**.
- Si no, vaya a **Paso 6**.

Paso 3 Compruebe si el rendimiento de almacenamiento proporcionado por el entorno de virtualización cumple con los requisitos de hardware. A continuación, vaya a **Paso 4**.

Paso 4 Inicie sesión en el nodo de alarma como usuario **root**, ejecute el comando **df -h** y compruebe si la salida del comando contiene el valor del campo **DiskName**.

- En caso afirmativo, vaya a **Paso 6**.
- Si no, vaya a **Paso 5**.

Paso 5 Ejecute el comando **lsblk** para comprobar si se ha creado la asignación entre el valor de **DiskName** y el disco.



- En caso afirmativo, vaya a **Paso 6**.
- Si no, vaya a **Paso 21**.

Paso 6 Inicie sesión en el nodo de alarma como usuario **root**, ejecute el comando **lsscsi | grep "/dev/sd[x]"** para ver la información del disco y compruebe si se ha configurado RAID.

NOTA

En el comando **/dev/sd[x]** indica el nombre del disco obtenido en el archivo **Paso 1**.

Ejemplo:

lsscsi | grep "/dev/sda"

En la salida del comando, si se muestra **ATA**, **SATA** o **SAS** en la tercera línea, el disco no se ha organizado en un grupo RAID. Si se muestra otra información, se ha configurado RAID.

- En caso afirmativo, vaya a **Paso 11**.
- Si no, vaya a **Paso 7**.

Paso 7 Ejecute el comando **smartctl -i /dev/sd[x]** para comprobar si el hardware admite la herramienta SMART.

Ejemplo:

smartctl -i /dev/sda

En la salida del comando, si se muestra "SMART support is: Enabled", el hardware soporta SMART. Si "Device does not support SMART" o se muestra otra información, el hardware no admite SMART.

- En caso afirmativo, vaya a **Paso 8**.
- Si no, vaya a **Paso 16**.

Paso 8 Ejecute el comando **smartctl -H --all /dev/sd[x]** para comprobar la información básica de SMART y determinar si el disco funciona correctamente.

Ejemplo:

smartctl -H --all /dev/sda

Compruebe el valor de **SMART overall-health self-assessment test result** en la salida del comando. Si el valor es de **FAILED**, el disco está defectuoso y necesita ser reemplazado. Si el valor es **PASSED**, compruebe el valor de **Reallocated_Sector_Ct** o **Elements in grown defect list**. Si el valor es mayor que 100, el disco está defectuoso y necesita ser reemplazado.

- En caso afirmativo, vaya a **Paso 9**.
- Si no, vaya a **Paso 17**.

Paso 9 Ejecute el comando **smartctl -l error -H /dev/sd[x]** para comprobar Glist del disco y determinar si el disco es normal.

Ejemplo:

smartctl -l error -H /dev/sda

Compruebe la columna **Command/Featrue_name** en la salida del comando. Si se muestra **READ SECTOR(S)** o **WRITE SECTOR(S)**, el disco tiene sectores defectuosos. Si se producen otros errores, la placa de circuito de disco está defectuosa. Ambos errores indican que el disco es anormal y necesita ser reemplazado.

Si se muestra "No Errors Logged", no existe ningún registro de errores. Puede realizar el paso 9 para activar la autocomprobación SMART del disco.

- En caso afirmativo, vaya a **Paso 10**.
- Si no, vaya a **Paso 17**.

Paso 10 Ejecute el comando **smartctl -t long /dev/sd[x]** para activar la autocomprobación SMART del disco. Después de ejecutar el comando, se muestra el tiempo en el que se va a completar la autocomprobación. Una vez completada la autocomprobación, repita **Paso 8** y **Paso 9** para comprobar si el disco funciona correctamente.

Ejemplo:

smartctl -t long /dev/sda

- En caso afirmativo, vaya a **Paso 16**.
- Si no, vaya a **Paso 17**.

Paso 11 Ejecute el comando **smartctl -d [sat|scsi]+megaraid,[DID] -H --all /dev/sd[x]** para comprobar si el hardware admite SMART.

NOTA

- En el comando **[sat|scsi]** indica el tipo de disco. Ambos tipos necesitan ser utilizados.
- **[DID]** indica la información de intervalo. Las ranuras 0 a 15 necesitan ser utilizadas.

Por ejemplo, ejecute los siguientes comandos en secuencia:

smartctl -d sat+megaraid,0 -H --all /dev/sda

smartctl -d sat+megaraid,1 -H --all /dev/sda

smartctl -d sat+megaraid,2 -H --all /dev/sda

...

Pruebe las combinaciones de comandos de diferentes tipos de disco e información de ranura. Si se muestra "SMART support is: Enabled" en la salida del comando, el disco soporta SMART. Registre los parámetros del tipo de disco y la información de ranura cuando se ejecuta correctamente un comando. Si "SMART support is: Enabled" no se muestra en la salida del comando, el disco no soporta SMART.

- En caso afirmativo, vaya a **Paso 12**.
- Si no, vaya a **Paso 15**.

Paso 12 Ejecute el comando **smartctl -d [sat|scsi]+megaraid,[DID] -H --all /dev/sd[x]** grabado en **Paso 11** para comprobar la información básica de SMART y determinar si el disco es normal.

Ejemplo:

smartctl -d sat+megaraid,2 -H --all /dev/sda

Compruebe el valor de **SMART overall-health self-assessment test result** en la salida del comando. Si el valor es de **FAILED**, el disco está defectuoso y necesita ser reemplazado. Si el valor es **PASSED**, compruebe el valor de **Reallocated_Sector_Ct** o **Elements in grown defect list**. Si el valor es mayor que 100, el disco está defectuoso y necesita ser reemplazado.

- En caso afirmativo, vaya a **Paso 13**.
- Si no, vaya a **Paso 17**.

Paso 13 Ejecute el comando **smartctl -d [sat|scsi]+megaraid,[DID] -l error -H /dev/sd[x]** para comprobar la lista G del disco y determinar si el disco duro funciona correctamente.

Ejemplo:

smartctl -d sat+megaraid,2 -l error -H /dev/sda

Compruebe la columna **Command/Featrue_name** en la salida del comando. Si se muestra **READ SECTOR(S)** o **WRITE SECTOR(S)**, el disco tiene sectores defectuosos. Si se producen otros errores, la placa de circuito de disco está defectuosa. Ambos errores indican que el disco es anormal y necesita ser reemplazado.

Si se muestra "No Errors Logged", no existe ningún registro de errores. Puede realizar el paso 9 para activar la autocomprobación SMART del disco.

- En caso afirmativo, vaya a **Paso 14**.
- Si no, vaya a **Paso 17**.

Paso 14 Ejecute el comando **smartctl -d [sat|scsi]+megaraid,[DID] -t long /dev/sd[x]** para activar la autocomprobación SMART del disco. Después de ejecutar el comando, se muestra el tiempo

en el que se va a completar la autocomprobación. Una vez completada la autocomprobación, repita **Paso 12** y **Paso 13** para comprobar si el disco funciona correctamente.

Ejemplo:

smartctl -d sat+megaraid,2 -t long /dev/sda

- En caso afirmativo, vaya a **Paso 16**.
- Si no, vaya a **Paso 17**.

Paso 15 Si la tarjeta controladora RAID configurada no es compatible con SMART, el disco no es compatible con SMART. En este caso, utilice la herramienta de comprobación proporcionada por el proveedor de tarjeta controladora RAID correspondiente para rectificar la falla. Entonces vaya a **Paso 16**.

Por ejemplo, LSI es una herramienta de MegaCLI.

Paso 16 En la página de detalles de alarma, haga clic en **Clear Alarm**. Compruebe si la alarma se notifica de nuevo en el mismo disco.

Si la alarma se notifica más de tres veces, cambie el disco.

- En caso afirmativo, vaya a **Paso 17**.
- En caso negativo, no se requiere ninguna otra acción.

Reemplazar el disco.

Paso 17 En MRS Manager, seleccione **Alarms**.

Paso 18 Vea la información detallada sobre la alarma. Compruebe los valores de **HostName** y **DiskName** en la información de ubicación para obtener la información sobre el disco defectuoso para el que se informa la alarma.

Paso 19 Reemplace un disco.

Paso 20 Verifique si la alarma se ha borrado.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 21**.

Recopilar información de fallas.

Paso 21 En MRS Manager, elija **System** > **Export Log**.

Paso 22 Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

Información relacionada

Ninguna

8.5.20 ALM-12034 Falla de copia de respaldo periódica (Para MRS 2.*x* o anterior)

Descripción

Esta alarma se genera cuando no se puede ejecutar una tarea de copia de respaldo periódica. Esta alarma se borra cuando la siguiente tarea de copia de respaldo se ejecuta correctamente.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
12034	Grave	Sí

Parámetros

Parámetro	Descripción
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
TaskName	Especifica el nombre de la tarea.

Impacto en el sistema

No hay ningún paquete de copia de respaldo disponible durante mucho tiempo, por lo que el sistema no se puede restaurar en caso de excepciones.

Causas posibles

La causa de la alarma depende de los detalles de la tarea. Manejar la alarma de acuerdo con los registros y detalles de alarma.

Procedimiento

Comprobar si el espacio de disco es suficiente

Paso 1 En MRS Manager, seleccione **Alarms**.

Paso 2 En la lista de alarmas, haga clic en ⌄ de la alarma y obtenga el nombre de la tarea del área **Location**.

Paso 3 Elija **System** > **Back Up Data**.

Paso 4 Busque la tarea de copia de respaldo basándose en el nombre de la tarea y elija **More** > **View History** en la columna **Operation** para ver información detallada sobre la tarea de copia de respaldo.

Paso 5 Elija **Details** > **View** y compruebe si el mensaje "Failed to backup xx due to insufficient disk space, move the data in the /srv/BigData/LocalBackup directory to other directories." existe.

- En caso afirmativo, vaya a **Paso 6**.
- Si no, vaya a **Paso 13**.

Paso 6 Elija **Backup Path** > **View** para obtener la ruta de copia de respaldo.

Paso 7 Inicie sesión en el nodo como usuario **root** y vea los detalles de montaje del nodo.

df -h

Paso 8 Compruebe si el espacio disponible del nodo en el que está montado la ruta de copia de respaldo es inferior a 20 GB.

- En caso afirmativo, vaya a **Paso 9**.
- Si no, vaya a **Paso 13**.

Paso 9 Compruebe si el paquete de copia de respaldo existe en el directorio de copia de respaldo y si el espacio disponible del nodo en el que está montado el directorio de copia de respaldo es inferior a 20 GB.

- En caso afirmativo, vaya a **Paso 10**.
- Si no, vaya a **Paso 13**.

Paso 10 Asegúrese de que el espacio disponible del nodo en el que está montado el directorio de copia de respaldo sea superior a 20 GB moviendo los paquetes de copia de respaldo fuera del directorio de copia de respaldo o eliminando los paquetes de copia de respaldo.

Paso 11 Inicie la tarea de copia de respaldo de nuevo y compruebe si la tarea de copia de respaldo está ejecutada.

- En caso afirmativo, vaya a **Paso 12**.
- Si no, vaya a **Paso 13**.

Paso 12 Después de 2 minutos, compruebe si la alarma está borrada.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 13**.

Recopilación de información de error

Paso 13 En MRS Manager, elija **System** > **Export Log**.

Paso 14 Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

Referencia

Ninguna

8.5.21 ALM-12035 Estado de datos desconocidos después de un error de tarea de recuperación (para MRS 2.*x* o anterior)

Descripción

Si una tarea de recuperación falla, el sistema intenta revertir automáticamente. Si la reversión falla, los datos pueden perderse. Si esto ocurre, se informa de una alarma. Esta alarma se borra cuando la tarea de recuperación se ejecuta correctamente más adelante.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
12035	Crítica	Sí

Parámetros

Parámetro	Descripción
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
TaskName	Especifica el nombre de la tarea.

Impacto en el sistema

Los datos pueden perderse o el estado de los datos puede ser desconocido, lo que puede afectar a los servicios.

Causas posibles

La posible causa de esta alarma es que el estado del componente no cumple con los requisitos antes de que se ejecute la tarea de restauración o se produzca un error en un paso durante la tarea de restauración. El error depende de los detalles de la tarea. Puede obtener registros y detalles de tareas para manejar la alarma.

Procedimiento

Comprobación del estado de componente

Paso 1 Inicie sesión en MRS Manager y elija **Services**. En la página que se muestra, compruebe si el estado de ejecución de los componentes cumple los requisitos. (OMS y DBService deben estar en el estado normal y se deben detener otros componentes.)

- En caso afirmativo, vaya a **Paso 7**.
- Si no, vaya a **Paso 2**.

Paso 2 Restaure el estado del componente según sea necesario e inicie de nuevo la tarea de recuperación.

Paso 3 Inicie sesión en MRS Manager y elija **Alarms**. En la lista de alarmas, haga clic en la fila que contiene la alarma y obtenga el nombre de la tarea del área **Location**.

Paso 4 Elija **System** > **Recovery Management**. Busque la tarea de restauración según el nombre de la tarea y vea los detalles de la tarea.

Paso 5 Inicie la tarea de restauración y compruebe si la tarea está ejecutada.

- En caso afirmativo, vaya a **Paso 6**.
- Si no, vaya a **Paso 7**.

Paso 6 Después de 2 minutos, compruebe si la alarma está borrada.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 7**.

Recopilación de información de error

Paso 7 En MRS Manager, elija **System** > **Export Log**.

Paso 8 Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

Referencia

Ninguna

8.5.22 ALM-12037 Servidor NTP anormal (Para MRS 2.*x* o anterior)

Descripción

Esta alarma se genera cuando el servidor NTP es anormal.

Esta alarma se borra cuando el servidor NTP se recupera.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
12037	Grave	Sí

Parámetros

Parámetro	Descripción
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica la dirección IP del servidor NTP para el que se genera la alarma.

Impacto en el sistema

El servidor NTP configurado en el nodo OMS activo es anormal. En este caso, el nodo OMS activo no puede sincronizar el tiempo con el servidor NTP y se puede generar un desplazamiento de tiempo en el clúster.

Causas posibles

- La red del servidor NTP es defectuosa.
- La autenticación del servidor NTP falla.
- La hora no se puede obtener del servidor NTP.
- El tiempo obtenido del servidor NTP no se actualiza continuamente.

Procedimiento

Paso 1 Compruebe la red del servidor NTP.

1. En la página de detalles del clúster MRS, haga clic en la alarma de la lista de alarmas en tiempo real.
2. En el área **Alarm Details**, vea la información adicional para comprobar si el servidor NTP no se puede hacer ping.
   - En caso afirmativo, vaya a **Paso 1.3**.
   - Si no, vaya a **Paso 2**.
3. Póngase en contacto con el personal de O&M para comprobar la configuración de la red y asegurarse de que la red entre el servidor NTP y el nodo OMS activo está en estado normal. Luego, verifique si la alarma se rectificó.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 2**.

Paso 2 Compruebe si falla la autenticación del servidor NTP.

1. Inicie sesión en el nodo de gestión activo.
2. Ejecute **ntpq -np** para comprobar si falla la autenticación del servidor NTP. Si **refid** del servidor NTP es **.AUTH.**, la autenticación falla.
   - En caso afirmativo, vaya a **Paso 5**.
   - Si no, vaya a **Paso 3**.

Paso 3 Compruebe si la hora se puede obtener del servidor NTP.

1. Ver la información adicional de la alarma para comprobar si la hora no se puede obtener del servidor NTP.
   - En caso afirmativo, vaya a **Paso 3.2**.
   - Si no, vaya a **Paso 4**.
2. Póngase en contacto con el personal de O&M para rectificar la falla del servidor NTP. Después de que el servidor NTP esté en estado normal, compruebe si la alarma está borrada.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 4**.

Paso 4 Compruebe si el tiempo obtenido del servidor NTP no se actualiza.

1. Ver la información adicional de la alarma para comprobar si la hora obtenida del servidor NTP no se actualiza.
   - En caso afirmativo, vaya a **Paso 4.2**.
   - Si no, vaya a **Paso 5**.
2. Póngase en contacto con el proveedor del servidor NTP para rectificar la falla del servidor NTP. Después de que el servidor NTP esté en estado normal, compruebe si la alarma está borrada.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 5**.

Paso 5 Recopilar información de fallas.

1. En MRS Manager, seleccione **System** > **Export Log**.
2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Referencia

Ninguna

8.5.23 ALM-12038 Falla de volcado de indicador de monitoreo (Para MRS 2.*x* o anterior)

Descripción

Esta alarma se genera cuando el volcado falla después de que el volcado del indicador de monitoreo se configura en MRS Manager.

Esta alarma se borra cuando el volcado tiene éxito.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
12038	Grave	Sí

Parámetros

Parámetro	Descripción
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

El sistema de gestión de capa superior no obtiene indicadores de monitoreo del sistema de MRS Manager.

Causas posibles

- El servidor no se puede conectar.
- No se puede acceder a la ruta de guardado del servidor.
- El archivo indicador de monitoreo no se puede cargar.

Procedimiento

Paso 1 Póngase en contacto con el personal de O&M para comprobar si la conexión de red entre el sistema MRS Manager y el servidor es normal.

- En caso afirmativo, vaya a **Paso 3**.
- Si no, vaya a **Paso 2**.

Paso 2 Póngase en contacto con el personal de O&M para restaurar la red y comprobar si la alarma está desactivada.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 3**.

Paso 3 Elija **System** > **Monitor Dumping Configuration** y compruebe si el nombre de usuario, la contraseña, el puerto, el modo de volcado y la clave pública de FTP configurados en la página de configuración de volcado del indicador de monitoreo son coherentes con los del servidor.

- En caso afirmativo, vaya a **Paso 5**.
- Si no, vaya a **Paso 4**.

Paso 4 Ingrese la configuración correcta, haga clic en **OK** y compruebe si la alarma está desactivada.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 5**.

Paso 5 Elija **System** > **Monitor Dumping Configuration** y compruebe los elementos de configuración, incluido el nombre de usuario FTP, la ruta de guardado y el modo de volcado.

- Si se utiliza el modo FTP, vaya a **Paso 6**.

- Si se utiliza el modo SFTP, vaya a **Paso 7**.

Paso 6 Inicie sesión en el servidor. En la ruta predeterminada, compruebe si la ruta de guardado (ruta relativa) tiene el permiso de lectura y escritura en el nombre de usuario FTP.

- En caso afirmativo, vaya a **Paso 9**.
- Si no, vaya a **Paso 8**.

Paso 7 Inicie sesión en el servidor. En la ruta predeterminada, compruebe si la ruta de guardado (ruta absoluta) tiene el permiso de lectura y escritura en el nombre de usuario FTP.

- En caso afirmativo, vaya a **Paso 9**.
- Si no, vaya a **Paso 8**.

Paso 8 Agregue el permiso de lectura y escritura y compruebe si la alarma está borrada.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 9**.

Paso 9 Inicie sesión en el servidor y compruebe si la ruta de guardado tiene suficiente espacio en disco.

- En caso afirmativo, vaya a **Paso 11**.
- Si no, vaya a **Paso 10**.

Paso 10 Elimine los archivos innecesarios o vaya a la página de configuración de volcado del indicador de supervisión para cambiar la ruta de guardado. Verifique si la alarma se ha borrado.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 11**.

Paso 11 Recopilar información de fallas.

1. En MRS Manager, seleccione **System** > **Export Log**.
2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Referencia

Ninguna

8.5.24 ALM-12039 Los datos de GaussDB no están sincronizados (Para MRS 2.*x* o anterior)

Descripción

El sistema comprueba el estado de sincronización de datos entre los nodos de GaussDB activo y en espera cada 10 segundos. Esta alarma se genera cuando el estado de sincronización no se puede consultar durante seis veces consecutivas o cuando el estado de sincronización es anormal.

Esta alarma se borra cuando el estado de sincronización de datos es normal.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
12039	Crítica	Sí

Parámetro

Parámetro	Descripción
ServiceName	Servicio para el que se genera la alarma.
RoleName	Rol para el que se genera la alarma.
HostName	Host para el que se genera la alarma.
Local GaussDB HA IP	Dirección IP de HA de la GaussDB local.
Peer GaussDB HA IP	Dirección IP de HA de la GaussDB del par.
SYNC_PERSENT	Porcentaje de sincronización.

Impacto en el sistema

Cuando los datos no están sincronizados entre las GaussDB activas y en espera, los datos pueden perderse o ser anormales si la instancia activa se vuelve anormal.

Causas posibles

- La red entre los nodos activos y en espera es inestable.
- La GaussDB en espera es anormal.
- El espacio de disco del nodo en espera está lleno.

Procedimiento

Paso 1 Vaya a la página de detalles del clúster de MRS. En la lista de alarmas de la página de pestaña de gestión de alarmas, haga clic en la fila que contiene la alarma. En los detalles de la alarma, vea la dirección IP del nodo de GaussDB en espera.

Paso 2 Inicie sesión en el nodo de gestión activo.

Paso 3 Ejecute el siguiente comando para comprobar si la GaussDB en espera es accesible:

ping *heartbeat IP address of the standby GaussDB*

En caso afirmativo, vaya a **Paso 6**.

Si no, vaya a **Paso 4**.

Paso 4 Póngase en contacto con el personal de O&M para comprobar si la red es defectuosa.

- En caso afirmativo, vaya a **Paso 5**.
- Si no, vaya a **Paso 6**.

Paso 5 Rectifique la falla de la red y compruebe si la alarma está borrada de la lista de alarmas.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 6**.

Paso 6 Inicie sesión en el nodo de GaussDB en espera.

Paso 7 Ejecute los siguientes comandos para cambiar el usuario:

sudo su - root

su - omm

Paso 8 Vaya al directorio **${BIGDATA_HOME}/om-0.0.1/sbin/**.

Ejecute el siguiente comando para comprobar si el estado del recurso de la GaussDB en espera es normal:

sh status-oms.sh

En la salida del comando, compruebe si se muestra la siguiente información en la fila donde **ResName** es **gaussDB**:

```
10_10_10_231 gaussDB Standby_normal Normal Active_standby
```

- En caso afirmativo, vaya a **Paso 9**.
- Si no, vaya a **Paso 15**.

Paso 9 Inicie sesión en el nodo de GaussDB en espera.

Paso 10 Ejecute los siguientes comandos para cambiar el usuario:

sudo su - root

su - omm

Paso 11 Ejecute el comando **echo ${BIGDATA_DATA_HOME}/dbdata_om** para obtener el directorio de datos de GaussDB.

Paso 12 Ejecute el comando **df -h** para comprobar el uso de la partición del disco del sistema.

Paso 13 Compruebe si el disco donde está montado el directorio de datos de GaussDB está lleno.

- En caso afirmativo, vaya a **Paso 14**.
- Si no, vaya a **Paso 15**.

Paso 14 Póngase en contacto con el personal de O&M para ampliar la capacidad del disco. Después de la ampliación de la capacidad, espere 2 minutos y compruebe si la alarma está desactivada.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 15**.

Paso 15 Recopilar información de fallas.

1. En MRS Manager, seleccione **System** > **Export Log**.
2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Referencia

Ninguna

8.5.25 ALM-12040 Entropía insuficiente del sistema (Para MRS 2.*x* o anterior)

Descripción

El sistema comprueba la entropía a las 00:00:00 todos los días y realiza cinco comprobaciones consecutivas cada vez. En primer lugar, el sistema comprueba si la herramienta rng-tools está habilitada y configurada correctamente. Si no es así, el sistema comprueba la entropía actual. Esta alarma se genera si la entropía es menor que 500 en las cinco comprobaciones.

Esta alarma se borra si se configura el modo de número aleatorio verdadero, los números aleatorios se configuran en el modo de número pseudoaleatorio, o ni el modo de número aleatorio verdadero ni el modo de número pseudoaleatorio están configurados, pero la entropía es mayor que o igual a 500 en al menos una comprobación entre las cinco comprobaciones.

Atributo

ID de alarma	Gravedad de alarma	Borrar automáticamente
12040	Grave	Sí

Parámetros

Parámetro	Descripción
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

Se producen fallas de descifrado y las funciones relacionadas con el descifrado se ven afectadas, por ejemplo, la instalación de DBService.

Causas posibles

El servicio de rngd es anormal.

Procedimiento

Paso 1 Vaya a la página de detalles del clúster y elija **Alarms**.

Paso 2 Vea los detalles de la alarma para obtener el valor del campo **HostName** en **Location**.

Paso 3 Inicie sesión en el nodo para el que se genera la alarma y ejecute el comando **sudo su - root** para cambiar a usuario **root**.

Paso 4 Ejecute el comando **/bin/rpm -qa | grep -w "rng-tools"**. Si el comando se ejecuta correctamente, ejecute el comando **ps -ef | grep -v "grep" | grep rngd | tr -d " " | grep "\-o/dev/random" | grep "\-r/dev/urandom"** y vea la salida del comando.

- Si el comando se ejecuta correctamente, el servicio rngd se instala, se configura correctamente y se ejecuta correctamente. Vaya a **Paso 8**.
- Si el comando no se ejecuta correctamente, el servicio rngd no se está ejecutando correctamente. Entonces vaya a **Paso 5**.

Paso 5 Ejecute el siguiente comando para iniciar el servicio rngd:

echo 'EXTRAOPTIONS="-r /dev/urandom -o /dev/random"' >> /etc/sysconfig/rngd

service rngd start

Paso 6 Ejecute el comando **service rngd status** para comprobar si el servicio rngd está en estado de ejecución.

- En caso afirmativo, vaya a **Paso 7**.
- Si no, vaya a **Paso 8**.

Paso 7 Espere hasta las 00:00:00 cuando el sistema vuelva a comprobar la entropía. Compruebe si la alarma se borra automáticamente.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 8**.

Paso 8 Recopilar información de fallas.

1. En MRS Manager, seleccione **System** > **Export Log**.
2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Referencia

Ninguna

8.5.26 ALM-12041 El permiso de archivos clave es anormal (Para MRS 2.*x* o anterior)

Descripción

El sistema comprueba los permisos, los usuarios y los grupos de usuarios de los directorios o archivos clave cada hora. Esta alarma se genera si alguno de estos es anormal.

Esta alarma se borra después de resolver el problema que provoca permisos, usuarios o grupos de usuarios anormales.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
12041	Grave	Sí

Parámetros

Parámetro	Descripción
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
PathName	Especifica la ruta de acceso o el nombre del archivo.

Impacto en el sistema

Las funciones del sistema no están disponibles.

Causas posibles

El usuario ha modificado manualmente el permiso del archivo, la información del usuario o los grupos de usuarios, o el sistema ha experimentado un apagado inesperado.

Procedimiento

Paso 1 Verifique el permiso del archivo.

1. Vaya a la página de detalles del clúster de MRS y elija **Alarms**.
2. En los detalles de la alarma, consulte el **HostName** (nombre del host con alarma) y el **PathName** (ruta o nombre del archivo involucrado).
3. Inicie sesión en el nodo con alarma.
4. Ejecute el comando **ll** *PathName* para consultar el usuario actual, el permiso y el grupo de usuarios del archivo o ruta de acceso.
5. Vaya al directorio **${BIGDATA_HOME}/nodeagent/etc/agent/autocheck** y ejecute el comando **vi keyfile**. Busque el nombre del archivo involucrado y consulte el permiso correcto del archivo.
6. Compare el permiso real del archivo con el permiso obtenido en **Paso 1.5**. Si son diferentes, cambie el permiso real, la información de usuario y el grupo de usuarios a los valores correctos.
7. Espere hasta que se complete la siguiente comprobación del sistema y compruebe si la alarma está desactivada.

– En caso afirmativo, no es necesario hacer nada más.
– Si no, vaya a **Paso 2**.

Paso 2 Recopilar información de fallas.

1. En MRS Manager, seleccione **System** > **Export Log**.
2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Información relacionada

N/A

8.5.27 ALM-12042 Las configuraciones de archivo clave son anormales (Para MRS 2.*x* o anterior)

Descripción

El sistema comprueba las configuraciones de archivos clave cada hora. Esta alarma se genera si cualquier configuración de clave es anormal.

Esta alarma se borra después de que la configuración se vuelve normal.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
12042	Grave	Sí

Parámetros

Parámetro	Descripción
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
PathName	Especifica la ruta de acceso o el nombre del archivo.

Impacto en el sistema

Las funciones relacionadas con el archivo son anormales.

Causas posibles

El usuario ha modificado manualmente las configuraciones de archivos o el sistema ha experimentado un apagado inesperado.

Procedimiento

Paso 1 Compruebe las configuraciones de archivos.

1. Vaya a la página de detalles del clúster de MRS y elija **Alarms**.
2. En los detalles de la alarma, consulte el **HostName** (nombre del host con alarma) y el **PathName** (ruta o nombre del archivo involucrado).
3. Inicie sesión en el nodo con alarma.
4. Verifique y modifique manualmente las configuraciones de archivos de acuerdo con los criterios de **Información relacionada**.
5. Espere hasta que se complete la siguiente comprobación del sistema y compruebe si la alarma está desactivada.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 2**.

Paso 2 Recopilar información de fallas.

1. En MRS Manager, seleccione **System** > **Export Log**.
2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Información relacionada

- **Checking /etc/fstab**

  Compruebe si las particiones configuradas en **/etc/fstab** existen en **/proc/mounts** y si las particiones de swap configuradas en //**etc/fstab** coinciden con las de **/proc/swaps**.

- **Checking /etc/hosts**

  Ejecute el comando **cat /etc/hosts**. Si existe alguna de las siguientes situaciones, las configuraciones de archivos son anormales.
  - El archivo **/etc/hosts** no existe.
  - El nombre de host no está configurado en el archivo.
  - La dirección IP del host es duplicada.
  - La dirección IP del host no existe en la lista **ipconfig**.
  - Una dirección IP en el archivo es utilizada por varios hosts.

8.5.28 ALM-12043 La duración de análisis de DNS supera el umbral (Para MRS 2.*x* o anterior)

Descripción

El sistema comprueba la duración del análisis de DNS cada 30 segundos. Esta alarma se genera cuando la duración del análisis DNS excede el umbral (el umbral predeterminado es 20,000 ms) varias veces (el valor predeterminado es **2**).

Puede cambiar el umbral seleccionando **System** > **Threshold Configuration** > **Device** > **Host** > **Network Status** > **DNS Resolution Duration** > **DNS Resolution Duration**.

Esta alarma se borra cuando **hit number** es **1** y la duración de la resolución de DNS es menor o igual que el umbral. Esta alarma se borra cuando **hit number** no es **1** y la duración de la resolución DNS es menor o igual al 90% del umbral.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
12043	Grave	Sí

Parámetros

Parámetro	Descripción
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

- La autenticación secundaria basada en Kerberos es lenta.
- El servicio ZooKeeper es anormal.
- El nodo está defectuoso.

Causas posibles

- El nodo se configura con el cliente de DNS.
- El nodo está equipado con el servidor DNS y se inicia el servidor DNS.

Procedimiento

Compruebe si el nodo está configurado con el cliente de DNS.

Paso 1 Vaya a la página de detalles del clúster de MRS y elija **Alarms**.

Paso 2 Vea los detalles de la alarma para obtener el valor del campo **HostName** en **Location**.

Paso 3 Utilice PuTTY para iniciar sesión en el nodo para el que se genera la alarma como usuario **root**.

Paso 4 Ejecute el comando **cat /etc/resolv.conf** para comprobar si el cliente DNS está instalado.

Si se muestra información similar a la siguiente, se instala e inicia el cliente DNS:


```
namesever 10.2.3.4
namesever 10.2.3.4
```

- En caso afirmativo, vaya a **Paso 5**.
- Si no, vaya a **Paso 7**.

Paso 5 Ejecute el comando **vi /etc/resolv.conf** para comentar el siguiente contenido usando los signos numéricos (#) y guarde el archivo:

```
# namesever 10.2.3.4
# namesever 10.2.3.4
```

Paso 6 Compruebe si esta alarma se borra después de 5 minutos.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 7**.

Compruebe si el nodo está equipado con el servidor DNS y si el servidor DNS está iniciado.

Paso 7 Ejecute el comando **service named status** para comprobar si el servicio DNS está instalado en el nodo.

Si se muestra información similar a la siguiente, se instala e inicia el servidor DNS:

```
Checking for nameserver BIND
version: 9.6-ESV-R7-P4
CPUs found: 8
worker threads: 8
number of zones: 17
debug level: 0
xfers running: 0
xfers deferred: 0
soa queries in progress: 0
query logging is ON
recursive clients: 4/0/1000
tcp clients: 0/100
server is up and running
```

- En caso afirmativo, vaya a **Paso 8**.
- Si no, vaya a **Paso 10**.

Paso 8 Ejecute el comando **service named stop** para detener el servidor DNS.

Paso 9 Compruebe si esta alarma se borra después de 5 minutos.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 10**.

Paso 10 Recopilar información de fallas.

1. En MRS Manager, seleccione **System** > **Export Log**.
2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Referencia

Ninguna

8.5.29 ALM-12045 La tasa de paquetes perdidos de lectura supera el umbral (Para MRS 2.*x* o anterior)

Descripción

El sistema comprueba la tasa de pérdida del paquete de lectura cada 30 segundos. Esta alarma se genera cuando la tasa de pérdida del paquete de lectura excede el umbral (el umbral predeterminado es 0.5%) varias veces (el valor predeterminado es **5**).

Puede cambiar el umbral seleccionando **System** > **Threshold Configuration** > **Device** > **Host** > **Network Reading** > **Network Read Packet Rate Information** > **Read Packet Dropped Rate**.

Esta alarma se borra cuando **hit number** es 1 y la tasa de paquetes perdidos de lectura es menor o igual que el umbral. Esta alarma se borra cuando **hit number** es mayor que 1 y la tasa de paquetes perdidos de lectura es menor o igual al 90% del umbral.

La detección de alarma está deshabilitada de forma predeterminada. Si desea habilitar esta función, compruebe si esta función se puede habilitar en función de Comprobación de entornos del sistema.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
12045	Grave	Sí

Parámetros

Parámetro	Descripción
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
NetworkCardName	Especifica el puerto de red para el que se genera la alarma.
Trigger Condition	Especifica el umbral para activar la alarma.

Impacto en el sistema

El rendimiento del servicio se deteriora o el tiempo de espera de algunos servicios.

Advertencia de riesgos: En SUSE kernel 3.0 o posterior o Red Hat 7.2, el kernel del sistema modifica el mecanismo para contar el número de paquetes de lectura perdidos. En este caso,

esta alarma puede generarse incluso si la red se está ejecutando correctamente, pero los servicios no se ven afectados. Se recomienda comprobar primero el entorno del sistema.

Causas posibles

- Se produce una excepción del sistema operativo.
- Las NIC están unidas en modo activo/en espera.
- El umbral de alarma está configurado incorrectamente.
- El entorno de red es anormal.

Procedimiento

Ver la tasa de pérdida de paquetes de red.

Paso 1 Utilice PuTTY para iniciar sesión en cualquier nodo que no sea de alarma en el clúster como usuario **omm** y ejecute el comando **ping** *IP address of the node for which the alarm is generated* **-c 100** para comprobar si se produce la pérdida de paquetes en la red.

```
# ping 10.10.10.12 -c 5
PING 10.10.10.12 (10.10.10.12) 56(84) bytes of data.
64 bytes from 10.10.10.11: icmp_seq=1 ttl=64 time=0.033 ms
64 bytes from 10.10.10.11: icmp_seq=2 ttl=64 time=0.034 ms
64 bytes from 10.10.10.11: icmp_seq=3 ttl=64 time=0.021 ms
64 bytes from 10.10.10.11: icmp_seq=4 ttl=64 time=0.033 ms
64 bytes from 10.10.10.11: icmp_seq=5 ttl=64 time=0.030 ms
--- 10.10.10.12 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4001ms   rtt min/avg/max/
mdev = 0.021/0.030/0.034/0.006 ms
```

NOTA

- *IP address of the node for which the alarm is generated*: Consultar la dirección IP del nodo para el que se genera la alarma en la página de gestión de nodo de la página de detalles del clúster MRS basándose en el valor de **HostName** en la información de ubicación de alarma. Compruebe tanto las direcciones IP del plano de gestión como del plano de servicio.
- **-c**: número de veces de comprobación. El valor predeterminado es **100**.

- En caso afirmativo, vaya a **Paso 11**.
- Si no, vaya a **Paso 2**.

Comprobar el entorno de sistema.

Paso 2 Utilice PuTTY para iniciar sesión en el nodo OMS activo o en el nodo para el que se genera la alarma como usuario **omm**.

Paso 3 Ejecute el comando **cat /etc/*-release** para comprobar el tipo de sistema operativo.

- Si el sistema operativo es EulerOS, vaya a **Paso 4**.

```
# cat  /etc/*-release                                    EulerOS release 2.0
(SP2)
EulerOS release 2.0 (SP2)
```

- Si el sistema operativo es SUSE, vaya a **Paso 5**.

```
# cat /etc/*-release
SUSE Linux Enterprise Server 11 (x86_64)
VERSION = 11
PATCHLEVEL = 3
```

- De lo contrario, vaya a **Paso 11**.

Paso 4 Ejecute el comando **cat /etc/euleros-release** para comprobar si la versión del sistema operativo es EulerOS 2.2.


```
# cat/etc/euleros-release
EulerOS release 2.0 (SP2)
```

- En caso afirmativo, no se puede activar la función de envío de alarmas. Vaya a **Paso 6**.
- Si no, vaya a **Paso 11**.

Paso 5 Ejecute el comando **cat /proc/version** para comprobar si la versión del kernel de SUSE es 3.0 o posterior.

```
# cat /proc/version
Linux version 3.0.101-63-default (geeko@buildhost) (gcc version 4.3.4 [gcc-4_3-
branch revision 152973] (SUSE Linux) ) #1 SMP Tue Jun 23 16:02:31 UTC 2015
(4b89d0c)
```

- En caso afirmativo, no se puede activar la función de envío de alarmas. Vaya a **Paso 6**.
- Si no, vaya a **Paso 11**.

Paso 6 Inicie sesión en MRS Manager y elija **System** > **Configuration** > **Threshold Configuration**.

Paso 7 En el panel de navegación de la página **Threshold Configuration**, seleccione **Network Reading** > **Network Read Packet Rate Information** > **Read Packet Dropped Rate**. En el panel derecho, compruebe si **Send Alarm** está seleccionado.

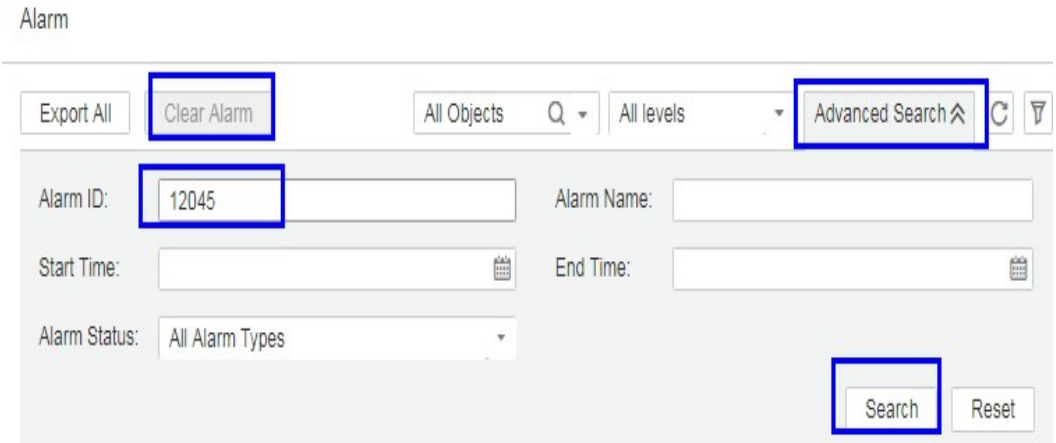
- En caso afirmativo, la función de envío de alarmas está activada. Vaya a **Paso 8**.
- Si no, la función de envío de alarmas está desactivada. Vaya a **Paso 10**.

Paso 8 En el panel derecho, anule la selección de **Send Alarm** para proteger la alarma "La tasa de paquetes perdidos de lectura de red supera el umbral."

Paso 9 Vaya a la página de detalles del clúster de MRS y elija **Alarms**.

Paso 10 Busque la alarma 12045 y borre manualmente las alarmas que no se borran automáticamente. No se requiere ninguna otra acción.

Figura 8-2 Gestión de alarma



NOTA

El ID de la tasa de pérdida de paquetes de lectura de red de alarma supera el umbral es 12045.

Compruebe si las NIC están enlazadas en modo activo/en espera.

Paso 11 Utilice PuTTY para iniciar sesión en el nodo para el que se genera la alarma como usuario **omm** y ejecute el comando **ls -l /proc/net/bonding** para comprobar si el directorio **/proc/net/bonding** existe en el nodo.

- En caso afirmativo, como se muestra en la siguiente figura, el modo de enlace se configura para el nodo. Vaya a **Paso 12**.

```
# ls -l /proc/net/bonding/
total 0
-r--r--r-- 1 root root 0 Oct 11 17:35 bond0
```

- Si no, el modo de enlace no está configurado para el nodo. Vaya a **Paso 14**.

```
# ls -l /proc/net/bonding/
ls: cannot access /proc/net/bonding/: No such file or directory
```

Paso 12 Ejecute el comando **cat /proc/net/bonding/bond0** para comprobar si el valor de **Bonding Mode** en el archivo de configuración es **fault-tolerance**.

NOTA

En el comando anterior, **bond0** es el nombre del archivo de configuración de enlace. Utilice el nombre de archivo obtenido en **Paso 11**.

```
# cat /proc/net/bonding/bond0
Ethernet Channel Bonding Driver: v3.7.1 (April 27, 2011)

Bonding Mode: fault-tolerance (active-backup)
Primary Slave: eth1 (primary_reselect always)
Currently Active Slave: eth1
MII Status: up
MII Polling Interval (ms): 100
Up Delay (ms): 0
Down Delay (ms): 0

Slave Interface: eth0
MII Status: up
Speed: 1000 Mbps
Duplex: full
Link Failure Count: 1
Slave queue ID: 0

Slave Interface: eth1
MII Status: up
Speed: 1000 Mbps
Duplex: full
Link Failure Count: 1
Slave queue ID: 0
```

- En caso afirmativo, las NIC se unen en modo activo/en espera. Vaya a **Paso 13**.
- Si no, vaya a **Paso 14**.

Paso 13 Compruebe si la NIC especificada por **NetworkCardName** en los detalles de la alarma es la NIC en espera.

- En caso afirmativo, la alarma de la NIC en espera no se puede borrar automáticamente. Borre manualmente la alarma en la página de gestión de alarmas. No se requiere ninguna otra acción.
- Si no, vaya a **Paso 14**.

NOTA

Para determinar la NIC en espera, compruebe el archivo de configuración **/proc/net/bonding/bond0**. Si el nombre de NIC correspondiente a **NetworkCardName** es **Slave Interface** pero no **Currently Active Slave** (la NIC activa actual), la NIC es la en espera.

Comprobar si el umbral está configurado correctamente.

Paso 14 Inicie sesión en MRS Manager y compruebe si el umbral (configurable, 0.5% por defecto) es apropiado.

- En caso afirmativo, vaya a **Paso 17**.

- Si no, vaya a **Paso 15**.

Paso 15 Seleccione **System** > **Threshold Configuration** > **Device** > **Host** > **Network Reading** > **Network Read Packet Rate Information** > **Read Packet Dropped Rate** y cambie el umbral de alarma según el uso real del servicio.

Paso 16 Espere 5 minutos y compruebe si la alarma está desactivada.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 17**.

Compruebe si la red es normal.

Paso 17 Póngase en contacto con el administrador del sistema para comprobar si la red es normal.

- En caso afirmativo, rectifique la falla de la red y vaya a **Paso 18**.
- Si no, vaya a **Paso 19**.

Paso 18 Espere 5 minutos y compruebe si la alarma está desactivada.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 19**.

Paso 19 Recopilar información de fallas.

1. En MRS Manager, seleccione **System** > **Export Log**.
2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Referencia

Ninguna

8.5.30 ALM-12046 La tasa de paquetes de escritura perdidos supera el umbral (Para MRS 2.*x* o anterior)

Descripción

El sistema comprueba la tasa de paquetes de escritura perdidos cada 30 segundos. This alarm is generated when the write packet dropped rate exceeds the threshold (the default threshold is 0.5%) for multiple times (the default value is **5**).

Puede cambiar el umbral seleccionando **System** > **Threshold Configuration** > **Device** > **Host** > **Network Writing** > **Network Write Packet Rate Information** > **Write Packet Dropped Rate**.

Cuando el **hit number** es **1**, esta alarma se borra cuando la tasa de paquetes perdidos de escritura en red es menor o igual al umbral. Cuando el **hit number** es mayor que **1**, esta alarma se borra cuando la tasa de paquetes perdidos de escritura en red es menor o igual al 90% del umbral.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
12046	Grave	Sí

Parámetros

Parámetro	Descripción
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
NetworkCardName	Especifica el puerto de red para el que se genera la alarma.
Trigger Condition	Especifica el umbral para activar la alarma.

Impacto en el sistema

El rendimiento del servicio se deteriora o el tiempo de espera de algunos servicios.

Causas posibles

- El umbral de alarma está configurado incorrectamente.
- El entorno de red es anormal.

Procedimiento

Comprobar si el umbral está configurado correctamente.

Paso 1 Inicie sesión en MRS Manager y compruebe si el umbral (configurable, 0.5% por defecto) es apropiado.

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 2**.

Paso 2 Seleccione **System** > **Threshold Configuration** > **Device** > **Host** > **Network Write Information** > **Network Write Packet Rate** > **Write Packet Dropped Rate** y cambie el umbral de alarma en función del uso real del servicio.

Paso 3 Espere 5 minutos y compruebe si la alarma está desactivada.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 4**.

Compruebe si la red es normal.

Paso 4 Póngase en contacto con el administrador del sistema para comprobar si la red es normal.

- En caso afirmativo, rectifique la falla de la red y vaya a **Paso 5**.
- Si no, vaya a **Paso 6**.

Paso 5 Espere 5 minutos y compruebe si la alarma está desactivada.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 6**.

Paso 6 Recopilar información de fallas.

1. En MRS Manager, seleccione **System** > **Export Log**.
2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Referencia

Ninguna

8.5.31 ALM-12047 La tasa de error de paquete de lectura supera el umbral (Para MRS 2.*x* o anterior)

Descripción

El sistema comprueba la tasa de errores del paquete leído cada 30 segundos. Esta alarma se genera cuando la tasa de error del paquete leído excede el umbral (el umbral predeterminado es de **0.5%**) varias veces (el valor predeterminado es de **5**).

Puede cambiar el umbral seleccionando **System** > **Threshold Configuration** > **Device** > **Host** > **Network Reading** > **Network Read Packet Rate Information** > **Read Packet Error Rate**.

Si el **hit number** es de **1**, esta alarma se borra cuando la tasa de error del paquete leído es menor o igual que el umbral. Si el **hit number** es mayor que **1** esta alarma se borra cuando la tasa de error del paquete leído es menor que o igual al 90% del umbral.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
12047	Grave	Sí

Parámetros

Parámetro	Descripción
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.

Parámetro	Descripción
HostName	Especifica el host para el que se genera la alarma.
NetworkCardName	Especifica el puerto de red para el que se genera la alarma.
Trigger Condition	Especifica el umbral para activar la alarma.

Impacto en el sistema

La comunicación se interrumpe intermitentemente y los servicios expiran.

Causas posibles

- El umbral de alarma está configurado incorrectamente.
- El entorno de red es anormal.

Procedimiento

Comprobar si el umbral está configurado correctamente.

Paso 1 Inicie sesión en MRS Manager y compruebe si el umbral (configurable, 0,5% por defecto) es apropiado.

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 2**.

Paso 2 Seleccione **System** > **Threshold Configuration** > **Device** > **Host** > **Network Reading** > **Network Read Packet Rate Information** > **Read Packet Error Rate** y cambie el umbral de alarma según el uso real del servicio.

Paso 3 Espere 5 minutos y compruebe si la alarma está desactivada.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 4**.

Compruebe si la red es normal.

Paso 4 Póngase en contacto con el administrador del sistema para comprobar si la red es normal.

- En caso afirmativo, rectifique la falla de la red y vaya a **Paso 5**.
- Si no, vaya a **Paso 6**.

Paso 5 Espere 5 minutos y compruebe si la alarma está desactivada.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 6**.

Paso 6 Recopilar información de fallas.

1. En MRS Manager, seleccione **System** > **Export Log**.
2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Referencia

Ninguna

8.5.32 ALM-12048 La tasa de error de escritura de paquetes supera el umbral (Para MRS 2.*x* o anterior)

Descripción

El sistema comprueba la tasa de errores de escritura de paquetes cada 30 segundos. Esta alarma se genera cuando la tasa de errores de paquete de escritura supera el umbral (el umbral predeterminado es de **0.5%**) varias veces (el valor predeterminado es de **5**).

Puede cambiar el umbral seleccionando **System** > **Threshold Configuration** > **Device** > **Host** > **Network Writing** > **Network Write Packet Rate Information** > **Write Packet Error Rate**.

Si **hit number** es de **1**, esta alarma se borra cuando la tasa de errores de paquete de escritura es menor o igual que el umbral. Si **hit number** es mayor que **1**, esta alarma se borra cuando la tasa de error de paquete de escritura es menor o igual al 90% del umbral.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
12048	Grave	Sí

Parámetros

Parámetro	Descripción
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
NetworkCardName	Especifica el puerto de red para el que se genera la alarma.
Trigger Condition	Especifica el umbral para activar la alarma.

Impacto en el sistema

La comunicación se interrumpe intermitentemente y los servicios expiran.

Causas posibles

- El umbral de alarma está configurado incorrectamente.
- El entorno de red es anormal.

Procedimiento

Comprobar si el umbral está configurado correctamente.

Paso 1 Inicie sesión en MRS Manager y compruebe si el umbral (configurable, 0.5% por defecto) es apropiado.

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 2**.

Paso 2 Seleccione **System** > **Threshold Configuration** > **Device** > **Host** > **Network Writing** > **Network Write Packet Rate Information** > **Write Packet Error Rate** y cambie el umbral de alarma en función del uso real del servicio.

Paso 3 Espere 5 minutos y compruebe si la alarma está desactivada.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 4**.

Compruebe si la red es normal.

Paso 4 Póngase en contacto con el administrador del sistema para comprobar si la red es normal.

- En caso afirmativo, rectifique la falla de la red y vaya a **Paso 5**.
- Si no, vaya a **Paso 6**.

Paso 5 Espere 5 minutos y compruebe si la alarma está desactivada.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 6**.

Paso 6 Recopilar información de fallas.

1. En MRS Manager, seleccione **System** > **Export Log**.
2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Referencia

Ninguna

8.5.33 ALM-12049 La tasa de rendimiento de lectura supera el umbral (Para MRS 2.*x* o anterior)

Descripción

El sistema comprueba la velocidad de procesamiento de lectura cada 30 segundos. Esta alarma se genera cuando la velocidad de procesamiento de lectura supera el umbral (el umbral predeterminado es de **80%**) varias veces (el valor predeterminado es de **5**).

Puede cambiar el umbral seleccionando **System** > **Threshold Configuration** > **Device** > **Host** > **Network Reading** > **Network Read Throughput Rate** > **Read Throughput Rate**.

Si el **hit number** es de **1**, esta alarma se borra cuando la tasa de rendimiento de lectura es menor o igual que el umbral. Si el **hit number** es mayor que **1**, esta alarma se borra cuando la tasa de rendimiento de lectura es menor o igual al 90% del umbral.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
12049	Grave	Sí

Parámetros

Parámetro	Descripción
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
NetworkCardName	Especifica el puerto de red para el que se genera la alarma.
Trigger Condition	Especifica el umbral para activar la alarma.

Impacto en el sistema

El sistema de servicio se ejecuta de forma anormal o no está disponible.

Causas posibles

- El umbral de alarma está configurado incorrectamente.
- La velocidad de puerto de red no cumple con los requisitos de servicio.

Procedimiento

Comprobar si el umbral está configurado correctamente.

Paso 1 Inicie sesión en MRS Manager y compruebe si el umbral (configurable, 80% por defecto) es apropiado.

- En caso afirmativo, vaya a **Paso 2**.
- Si no, vaya a **Paso 4**.

Paso 2 Elija **System** > **Threshold Configuration** > **Device** > **Host** > **Network Reading** > **Network Read Throughput Rate** > **Read Throughput Rate** para cambiar el umbral de alarma según el uso real del servicio.

Paso 3 Espere 5 minutos y compruebe si la alarma está desactivada.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 4**.

Compruebe si la velocidad del puerto de red cumple los requisitos.

Paso 4 En la lista de alarmas en tiempo real, haga clic en la alarma. En el área **Alarm Details**, obtenga la dirección IP y el nombre del puerto de red del host para el que se genera la alarma.

Paso 5 Utilice PuTTY para iniciar sesión en el host para el que se genera la alarma como usuario **root**.

Paso 6 Ejecute el comando **ethtool** *network port name* para comprobar el **Speed** máximo de velocidad de puerto de red.

NOTA

En un entorno de VM, es posible que no se obtenga la velocidad de puerto de red ejecutando comandos. Se recomienda que se ponga en contacto con el administrador del sistema para comprobar si la velocidad de puerto de red cumple los requisitos.

Paso 7 Si la tasa de rendimiento de lectura excede el umbral, póngase en contacto con el administrador del sistema para aumentar la tasa de puerto de red.

Paso 8 Verifique si la alarma se ha borrado.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 9**.

Paso 9 Recopilar información de fallas.

1. En MRS Manager, seleccione **System** > **Export Log**.
2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Referencia

Ninguna

8.5.34 ALM-12050 La tasa de rendimiento de escritura supera el umbral (Para MRS 2.*x* o anterior)

Descripción

El sistema comprueba la tasa de rendimiento de escritura cada 30 segundos. Esta alarma se genera cuando la tasa de rendimiento de escritura supera el umbral (el umbral predeterminado es de **80%**) varias veces (el valor predeterminado es de **5**).

Puede cambiar el umbral seleccionando **System** > **Threshold Configuration** > **Device** > **Host** > **Network Writing** > **Network Write Throughput Rate** > **Write Throughput Rate**.

Si el **hit number** es de **1**, esta alarma se borra cuando la tasa de rendimiento de escritura es menor o igual que el umbral. Si el **hit number** es mayor que **1**, esta alarma se borra cuando la tasa de rendimiento de escritura es menor o igual al 90% del umbral.

Atributo

ID de alarma	Gravedad de alarma	Borrar automáticamente
12050	Grave	Sí

Parámetros

Parámetro	Descripción
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
NetworkCardName	Especifica el puerto de red para el que se genera la alarma.
Trigger Condition	Especifica el umbral para activar la alarma.

Impacto en el sistema

El sistema de servicio se ejecuta de forma anormal o no está disponible.

Causas posibles

- El umbral de alarma está configurado incorrectamente.
- La velocidad de puerto de red no cumple con los requisitos de servicio.

Procedimiento

Comprobar si el umbral está configurado correctamente.

Paso 1 Inicie sesión en MRS Manager y compruebe si el umbral (configurable, 80% por defecto) es apropiado.

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 2**.

Paso 2 Seleccione **System** > **Threshold Configuration** > **Device** > **Host** > **Network Writing** > **Network Write Throughput Rate** > **Write Throughput Rate** para cambiar el umbral de alarma según el uso real del servicio.

Paso 3 Espere 5 minutos y compruebe si la alarma está desactivada.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 4**.

Compruebe si la velocidad del puerto de red cumple los requisitos.

Paso 4 En la lista de alarmas en tiempo real, haga clic en la alarma. En el área **Alarm Details**, obtenga la dirección IP y el puerto de red del host para el que se genera la alarma.

Paso 5 Utilice PuTTY para iniciar sesión en el host para el que se genera la alarma como usuario **root**.

Paso 6 Ejecute el comando **ethtool** *network port name* para comprobar el **Speed** máximo de velocidad de puerto de red.

NOTA

En un entorno de VM, es posible que no se obtenga la velocidad de puerto de red ejecutando comandos. Se recomienda que se ponga en contacto con el administrador del sistema para comprobar si la velocidad de puerto de red cumple los requisitos.

Paso 7 Si la tasa de rendimiento de escritura excede el umbral, póngase en contacto con el administrador del sistema para aumentar la tasa de puerto de red.

Paso 8 Verifique si la alarma se ha borrado.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 9**.

Paso 9 Recopilar información de fallas.

1. En MRS Manager, seleccione **System** > **Export Log**.
2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Referencia

Ninguna

8.5.35 ALM-12051 El uso del Inode de disco supera el umbral (Para MRS 2.*x* o anterior)

Descripción

El sistema comprueba el uso del inode de disco cada 30 segundos. Esta alarma se genera cuando el uso del disco de inode excede el umbral (el umbral predeterminado es 80%) varias veces (el valor predeterminado es 5).

Puede cambiar el umbral seleccionando **System** > **Threshold Configuration** > **Device** > **Host** > **Disk** > **Disk Inode Usage** > **Disk Inode Usage**.

Si el **hit number** es de **1** esta alarma se borra cuando el uso del inode del disco es menor o igual al umbral. Si el **hit number** es mayor que **1**, esta alarma se borra cuando el uso del inode del disco es menor o igual al 90% del umbral.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
12051	Grave	Sí

Parámetros

Parámetro	Descripción
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
PartitionName	Especifica la partición de disco para la que se genera la alarma.
Trigger Condition	Especifica el umbral para activar la alarma.

Impacto en el sistema

Los datos no se pueden escribir en el sistema de archivos.

Causas posibles

- Hay demasiados archivos pequeños en el disco.
- El sistema no funciona normalmente.

Procedimiento

Hay demasiados archivos pequeños en el disco.

Paso 1 Vaya a la página de detalles del clúster de MRS y elija **Alarms**.

Paso 2 En la lista de alarmas en tiempo real, haga clic en la alarma. En el área **Alarm Details**, obtenga la dirección IP y las particiones de disco del host para el que se genera la alarma.

Paso 3 Utilice PuTTY para iniciar sesión en el host para el que se genera la alarma como usuario **root**.

Paso 4 Ejecute el comando **df -i** *partition name* para comprobar el uso actual del disco inode.

Paso 5 Si el uso del inode excede el umbral, compruebe manualmente si se pueden eliminar los archivos pequeños de la partición.

- En caso afirmativo, elimine los archivos y vaya a **Paso 6**.
- Si no, ajuste la capacidad. Entonces vaya a **Paso 7**.

Paso 6 Espere 5 minutos y compruebe si la alarma está desactivada.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 7**.

Comprobar si el entorno de sistema es normal.

Paso 7 Póngase en contacto con el personal de mantenimiento del sistema operativo para comprobar si el entorno del sistema es anormal.

- En caso afirmativo, rectifique el fallo del sistema operativo y vaya a **Paso 8**.
- Si no, vaya a **Paso 9**.

Paso 8 Espere 5 minutos y compruebe si la alarma está desactivada.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 9**.

Paso 9 Recopilar información de fallas.

1. En MRS Manager, seleccione **System** > **Export Log**.
2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Referencia

Ninguna

8.5.36 ALM-12052 El uso de puertos de TCP temporales supera el umbral (Para MRS 2.*x* o anterior)

Descripción

El sistema comprueba el uso de puertos de TCP temporales cada 30 segundos. Esta alarma se genera cuando el uso de puertos TCP temporales excede el umbral (el umbral predeterminado es de **80%**) varias veces (el valor predeterminado es de **5**).

Puede cambiar el umbral seleccionando **System** > **Threshold Configuration** > **Host** > **Network Status** > **TCP Ephemeral Port Usage** > **TCP Ephemeral Port Usage**.

Si el **hit number** es de **1**, esta alarma se borra cuando el uso de puertos de TCP temporales es menor o igual al umbral. Si el **hit number** es mayor que **1**, esta alarma se borra cuando el uso de puertos de TCP temporales es menor o igual al 90% del umbral.

Atributo

ID de alarma	Gravedad de alarma	Borrar automáticamente
12052	Grave	Sí

Parámetros

Parámetro	Descripción
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.

Parámetro	Descripción
HostName	Especifica el host para el que se genera la alarma.
Trigger Condition	Especifica el umbral para activar la alarma.

Impacto en el sistema

Los servicios en el host no pueden establecer conexiones con el externo y los servicios se interrumpen.

Causas posibles

- Los puertos temporales no cumplen con los requisitos de servicio.
- El sistema no funciona normalmente.

Procedimiento

Expandir el rango de puertos temporales.

Paso 1 Vaya a la página de detalles del clúster de MRS y elija **Alarms**.

Paso 2 En la lista de alarmas en tiempo real, haga clic en la alarma. En el área **Alarm Details**, obtenga la dirección IP del host para el que se genera la alarma.

Paso 3 Utilice PuTTY para iniciar sesión en el host para el que se genera la alarma como usuario **omm**.

Paso 4 Ejecute el comando **cat /proc/sys/net/ipv4/ip_local_port_range |cut -f 1** para obtener el número de puerto de inicio. Ejecute el comando **cat /proc/sys/net/ipv4/ip_local_port_range | cut -f 2** para obtener el número de puerto final. Reste el número de puerto inicial del número de puerto final para obtener el número total de puertos temporales. Si el número total de puertos temporales es inferior a 28,232, el rango de puertos aleatorios del sistema operativo es demasiado pequeño. En este caso, póngase en contacto con el administrador del sistema para ampliar el rango de puertos.

Paso 5 Ejecute el comando **ss -ant 2>/dev/null | grep -v LISTEN | awk 'NR > 2 {print $4}'|cut -d ':' -f 2 | awk '$1 >"***start port number***" {print $1}' | sort -u | wc -l** para calcular el número de puertos temporales usados.

Paso 6 Calcule el uso de puertos temporales utilizando la siguiente fórmula: Uso de puertos temporales = (Número de puertos temporales usados/Número total de puertos temporales) x 100. Compruebe si el uso excede el umbral.

- En caso afirmativo, vaya a **Paso 8**.
- Si no, vaya a **Paso 7**.

Paso 7 Espere 5 minutos y compruebe si la alarma está desactivada.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 8**.

Comprobar si el entorno de sistema es normal.

Paso 8 Ejecute el siguiente comando para importar el archivo temporal y ver los puertos más utilizados en el archivo **port_result.txt**:

netstat -tnp > $BIGDATA_HOME/tmp/port_result.txt

```
netstat -tnp

Active Internet connections (w/o servers)

Proto Recv Send LocalAddress ForeignAddress State PID/ProgramName tcp   0   0
10-120-85-154:45433  10-120-8:25009 CLOSE_WAIT 94237/java
tcp   0   0 10-120-85-154:45434  10-120-8:25009 CLOSE_WAIT 94237/java
tcp   0   0 10-120-85-154:45435  10-120-8:25009 CLOSE_WAIT 94237/java
...
```

Paso 9 Ejecute el siguiente comando para comprobar los procesos que ocupan un gran número de puertos:

ps -ef |grep *PID*

NOTA

- *PID* indica el ID de proceso del puerto consultado en **Paso 8**.
- Ejecute el siguiente comando para recopilar información sobre todos los procesos del sistema y comprobar los procesos que ocupan un gran número de puertos:

  ps -ef > $BIGDATA_HOME/tmp/ps_result.txt

Paso 10 Póngase en contacto con el administrador del sistema para despejar los procesos que ocupan un gran número de puertos. Espere 5 minutos y compruebe si la alarma está desactivada.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 11**.

Paso 11 Recopilar información de fallas.

1. En MRS Manager, seleccione **System** > **Export Log**.
2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Referencia

Ninguna

8.5.37 ALM-12053 El uso del identificador de archivo supera el umbral (para MRS 2.*x* o anterior)

Descripción

El sistema comprueba el uso del identificador cada 30 segundos. Esta alarma se genera cuando el uso del identificador excede el umbral (el umbral predeterminado es de **80%**) varias veces (el valor predeterminado es de **5**).

Puede cambiar el umbral seleccionando **System** > **Threshold Configuration** > **Device** > **Host** > **Host Status** > **Host File Handle Usage** > **Host File Handle Usage**.

Si el **hit number** es de **1**, esta alarma se borra cuando el uso del identificador de archivo es menor o igual al umbral. Si el **hit number** es mayor que **1**, esta alarma se borra cuando el uso del identificador de archivo es menor o igual al 90% del umbral.

Atributo

ID de alarma	Gravedad de alarma	Borrar automáticamente
12053	Grave	Sí

Parámetros

Parámetro	Descripción
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger Condition	Especifica el umbral para activar la alarma.

Impacto en el sistema

Las aplicaciones del sistema no pueden abrir archivos, acceder a redes y realizar otras operaciones de E/S. Las aplicaciones se están ejecutando incorrectamente.

Causas posibles

- El número de identificadores de archivo no cumple con los requisitos de servicio.
- El sistema no funciona normalmente.

Procedimiento

Aumentar el número de identificadores de archivo.

Paso 1 Vaya a la página de detalles del clúster de MRS y elija **Alarms**.

Paso 2 En la lista de alarmas en tiempo real, haga clic en la alarma. En el área **Alarm Details**, obtenga la dirección IP del host para el que se genera la alarma.

Paso 3 Utilice PuTTY para iniciar sesión en el host para el que se genera la alarma como usuario **root**.

Paso 4 Ejecute el comando **ulimit -n** para comprobar el número máximo de identificadores establecidos en el sistema.

Paso 5 Si el uso del identificador de archivo excede el umbral, póngase en contacto con el administrador del sistema para aumentar el número de identificadores de archivo del sistema.

Paso 6 Espere 5 minutos y compruebe si la alarma está desactivada.

- En caso afirmativo, no es necesario hacer nada más.

- Si no, vaya a **Paso 7**.

Comprobar si el entorno de sistema es normal.

Paso 7 Póngase en contacto con el administrador del sistema para comprobar si el sistema operativo es anormal.

- En caso afirmativo, rectifique la falla del sistema operativo y vaya a **Paso 8**.
- Si no, vaya a **Paso 9**.

Paso 8 Espere 5 minutos y compruebe si la alarma está desactivada.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 9**.

Paso 9 Recopilar información de fallas.

1. En MRS Manager, seleccione **System** > **Export Log**.
2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Referencia

Ninguna

8.5.38 ALM-12054 Archivo de certificado no válido (Para MRS 2.*x* o anterior)

Descripción

El sistema comprueba si el archivo de certificado no es válido (ha caducado o aún no es válido) a las 23:00 todos los días. Esta alarma se genera cuando el archivo de certificado no es válido.

Esta alarma se borra cuando el estado del certificado recién importado es válido.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
12054	Grave	Sí

Parámetros

Parámetro	Descripción
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.

Parámetro	Descripción
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

El sistema recuerda a los usuarios que el archivo de certificado no es válido. Si el archivo de certificado no es válido, algunas funciones están restringidas y no se pueden usar correctamente.

Causas posibles

No se importa ningún certificado (certificado raíz HA o certificado de usuario HA) en el sistema, el certificado no se importa o el archivo de certificado no es válido.

Procedimiento

Comprobar la causa de la alarma.

Paso 1 Vaya a la página de detalles del clúster de MRS y elija **Alarms**.

Paso 2 En la lista de alarmas en tiempo real, haga clic en la fila que contiene la alarma.

En el área **Alarm Details**, vea la información adicional sobre la alarma.

- Si aparece **CA Certificate** en la información de alarma adicional, utilice PuTTY para iniciar sesión en el nodo de gestión de OMS activo como usuario **omm** y vaya a **Paso 3**.
- Si aparece **HA root Certificate** en la información adicional, marque **Location** para obtener el nombre del host involucrado en esta alarma. A continuación, utilice PuTTY para iniciar sesión en el host como usuario **omm** y vaya a **Paso 4**.
- Si aparece **HA server Certificate** en la información adicional, marque **Location** para obtener el nombre del host involucrado en esta alarma. A continuación, utilice PuTTY para iniciar sesión en el host como usuario **omm** y vaya a **Paso 5**.

Verificar el período de validez de los archivos del certificado en el sistema.

Paso 3 Compruebe si la hora actual del sistema está en el período de validez del certificado de CA.

Ejecute el comando **openssl x509 -noout -text -in ${CONTROLLER_HOME}/security/cert/root/ca.crt** para comprobar el tiempo efectivo y el tiempo de vencimiento del certificado raíz.

- En caso afirmativo, vaya a **Paso 8**.
- Si no, vaya a **Paso 6**.

Paso 4 Compruebe si la hora actual del sistema está en el período de validez del certificado raíz de HA.

Ejecute el comando **openssl x509 -noout -text -in ${CONTROLLER_HOME}/security/certHA/root-ca.crt** para comprobar el tiempo efectivo y el tiempo de vencimiento del certificado raíz HA.

- En caso afirmativo, vaya a **Paso 8**.
- Si no, vaya a **Paso 7**.

Paso 5 Compruebe si la hora actual del sistema está en el período de validez del certificado de usuario de HA.

Ejecute el comando **openssl x509 -noout -text -in ${CONTROLLER_HOME}/security/certHA/server.crt** para comprobar el tiempo efectivo y el tiempo de vencimiento del certificado de usuario HA.

- En caso afirmativo, vaya a **Paso 8**.
- Si no, vaya a **Paso 7**.

  A continuación se muestra un ejemplo del tiempo efectivo y el tiempo de caducidad de un certificado de CA o HA:

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            97:d5:0e:84:af:ec:34:d8
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=CountryName, ST=State, L=Locality, O=Organization, OU=IT,
CN=HADOOP.COM
        Validity
            Not Before: Dec 13 06:38:26 2016 GMT            // Effective time
            Not After : Dec 11 06:38:26 2026 GMT            // Expiration
time
```

Importar archivos de certificado.

Paso 6 Importar un nuevo archivo de certificado de CA.

Póngase en contacto con el personal de O&M para solicitar o generar un nuevo archivo de certificado de CA e importarlo. Borre manualmente la alarma y compruebe si esta alarma se genera de nuevo durante la comprobación periódica.

- En caso afirmativo, vaya a **Paso 8**.
- En caso negativo, no se requiere ninguna otra acción.

Paso 7 Importe un nuevo archivo de certificado HA.

Solicite o genere un nuevo archivo de certificado HA e impórtelo haciendo referencia a **Sustitución del certificado de HA**. Borre manualmente la alarma y compruebe si esta alarma se genera de nuevo durante la comprobación periódica.

- En caso afirmativo, vaya a **Paso 8**.
- En caso negativo, no se requiere ninguna otra acción.

Paso 8 Recopilar información de fallas.

1. En MRS Manager, seleccione **System** > **Export Log**.
2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Referencia

Para obtener más información acerca de cómo manejar un certificado OBS caducado, consulte **Certificado de OBS caducado en un clúster**.

8.5.39 ALM-12055 El archivo de certificado está a punto de caducar (Para MRS 2.*x* o anterior)

Descripción

El sistema comprueba el archivo de certificado a las 23:00 todos los días. Esta alarma se genera si el archivo de certificado está a punto de expirar con un período de validez inferior a días establecido en el umbral de alarma.

Esta alarma se genera si el estado del certificado recién importado es válido.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
12055	Menor	Sí

Parámetros

Parámetro	Descripción
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

El sistema recuerda a los usuarios que la licencia está a punto de caducar. Si la licencia expira, algunas funciones están restringidas y no se pueden usar correctamente.

Causas posibles

El período de validez restante del certificado de CA, el certificado raíz de HA o el certificado de usuario de HA es menor que el umbral de alarma.

Procedimiento

Comprobar la causa de la alarma.

Paso 1 Vaya a la página de detalles del clúster de MRS y elija **Alarms**.

Paso 2 En la lista de alarmas en tiempo real, haga clic en la fila que contiene la alarma.

En el área **Alarm Details**, vea la información adicional sobre la alarma.

- Si aparece **CA Certificate** en la información de alarma adicional, utilice PuTTY para iniciar sesión en el nodo de gestión de OMS activo como usuario **omm** y vaya a **Paso 3**.
- Si aparece **HA root Certificate** en la información adicional, marque **Location** para obtener el nombre del host involucrado en esta alarma. A continuación, utilice PuTTY para iniciar sesión en el host como usuario **omm** y vaya a **Paso 4**.
- Si aparece **HA server Certificate** en la información adicional, marque **Location** para obtener el nombre del host involucrado en esta alarma. A continuación, utilice PuTTY para iniciar sesión en el host como usuario **omm** y vaya a **Paso 5**.

Verificar el período de validez de los archivos del certificado en el sistema.

Paso 3 Compruebe si el período de validez restante del certificado de CA es menor que el umbral de alarma.

Ejecute el comando **openssl x509 -noout -text -in ${CONTROLLER_HOME}/security/cert/root/ca.crt** para comprobar el tiempo efectivo y el tiempo de vencimiento del certificado raíz.

- En caso afirmativo, vaya a **Paso 6**.
- Si no, vaya a **Paso 8**.

Paso 4 Compruebe si el período de validez restante del certificado raíz de HA es menor que el umbral de alarma.

Ejecute el comando **openssl x509 -noout -text -in ${CONTROLLER_HOME}/security/certHA/root-ca.crt** para comprobar el tiempo efectivo y el tiempo de vencimiento del certificado raíz HA.

- En caso afirmativo, vaya a **Paso 7**.
- Si no, vaya a **Paso 8**.

Paso 5 Compruebe si el período de validez restante del certificado de usuario de HA es menor que el umbral de alarma.

Ejecute el comando **openssl x509 -noout -text -in ${CONTROLLER_HOME}/security/certHA/server.crt** para comprobar el tiempo efectivo y el tiempo de vencimiento del certificado de usuario HA.

- En caso afirmativo, vaya a **Paso 7**.
- Si no, vaya a **Paso 8**.

  A continuación se muestra un ejemplo del tiempo efectivo y el tiempo de caducidad de un certificado de CA o HA:

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            97:d5:0e:84:af:ec:34:d8
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=CountryName, ST=State, L=Locality, O=Organization, OU=IT,
CN=HADOOP.COM
        Validity
            Not Before: Dec 13 06:38:26 2016 GMT             // Effective time
            Not After : Dec 11 06:38:26 2026 GMT             // Expiration
time
```

Importar archivos de certificado.

Paso 6 Importar un nuevo archivo de certificado de CA.

Póngase en contacto con el personal de O&M para solicitar o generar un nuevo archivo de certificado de CA e importarlo. Borre manualmente la alarma y compruebe si esta alarma se genera de nuevo durante la comprobación periódica.

- En caso afirmativo, vaya a **Paso 8**.
- En caso negativo, no se requiere ninguna otra acción.

Paso 7 Importe un nuevo archivo de certificado HA.

Solicite o genere un nuevo archivo de certificado HA e impórtelo haciendo referencia a **Sustitución del certificado de HA**. Borre manualmente la alarma y compruebe si esta alarma se genera de nuevo durante la comprobación periódica.

- En caso afirmativo, vaya a **Paso 8**.
- En caso negativo, no se requiere ninguna otra acción.

Paso 8 Recopilar información de fallas.

1. En MRS Manager, seleccione **System** > **Export Log**.
2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Referencia

Para obtener más información acerca de cómo manejar un certificado OBS caducado, consulte **Certificado OBS caducado en un clúster**.

8.5.40 ALM-12180 Disk Card I/O (For MRS 2.*x* or Earlier)

Description

For MRS 2.*x* or earlier:

- For HDDs, the alarm is triggered when any of the following conditions is met:
  - The system collects data every 3 seconds, and detects that the **svctm** value exceeds 6s for 10 consecutive periods within 30 seconds.
  - The system collects data every 3 seconds, and detects that the **avgqu-sz** value is greater than 0, the IOPS or bandwidth is 0, and the **ioutil** value is greater than **99%** for 10 consecutive periods within 30 seconds.
- For SSDs, the alarm is triggered when any of the following conditions is met:
  - The system collects data every 3 seconds, and detects that the **svctm** value exceeds 2s for 10 consecutive periods within 30 seconds.
  - The system collects data every 3 seconds, and detects that the **avgqu-sz** value is greater than 0, the IOPS or bandwidth is 0, and the **ioutil** value is greater than **99%** for 10 consecutive periods within 30 seconds.

This alarm is automatically cleared when none of the conditions are met for 90 seconds.

For MRS 1.9.3.10 or later:

- For HDDs, the alarm is triggered when any of the following conditions is met:

  - By default, the system collects data every 3 seconds. The svctm latency reaches 6 seconds within 30 seconds in at least seven collection periods.
  - By default, the system collects data every 3 seconds. Disk queue depth (**avgqu-sz**) > 0 and IOPS = 0, or bandwidth = 0 and **ioutil** > 99% in at least 10 collection periods within 30 seconds.
  - By default, the system collects data every 3 seconds. At least 50% of detected svctm take no less than 1000 ms within 300 seconds.
- For SSDs, the alarm is triggered when any of the following conditions is met:
  - By default, the system collects data every 3 seconds. The svctm latency reaches 3 seconds within 30 seconds in at least seven collection periods.
  - By default, the system collects data every 3 seconds. Disk queue depth (**avgqu-sz**) > 0 and IOPS = 0, or bandwidth = 0 and **ioutil** > 99% in at least 10 collection periods within 30 seconds.
  - By default, the system collects data every 3 seconds. At least 50% of detected svctm take no less than 500 ms within 300 seconds.

The collection period is 3 seconds, and the detection period is 30 or 300 seconds. This alarm is automatically cleared when none of the conditions are met for three consecutive detection periods (30 or 300 seconds).

NOTA

For details about how to obtain related parameters, see **Related Information**.

Attribute

Alarm ID	Alarm Severity	Auto Clear
12180	Major	Yes

Parameters

Parameter	Description
Source	Specifies the cluster or system for which the alarm is generated.
ServiceName	Specifies the service for which the alarm is generated.
RoleName	Specifies the role for which the alarm is generated.
HostName	Specifies the host for which the alarm is generated.
DiskName	Specifies the disk for which the alarm is generated.

Impact on the System

A continuously high I/O usage may adversely affect service operations and result in service loss.

Possible Causes

The disk is aged.

Procedure

Replace the disk.

Paso 1 Log in to FusionInsight Manager and choose **O&M** > **Alarm** > **Alarms**.

Paso 2 View the detailed information about the alarm. Check the values of **HostName** and **DiskName** in the location information to obtain the information about the faulty disk for which the alarm is reported.

Paso 3 Replace the faulty disk.

Paso 4 Check whether the alarm is cleared.

- If yes, no further action is required.
- If no, perform **Paso 5**.

Collect the fault information.

Paso 5 On MRS Manager, choose **System** > **Export Log**.

Paso 6 Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Alarm Clearing

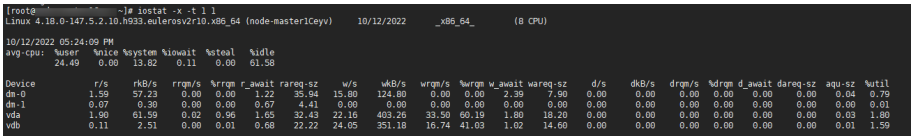
This alarm is automatically cleared after the fault is rectified.

Related Information

To obtain the related parameters, perform the following steps:

- Run the following command in the OS to collect data:

  iostat -x -t 1 1



  The command parameters are as follows:

  avgqu-sz indicates the disk queue depth.

  The sum of **r/s** and **w/s** is the IOPS.

  The sum of **rkB/s** and **wkB/s** is the bandwidth.

  %util is the value of **ioutil**.

- The value of **svctm** is calculated as follows:

  svctm = (tot_ticks_new - tot_ticks_old) / (rd_ios_new + wr_ios_new - rd_ios_old - wr_ios_old)

  For MRS 2.*x* or earlier:

  If **rd_ios_new + wr_ios_new - rd_ios_old - wr_ios_old** is **0**, then **svctm** is **0**.

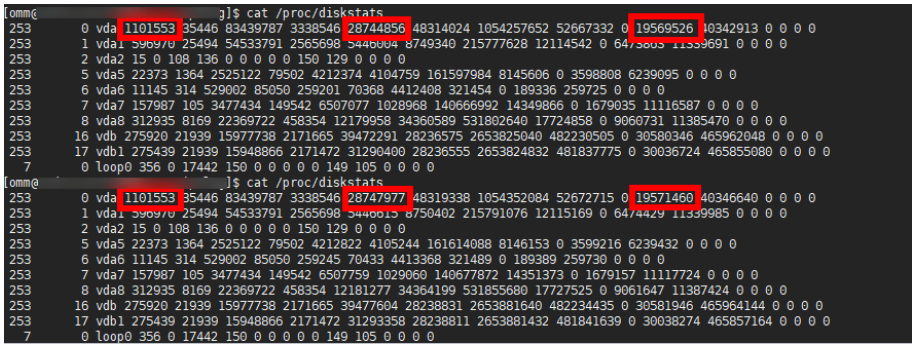
  For MRS 1.9.3.10 or later:

  When the detection period is 30 seconds, if **rd_ios_new + wr_ios_new - rd_ios_old - wr_ios_old = 0**, then **svctm = 0**.

  When the detection period is 300 seconds and **rd_ios_new + wr_ios_new - rd_ios_old - wr_ios_old = 0**, if **tot_ticks_new - tot_ticks_old = 0**, then **svctm = 0**; otherwise, the value of **svctm** is infinite.

  The parameters in the preceding expression can be obtained as follows:

  Obtain the parameter values from the data collected via the **cat /proc/diskstats** command run by the system every 3 seconds. The following shows an example.



  In the data collected for the first time, the number in the fourth column is the value of **rd_ios_old**, the number in the eighth column is the value of **wr_ios_old**, and the number in the thirteenth column is the value of **tot_ticks_old**.

  In the data collected for the second time, the number in the fourth column is the value of **rd_ios_new**, the number in the eighth column is the value of **wr_ios_new**, and the number in the thirteenth column is the value of **tot_ticks_new**.

  In this case, the value of **svctm** is as follows:

  (19571460 - 19569526) / (1101553 + 28747977 - 1101553 - 28744856) = 0.6197

8.5.41 ALM-12357 Error al exportar registros de auditoría a OBS (Para MRS 2.*x* o anterior)

Descripción

Si el usuario ha configurado la exportación del registro de auditoría a la OBS en MRS Manager, el sistema exporta regularmente los registros de auditoría a la OBS. Esta alarma se notifica si el sistema no puede acceder a OBS.

Esta alarma se borra después de que el sistema exporte los registros de auditoría a la OBS correctamente.

Atributo

ID de alarma	Gravedad de alarma	Borrar automáticamente
12357	Grave	Sí

Parámetros

Parámetro	Descripción
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

El sistema local guarda un máximo de siete archivos de registro de auditoría de servicio comprimidos. Si esta alarma persiste, es posible que se pierdan los registros de auditoría del servicio local.

El sistema local guarda un máximo de 50 archivos de registro de auditoría de gestión (cada archivo contiene 100,000 registros). Si esta alarma persiste, es posible que se pierdan los registros de auditoría de la gestión local.

Causas posibles

- Se produce un error en la conexión al servidor de OBS.
- El sistema de archivos de OBS especificado no existe.
- La información de AK/SK del usuario no es válida.
- No se puede obtener la configuración de OBS local.

Procedimiento

Paso 1 Inicie sesión en el servidor de OBS y compruebe si se puede acceder correctamente al servidor de OBS.

- En caso afirmativo, vaya a **Paso 3**.
- Si no, vaya a **Paso 2**.

Paso 2 Póngase en contacto con el personal de mantenimiento para reparar OBS. Después compruebe si la alarma se ha rectificado.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 3**.

Paso 3 En MRS Manager, seleccione **System** > **Export Audit Log**. Compruebe si la información de AK/SK, el nombre del sistema de archivos y la ruta son correctas.

- En caso afirmativo, vaya a **Paso 5**.
- Si no, vaya a **Paso 4**.

Paso 4 Corrija la información. A continuación, compruebe si la alarma se borra cuando la tarea de exportación se ejecuta de nuevo.

NOTA

Para comprobar la liquidación de alarmas rápidamente, puede establecer la hora de inicio de la recopilación de registros de auditoría en 10 o 30 minutos más tarde que la hora actual. Después de comprobar el resultado, restaure la hora de inicio original.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 5**.

Paso 5 Recopilar información de fallas.

1. En MRS Manager, seleccione **System** > **Export Log**.
2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Información relacionada

N/A

8.5.42 ALM-13000 El servicio ZooKeeper no está disponible (Para MRS 2.*x* o anterior)

Descripción

El sistema comprueba el estado del servicio ZooKeeper cada 30 segundos. Esta alarma se genera cuando el servicio ZooKeeper no está disponible.

Esta alarma se borra cuando se recupera el servicio ZooKeeper.

Atributo

ID de alarma	Gravedad de alarma	Borrar automáticamente
13000	Crítica	Sí

Parámetros

Parámetro	Descripción
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.

Parámetro	Descripción
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

ZooKeeper no proporciona servicios de coordinación para componentes de capa superior y los componentes que dependen de ZooKeeper pueden no funcionar correctamente.

Causas posibles

- La instancia de ZooKeeper es anormal.
- La capacidad del disco es insuficiente.
- La red está defectuosa.
- El DNS se instala en el nodo de ZooKeeper.

Procedimiento

Verificar el estado de la instancia del servicio ZooKeeper.

Paso 1 En la página de detalles del clúster de MRS, seleccione **Components** > **ZooKeeper** > **quorumpeer**.

Paso 2 Compruebe si las instancias ZooKeeper son normales.

- En caso afirmativo, vaya a **Paso 6**.
- Si no, vaya a **Paso 3**.

Paso 3 Seleccione instancias cuyo estado no es bueno y elija **More** > **Restart Instance**.

Paso 4 Compruebe si el estado de la instancia es bueno después del reinicio.

- En caso afirmativo, vaya a **Paso 5**.
- Si no, vaya a **Paso 19**.

Paso 5 En la página de pestaña **Alarms**, compruebe si la alarma está desactivada.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 6**.

Comprobar estado de disco.

Paso 6 En la página de detalles del clúster de MRS, elija **Components** > **ZooKeeper** > **quorumpeer** y compruebe la información de host de cada nodo que alberga la instancia del ZooKeeper.

Paso 7 En la página de detalles del clúster de MRS, haga clic en la pestaña **Nodes** y expanda un grupo de nodos.

Paso 8 En la columna **Disk Usage**, compruebe si el espacio en disco de cada nodo que contiene instancias de ZooKeeper es insuficiente (el uso del disco supera el 80%).

- En caso afirmativo, vaya a **Paso 9**.
- Si no, vaya a **Paso 11**.

Paso 9 Amplíe la capacidad del disco. Para obtener más información, consulte **ALM-12017 Capacidad de disco insuficiente (para MRS 2.x o anterior)**.

Paso 10 En la página de pestaña **Alarms**, compruebe si la alarma está desactivada.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 11**.

Comprobar el estado de comunicación de la red.

Paso 11 En el nodo de Linux que contiene la instancia de ZooKeeper, ejecute el comando **ping** para comprobar si los nombres de host de otros nodos que contienen las instancias de ZooKeeper se pueden hacer pings correctamente.

- En caso afirmativo, vaya a **Paso 15**.
- Si no, vaya a **Paso 12**.

Paso 12 Modifique las direcciones IP de **/etc/hosts** y agregue la asignación entre los nombres de host y las direcciones IP.

Paso 13 Ejecute de nuevo el comando **ping** para comprobar si los nombres de host de otros nodos que albergan las instancias ZooKeeper se pueden hacer pings correctamente.

- En caso afirmativo, vaya a **Paso 14**.
- Si no, vaya a **Paso 19**.

Paso 14 En la página de pestaña **Alarms**, compruebe si la alarma está desactivada.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 15**.

Comprobar el DNS.

Paso 15 Compruebe si el DNS está instalado en el nodo que alberga la instancia de ZooKeeper. En el nodo Linux que contiene la instancia ZooKeeper, ejecute el comando **cat /etc/resolv.conf** para comprobar si el archivo está vacío.

- En caso afirmativo, vaya a **Paso 16**.
- Si no, vaya a **Paso 19**.

Paso 16 Ejecute el comando **service named status** para comprobar si se ha iniciado el DNS.

- En caso afirmativo, vaya a **Paso 17**.
- Si no, vaya a **Paso 19**.

Paso 17 Ejecute el comando **service named stop** para detener el servicio DNS. Si "Shutting down name server BIND waiting for named to shut down (28s)" se muestra, el servicio DNS se detiene correctamente. Comente el contenido (si lo hubiera) en **/etc/resolv.conf**.

Paso 18 En la página de pestaña **Alarms**, compruebe si la alarma está desactivada.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 19**.

Paso 19 Recopilar información de fallas.

1. En MRS Manager, seleccione **System** > **Export Log**.
2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Referencia

Ninguna

8.5.43 ALM-13001 Las conexiones de ZooKeeper disponibles son insuficientes (Para MRS 2.*x* o anterior)

Descripción

El sistema comprueba las conexiones de ZooKeeper cada 30 segundos. Esta alarma se genera cuando el sistema detecta que el número de conexiones de instancia ZooKeeper usadas excede el umbral (80% de las conexiones máximas).

Esta alarma se borra cuando el número de conexiones de instancia de ZooKeeper usadas es menor que el umbral.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
13001	Grave	Sí

Parámetros

Parámetro	Descripción
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger Condition	Genera una alarma cuando el valor real del indicador excede el umbral especificado.

Impacto en el sistema

Las conexiones de ZooKeeper disponibles son insuficientes. Cuando el uso de la conexión alcanza el 100%, las conexiones externas no se pueden manejar.

Causas posibles

El número de conexiones al nodo de ZooKeeper supera el umbral. La fuga de conexión ocurre en algunos procesos de conexión, o el número máximo de conexiones no cumple con el requisito del escenario real.

Procedimiento

Paso 1 Compruebe el estado de la conexión.

1. En la página de detalles del clúster de MRS, elija **Alarms** > **ALM-13001 Available ZooKeeper Connections Are Insufficient** > **Location**. Compruebe la dirección IP del nodo para el que se genera la alarma.
2. Obtenga el PID del proceso de ZooKeeper. Inicie sesión en el nodo para el que se genera esta alarma y ejecute el comando **pgrep -f proc_zookeeper**.
3. Compruebe si el PID se puede obtener correctamente.
   - En caso afirmativo, vaya a **Paso 1.4**.
   - Si no, vaya a **Paso 2**.
4. Obtenga todas las direcciones IP conectadas a la instancia de ZooKeeper y el número de conexiones y compruebe 10 direcciones IP con conexiones superiores. Ejecute el comando **lsof -i|grep $pid | awk '{print $9}' | cut -d : -f 2 | cut -d \> -f 2 | awk '{a[$1]++} END {for(i in a){print i,a[i] | "sort -r -g -k 2"}}' | head -10** basado en el valor de PID obtenido. (**$pid** es el PID obtenido en el paso anterior.)
5. Compruebe si las direcciones IP del nodo y el número de conexiones se obtienen correctamente.
   - En caso afirmativo, vaya a **Paso 1.6**.
   - Si no, vaya a **Paso 2**.
6. Obtenga el ID del puerto conectado al proceso. Ejecute el comando **lsof -i|grep $pid | awk '{print $9}'|cut -d \> -f 2 |grep $IP| cut -d : -f 2** basado en el PID y la dirección IP obtenidas. (**$pid** y **$IP** son el PID y la dirección IP obtenidas en el paso anterior.)
7. Compruebe si el ID de puerto se ha obtenido correctamente.
   - En caso afirmativo, vaya a **Paso 1.8**.
   - Si no, vaya a **Paso 2**.
8. Obtenga el ID del proceso conectado. Inicie sesión en cada dirección IP y ejecute el siguiente comando basado en el ID de puerto obtenido: **lsof -i|grep $port**. (**$port** es el ID de puerto obtenido en el paso anterior.)
9. Compruebe si el ID de proceso se obtiene correctamente.
   - En caso afirmativo, vaya a **Paso 1.10**.
   - Si no, vaya a **Paso 2**.
10. Compruebe si se produce una fuga de conexión en el proceso basándose en el ID de proceso obtenido.
    - En caso afirmativo, vaya a **Paso 1.11**.
    - Si no, vaya a **Paso 1.12**.
11. Cierre el proceso donde se produce una fuga de conexión y compruebe si la alarma está desactivada.
    - En caso afirmativo, no es necesario hacer nada más.
    - Si no, vaya a **Paso 1.12**.
12. En la página de detalles del clúster de MRS, seleccione **Components** > **ZooKeeper** > **Service Configuration**. Establezca **Type** en **All** y elija **quorumpeer** > **Performance** y cambie el valor de **maxCnxns** a **20000** o más.
13. Verifique si la alarma se ha borrado.

– En caso afirmativo, no es necesario hacer nada más.
– Si no, vaya a **Paso 2**.

Paso 2 Recopilar información de fallas.

1. En MRS Manager, seleccione **System** > **Export Log**.
2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Referencia

Ninguna

8.5.44 ALM-13002 El uso de memoria de ZooKeeper supera el umbral (Para MRS 2.*x* o anterior)

Descripción

El sistema comprueba el estado del servicio ZooKeeper cada 30 segundos. La alarma se genera cuando el uso de memoria de una instancia de ZooKeeper excede el umbral (80% de la memoria máxima).

La alarma se borra cuando el uso de memoria es menor que el umbral.

Atributo

ID de alarma	Gravedad de alarma	Borrar automáticamente
13002	Grave	Sí

Parámetros

Parámetro	Descripción
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger Condition	Genera una alarma cuando el valor real del indicador excede el umbral especificado.

Impacto en el sistema

Si la memoria ZooKeeper disponible es insuficiente, se produce un desbordamiento de memoria y el servicio se interrumpe.

Causas posibles

El uso de memoria de la instancia de ZooKeeper se utiliza en exceso o la memoria se asigna de forma inapropiada.

Procedimiento

Paso 1 Compruebe el uso de la memoria.

1. En la página de detalles del clúster de MRS, elija **Alarms** > **ALM-13002 ZooKeeper Memory Usage Exceeds the Threshold** > **Location**. Compruebe la dirección IP de la instancia para la que se genera la alarma.
2. En la página de detalles del clúster MRS, elija **Components** > **ZooKeeper** > **Instances** > **quorumpeer** (Dirección IP de la instancia para la que se genera la alarma) > **Customize** > **ZooKeeper Heap And Direct Buffer Resource**. Compruebe el uso de la memoria heap.
3. Compruebe si la memoria heap utilizada de ZooKeeper alcanza el 80% de la memoria heap máxima especificada para ZooKeeper.
   - En caso afirmativo, vaya a **Paso 1.4**.
   - Si no, vaya a **Paso 1.6**.
4. En MRS Manager, elija **Services** > **ZooKeeper** > **Configuration** > **All** > **quorumpeer** > **System**. Aumente el valor de **-Xmx** en **GC_OPTS** según sea necesario.
5. Verifique si la alarma se ha borrado.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 1.6**.
6. En la página de detalles del clúster MRS, elija **Components** > **ZooKeeper** > **Instances** > **quorumpeer** (Dirección IP de la instancia para la que se genera la alarma) > **Customize** > **ZooKeeper Heap And Direct Buffer Resource**. Compruebe el uso de la memoria directa intermedia.
7. Compruebe si la memoria intermedia directa utilizada de ZooKeeper alcanza el 80% de la memoria intermedia directa máxima especificada para ZooKeeper.
   - En caso afirmativo, vaya a **Paso 1.8**.
   - Si no, vaya a **Paso 2**.
8. En la página de detalles del clúster de MRS, seleccione **Components** > **ZooKeeper** > **Service Configuration**. Establezca **Type** en **All** y elija **quorumpeer** > **System**.

   Aumente el valor de **-XX:MaxDirectMemorySize** en **GC_OPTS** según sea necesario.
9. Verifique si la alarma se ha borrado.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 2**.

Paso 2 Recopilar información de fallas.

1. En MRS Manager, seleccione **System** > **Export Log**.
2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Referencia

Ninguna

8.5.45 ALM-14000 Servicio HDFS no disponible (para MRS 2.*x* o anterior)

Descripción

El sistema comprueba el estado del servicio de NameService cada 30 segundos. Esta alarma se genera cuando el sistema considera que el servicio HDFS no está disponible porque todos los servicios NameService son anormales.

Esta alarma se borra cuando al menos un servicio NameService es normal y el sistema considera que el servicio HDFS se recupera.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
14000	Crítica	Sí

Parámetros

Parámetro	Descripción
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

HDFS no proporciona servicios para componentes de capa superior basados en servicios HDFS, como HBase y MapReduce. Como resultado, los usuarios no pueden leer ni escribir archivos.

Causas posibles

- ZooKeeper es anormal.
- Todos los servicios de NameService son anormales.

Procedimiento

Paso 1 Compruebe el estado del ZooKeeper.

1. Vaya a la página de detalles del clúster de MRS. En la página de la pestaña **Components**, compruebe si el estado del servicio ZooKeeper es **Good**.
   - En caso afirmativo, vaya a **Paso 1.2**.

- Si no, vaya a **Paso 2.1**.

2. Rectificar el estado de salud del servicio ZooKeeper. Para obtener más información, consulte **ALM-13000 El servicio ZooKeeper no está disponible (Para MRS 2.x o anterior)**. A continuación, compruebe si el estado de salud del servicio ZooKeeper es **Good**.
   - En caso afirmativo, vaya a **Paso 1.3**.
   - Si no, vaya a **Paso 3**.
3. Espere 5 minutos y compruebe si la alarma está desactivada.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 2.1**.

Paso 2 Maneje la alarma de excepción de servicio NameService.

1. Vaya a la página de detalles del clúster de MRS. En la página **Alarms**, compruebe si todos los servicios de NameService tienen alarmas anormales.
   - En caso afirmativo, vaya a **Paso 2.2**.
   - Si no, vaya a **Paso 3**.
2. Maneje los servicios NameService anormales siguiendo las instrucciones en **ALM-14010 NameService es anormal (Para MRS 2.x o anterior)** y comprobar si cada alarma de excepción de servicio NameService está borrada.
   - En caso afirmativo, vaya a **Paso 2.3**.
   - Si no, vaya a **Paso 3**.
3. Espere 5 minutos y compruebe si la alarma está desactivada.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 3**.

Paso 3 Recopile información de fallas.

1. En MRS Manager, seleccione **System** > **Export Log**.
2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Referencia

Ninguna

8.5.46 ALM-14001 El uso del disco de HDFS supera el umbral (Para MRS 2.*x* o anterior)

Descripción

El sistema comprueba el uso del disco del clúster HDFS cada 30 segundos y compara el uso real del disco con el umbral. El indicador de uso de disco de clúster HDFS tiene un umbral predeterminado. Esta alarma se genera cuando el uso del disco HDFS excede el umbral.

Esta alarma se borra cuando el uso del disco del clúster HDFS es menor o igual al umbral.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
14001	Grave	Sí

Parámetros

Parámetro	Descripción
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
NSName	Especifica el servicio NameService para el que se genera la alarma.
Trigger condition	Genera una alarma cuando el valor real del indicador excede el umbral especificado.

Impacto en el sistema

El rendimiento de la escritura de datos en HDFS se ve afectado.

Causas posibles

El espacio en disco configurado para el clúster HDFS es insuficiente.

Procedimiento

Paso 1 Compruebe la capacidad del disco y elimine los archivos innecesarios.

1. En la página de detalles del clúster MRS, seleccione **Components** > **HDFS**. Se muestra la página **Service Status**.
2. En el área **Charts**, vea el valor del indicador de monitoreo **Percentage of HDFS Capacity** para comprobar si el uso del disco de HDFS excede el umbral (80% de forma predeterminada).
   - En caso afirmativo, vaya a **Paso 1.3**.
   - Si no, vaya a **Paso 3**.
3. Utilice el cliente en el nodo del clúster y ejecute el comando **hdfs dfsadmin -report** para comprobar si el valor de **DFS Used%** es inferior al 100% menos el umbral.
   - En caso afirmativo, vaya a **Paso 1.5**.
   - Si no, vaya a **Paso 3**.
4. Utilice el cliente en el nodo del clúster y ejecute el comando **hdfs dfs -rm -r** *file or directory path* para eliminar archivos innecesarios.

5. Espere 5 minutos y compruebe si la alarma está desactivada.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 2.1**.

Paso 2 Expanda el sistema.

1. Amplíe la capacidad del disco.
2. Espere 5 minutos y compruebe si la alarma está desactivada.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 3**.

Paso 3 Recopilar información de fallas.

1. En MRS Manager, seleccione **System** > **Export Log**.
2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Referencia

Ninguna

8.5.47 ALM-14002 El uso del disco de DataNode supera el umbral (Para MRS 2.*x* o anterior)

Descripción

El sistema comprueba el uso del disco de DataNode cada 30 segundos y compara el uso real del disco con el umbral. El indicador **Percentage of DataNode Capacity** tiene un umbral predeterminado. Esta alarma se genera cuando el valor del indicador **Percentage of DataNode Capacity** excede el umbral.

Esta alarma se borra cuando el valor del indicador **Percentage of DataNode Capacity** es menor o igual que el umbral.

Atributo

ID de alarma	Gravedad de alarma	Borrar automáticamente
14002	Grave	Sí

Parámetros

Parámetro	Descripción
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.

Parámetro	Descripción
HostName	Especifica el host para el que se genera la alarma.
Trigger condition	Genera una alarma cuando el valor real del indicador excede el umbral especificado.

Impacto en el sistema

La falta de espacio en disco afectará a la lectura/escritura en HDFS.

Causas posibles

- El espacio en disco configurado para el clúster HDFS es insuficiente.
- La desviación de los datos se produce entre los DataNodes.

Procedimiento

Paso 1 Compruebe la capacidad del disco del clúster.

1. Vaya a la página de detalles del clúster de MRS. En la página **Alarms**, compruebe si existe la alarma ALM-14001 El uso de disco de HDFS excede el umbral.
   - En caso afirmativo, vaya a **Paso 1.2**.
   - Si no, vaya a **Paso 2.1**.
2. Maneje la alarma siguiendo las instrucciones en ALM-14001 El uso de disco de HDFS excede el umbral y compruebe si la alarma está borrada.
   - En caso afirmativo, vaya a **Paso 1.3**.
   - Si no, vaya a **Paso 3**.
3. Espere 5 minutos y compruebe si la alarma está desactivada.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 2.1**.

Paso 2 Comprueba el estado del saldo de DataNodes.

1. Utilice el cliente en el nodo del clúster, ejecute el comando **hdfs dfsadmin -report** para ver el valor de **DFS Used%** en el DataNode para el que se genera la alarma y compare el valor con los de otros DataNodes. Compruebe si la diferencia entre los valores es mayor que 10.
   - En caso afirmativo, vaya a **Paso 2.2**.
   - Si no, vaya a **Paso 3**.
2. Si se produce un sesgo de datos, utilice el cliente en el nodo del clúster y ejecute el comando **hdfs balancer -threshold 10**.
3. Espere 5 minutos y compruebe si la alarma está desactivada.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 3**.

Paso 3 Recopilar información de fallas.

1. En MRS Manager, seleccione **System** > **Export Log**.
2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Referencia

Ninguna

8.5.48 ALM-14003 El número de bloques HDFS perdidos supera el umbral (Para MRS 2.*x* o anterior)

Descripción

El sistema comprueba el número de bloques perdidos cada 30 segundos y compara el número de bloques perdidos con el umbral. El indicador de bloques perdidos tiene un umbral predeterminado. Esta alarma se genera cuando el número de bloques perdidos excede el umbral.

Esta alarma se borra cuando el número de bloques perdidos es menor o igual que el umbral.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
14003	Grave	Sí

Parámetros

Parámetro	Descripción
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
NSName	Especifica el servicio NameService para el que se genera la alarma.
Trigger condition	Genera una alarma cuando el valor real del indicador excede el umbral especificado.

Impacto en el sistema

Los datos almacenados en HDFS se pierden. HDFS puede entrar en el modo seguro y no puede proporcionar servicios de escritura. Los datos de bloques perdidos no se pueden restaurar.

Causas posibles

- La instancia DataNode es anormal.
- Los datos se eliminan.

Procedimiento

Paso 1 Compruebe la instancia DataNode.

1. En la página de detalles del clúster MRS, seleccione **Components** > **HDFS** > **Instances**.
2. Compruebe si el estado de todas las instancias de DataNode es **Good**.
   - En caso afirmativo, vaya a **Paso 3**.
   - Si no, vaya a **Paso 1.3**.
3. Reinicie la instancia DataNode y compruebe si el reinicio se realiza correctamente.
   - En caso afirmativo, vaya a **Paso 2.2**.
   - Si no, vaya a **Paso 2.1**.

Paso 2 Elimine el archivo dañado.

1. Utilice el cliente en el nodo del clúster. Ejecute el comando **hdfs fsck / -delete** para eliminar el archivo perdido. A continuación, vuelva a escribir el archivo y recuperar los datos.
2. Espere 5 minutos y compruebe si la alarma está desactivada.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 3**.

Paso 3 Recopile información de fallas.

1. En MRS Manager, seleccione **System** > **Export Log**.
2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Referencia

Ninguna

8.5.49 ALM-14004 El número de bloques HDFS dañados supera el umbral (Para MRS 2.*x* o anterior)

Descripción

El sistema comprueba el número de bloques dañados cada 30 segundos y compara el número de bloques dañados con el umbral. El indicador de bloques dañados tiene un umbral predeterminado. Esta alarma se genera cuando el número de bloques dañados excede el umbral.

Esta alarma se borra cuando el número de bloques dañados es menor o igual que el umbral. Se recomienda ejecutar el comando **hdfs fsck /** para comprobar si algún archivo está completamente dañado.

Atributo

ID de alarma	Gravedad de alarma	Borrar automáticamente
14004	Grave	Sí

Parámetros

Parámetro	Descripción
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
NSName	Especifica el servicio NameService para el que se genera la alarma.
Trigger condition	Genera una alarma cuando el valor real del indicador excede el umbral especificado.

Impacto en el sistema

Los datos están dañados y HDFS no puede leer archivos.

Causas posibles

- La instancia DataNode es anormal.
- La información de verificación de datos está dañada.

Procedimiento

Paso 1 Recopilar información de fallas.

1. En MRS Manager, seleccione **System** > **Export Log**.
2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Referencia

Ninguna

8.5.50 ALM-14006 El número de archivos de HDFS supera el umbral (Para MRS 2.*x* o anterior)

Descripción

El sistema comprueba periódicamente el número de archivos de HDFS cada 30 segundos y compara el número de archivos de HDFS con el umbral. Esta alarma se genera cuando el sistema detecta que el número de archivos de HDFS excede el umbral.

Esta alarma se borra cuando el número de archivos de HDFS es menor o igual al umbral.

Atributo

ID de alarma	Gravedad de alarma	Borrar automáticamente
14006	Grave	Sí

Parámetros

Parámetro	Descripción
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
NSName	Especifica el servicio NameService para el que se genera la alarma.
Trigger condition	Genera una alarma cuando el valor real del indicador excede el umbral especificado.

Impacto en el sistema

El espacio de almacenamiento en disco es insuficiente, lo que puede provocar un error en la importación de datos. El rendimiento del sistema HDFS se ve afectado.

Causas posibles

El número de archivos de HDFS excede el umbral.

Procedimiento

Paso 1 Compruebe si existen archivos innecesarios en el sistema.

1. Utilice el cliente en el nodo del clúster y ejecute el comando **hdfs dfs -ls** *file or directory path* para comprobar si se puede eliminar el archivo o el directorio.

- En caso afirmativo, vaya a **Paso 1.2**.
- Si no, vaya a **Paso 2.1**.

2. Ejecute el comando **hdfs dfs -rm -r** *file or directory path*. Elimine los archivos innecesarios, espere 5 minutos y compruebe si la alarma está desactivada.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 2.1**.

Paso 2 Compruebe el número de archivos en el sistema.

1. En MRS Manager, elija **System** > **Threshold Configuration**.
2. En el árbol de navegación de la izquierda, elija **Services** > **HDFS** > **HDFS File** > **Total Number of Files**.
3. En el panel derecho, modifique el umbral de la regla en función del número de archivos de HDFS actuales.

   Para comprobar el número de archivos de HDFS, elija **Services** > **HDFS**, haga clic en **Customize** en el área **Real-Time Statistics** de la derecha y seleccione el elemento de monitoreo de **HDFS File**.
4. Espere 5 minutos y compruebe si la alarma está desactivada.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 3**.

Paso 3 Recopilar información de fallas.

1. En MRS Manager, seleccione **System** > **Export Log**.
2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Referencia

Ninguna

8.5.51 ALM-14007 El uso de memoria de NameNode de HDFS supera el umbral (Para MRS 2.*x* o anterior)

Descripción

El sistema comprueba el uso de la memoria de NameNode de HDFS cada 30 segundos y compara el uso real de la memoria con el umbral. El uso de memoria de NameNode de HDFS tiene un umbral predeterminado. Esta alarma se genera cuando el uso de memoria de NameNode de HDFS excede el umbral.

Esta alarma se borra cuando el uso de memoria de NameNode de HDFS es menor o igual que el umbral.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
14007	Grave	Sí

Parámetros

Parámetro	Descripción
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger condition	Genera una alarma cuando el valor real del indicador excede el umbral especificado.

Impacto en el sistema

Si el uso de memoria del HDFS NameNode es demasiado alto, el rendimiento de lectura/escritura de datos de HDFS se verá afectado.

Causas posibles

La memoria de NameNode de HDFS es insuficiente.

Procedimiento

Paso 1 Borre todos los archivos innecesarios.

1. Utilice el cliente en el nodo del clúster y ejecute el comando **hdfs dfs -rm -r** *file or directory path* para eliminar archivos innecesarios.
2. Espere 5 minutos y compruebe si la alarma está desactivada.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 2**.

Paso 2 Recopilar información de fallas.

1. En MRS Manager, seleccione **System** > **Export Log**.
2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Referencia

Ninguna

8.5.52 ALM-14008 El uso de memoria de HDFS DataNode supera el umbral (para MRS 2.*x* o anterior)

Descripción

El sistema comprueba el uso de la memoria de HDFS DataNode cada 30 segundos y compara el uso real de la memoria con el umbral. El uso de memoria de HDFS DataNode tiene un

umbral predeterminado. Esta alarma se genera cuando el uso de memoria de HDFS DataNode excede el umbral.

Esta alarma se borra cuando el uso de memoria de HDFS DataNode es menor o igual que el umbral.

Atributo

ID de alarma	Gravedad de alarma	Borrar automáticamente
14007	Grave	Sí

Parámetros

Parámetro	Descripción
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger condition	Genera una alarma cuando el valor real del indicador excede el umbral especificado.

Impacto en el sistema

El uso de memoria de HDFS DataNode es demasiado alto, lo que afecta al rendimiento de lectura/escritura de datos del HDFS.

Causas posibles

La memoria de HDFS DataNode es insuficiente.

Procedimiento

Paso 1 Borre todos los archivos innecesarios.

1. Utilice el cliente en el nodo del clúster y ejecute el comando **hdfs dfs -rm -r** *file or directory path* para eliminar archivos innecesarios.
2. Espere 5 minutos y compruebe si la alarma está desactivada.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 2**.

Paso 2 Recopilar información de fallas.

1. En MRS Manager, seleccione **System** > **Export Log**.

2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Referencia

Ninguna

8.5.53 ALM-14009 El número de DataNodes defectuoso supera el umbral (para MRS 2.*x* o anterior)

Descripción

El sistema comprueba periódicamente el número de DataNodes defectuosos en el clúster HDFS cada 30 segundos y compara el número con el umbral. El número de DataNodes defectuosos tiene un umbral predeterminado. Esta alarma se genera cuando el número de DataNodes defectuosos en el clúster HDFS excede el umbral.

Esta alarma se borra cuando el número de DataNodes defectuosos en el clúster HDFS es menor o igual que el umbral.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
14009	Grave	Sí

Parámetros

Parámetro	Descripción
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger condition	Genera una alarma cuando el valor real del indicador excede el umbral especificado.

Impacto en el sistema

Los DataNodes defectuosos no pueden proporcionar servicios HDFS.

Causas posibles

- DataNodes están defectuosos o sobrecargados.

- La red entre el NameNode y el DataNode está desconectada u ocupada.
- Los NameNodes están sobrecargados.

Procedimiento

Paso 1 Compruebe si los DataNodes son defectuosos.

1. Utilice el cliente en el nodo del clúster y ejecute el comando **hdfs dfsadmin -report** para comprobar si las DataNodes son defectuosas.
   - En caso afirmativo, vaya a **Paso 1.2**.
   - Si no, vaya a **Paso 2.1**.
2. En la página de detalles del clúster MRS, elija **Components** > **HDFS** > **Instances** para comprobar si el DataNode está detenido.
   - En caso afirmativo, vaya a **Paso 1.3**.
   - Si no, vaya a **Paso 2.1**.
3. Seleccione la instancia DataNode y elija **More** > **Restart Instance** para reiniciarla. Espere 5 minutos y compruebe si la alarma está desactivada.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 2.1**.

Paso 2 Compruebe el estado de la red entre el NameNode y el DataNode.

1. Inicie sesión en la dirección IP del servicio del nodo donde se encuentra el DataNode defectuoso y ejecute el comando **ping** *IP address of the NameNode* para comprobar si la red entre el DataNode y el NameNode es anormal.
   - En caso afirmativo, vaya a **Paso 2.2**.
   - Si no, vaya a **Paso 3.1**.
2. Rectifique el fallo de la red. Espere 5 minutos y compruebe si la alarma está desactivada.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 3.1**.

Paso 3 Compruebe si el DataNode está sobrecargado.

1. En la página de detalles del clúster MRS, haga clic en **Alarms** y compruebe si existe la alarma ALM-14008 El uso de memoria de HDFS DataNode supera el umbral.
   - En caso afirmativo, vaya a **Paso 3.2**.
   - Si no, vaya a **Paso 4.1**.
2. Siga los procedimientos de **ALM-14008 El uso de memoria de HDFS DataNode supera el umbral (para MRS 2.x o anterior)** para manejar la alarma y comprobar si la alarma está desactivada.
   - En caso afirmativo, vaya a **Paso 3.3**.
   - Si no, vaya a **Paso 4.1**.
3. Espere 5 minutos y compruebe si la alarma está desactivada.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 4.1**.

Paso 4 Compruebe si el NameNode está sobrecargado.

1. En la página de detalles del clúster MRS, haga clic en **Alarms** y compruebe si la alarma ALM-14007 El uso de memoria de HDFS NameNode supera el umbral.

- En caso afirmativo, vaya a **Paso 4.2**.
- Si no, vaya a **Paso 5**.

2. Siga los procedimientos de **ALM-14007 El uso de memoria de NameNode de HDFS supera el umbral (Para MRS 2.x o anterior)** para manejar la alarma y comprobar si la alarma está desactivada.
   - En caso afirmativo, vaya a **Paso 4.3**.
   - Si no, vaya a **Paso 5**.
3. Espere 5 minutos y compruebe si la alarma está desactivada.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 5**.

Paso 5 Recopile información de fallas.

1. En MRS Manager, seleccione **System** > **Export Log**.
2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Referencia

Ninguna

8.5.54 ALM-14010 NameService es anormal (Para MRS 2.*x* o anterior)

Descripción

El sistema comprueba el estado del servicio NameService cada 180 segundos. Esta alarma se genera cuando el servicio NameService no está disponible.

Esta alarma se borra cuando se recupera el servicio NameService.

Atributo

ID de alarma	Gravedad de alarma	Borrar automáticamente
14010	Grave	Sí

Parámetros

Parámetro	Descripción
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.

Parámetro	Descripción
HostName	Especifica el host para el que se genera la alarma.
NSName	Especifica el servicio NameService para el que se genera la alarma.

Impacto en el sistema

HDFS no proporciona servicios para componentes de capa superior basados en el servicio NameService, como HBase y MapReduce. Como resultado, los usuarios no pueden leer ni escribir archivos.

Causas posibles

- El JournalNode es defectuosa.
- El DataNode está defectuoso.
- La capacidad del disco es insuficiente.
- El NameNode entra en modo seguro.

Procedimiento

Paso 1 Compruebe el estado de la instancia de JournalNode.

1. En la página de inicio del MRS Manager haga clic en **Components**.
2. Haga clic en **HDFS**.
3. Haga clic en **Instance**.
4. Comprueba si el **Health Status** del JournalNode es **Good**.
   - En caso afirmativo, vaya a **Paso 2.1**.
   - Si no, vaya a **Paso 1.5**.
5. Seleccione el JournalNode defectuoso y elija **More** > **Restart Instance**. Compruebe si el JournalNode se reinicia correctamente.
   - En caso afirmativo, vaya a **Paso 1.6**.
   - Si no, vaya a **Paso 5**.
6. Espere 5 minutos y compruebe si la alarma está desactivada.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 2.1**.

Paso 2 Compruebe el estado de la instancia de DataNode.

1. En la página de detalles del clúster de MRS, haga clic en **Components**.
2. Haga clic en **HDFS**.
3. En el caso de **Operation and Health Summary**, compruebe si el **Health Status** de todos los DataNodes es **Good**.
   - En caso afirmativo, vaya a **Paso 3.1**.
   - Si no, vaya a **Paso 2.4**.

4. Haga clic en **Instances**. En la página de gestión del DataNode, seleccione el DataNode defectuoso y elija **More** > **Restart Instance**. Compruebe si el DataNode se reinicia correctamente.
   - En caso afirmativo, vaya a **Paso 2.5**.
   - Si no, vaya a **Paso 3.1**.
5. Espere 5 minutos y compruebe si la alarma está desactivada.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 4.1**.

Paso 3 Verifique el estado del disco.

1. En la página de detalles del clúster de MRS, haga clic en la pestaña **Nodes** y expanda un grupo de nodos.
2. En la columna **Disk Usage**, compruebe si el espacio en disco es insuficiente.
   - En caso afirmativo, vaya a **Paso 3.3**.
   - Si no, vaya a **Paso 4.1**.
3. Amplíe la capacidad del disco.
4. Espere 5 minutos y compruebe si la alarma está desactivada.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 4.1**.

Paso 4 Compruebe si NameNode está en el modo seguro.

1. Utilice el cliente en el nodo del clúster y ejecute el comando **hdfs dfsadmin -safemode get** para comprobar si se muestra **Safe mode is ON**.

   La información detrás de **Safe mode is ON** es información de alarma y se muestra en función de las condiciones reales.
   - En caso afirmativo, vaya a **Paso 4.2**.
   - Si no, vaya a **Paso 5**.
2. Utilice el cliente en el nodo del clúster y ejecute el comando **hdfs dfsadmin -safemode leave**.
3. Espere 5 minutos y compruebe si la alarma está desactivada.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 5**.

Paso 5 Recopilar información de fallas.

1. En MRS Manager, seleccione **System** > **Export Log**.
2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Referencia

Ninguna

8.5.55 ALM-14011 El directorio de datos de HDFS DataNode no está configurado correctamente (Para MRS 2.*x* o anterior)

Descripción

El parámetro **dfs.datanode.data.dir** especifica el directorio de datos de DataNode. Esta alarma se genera en cualquiera de los siguientes escenarios:

- No se puede crear un directorio de datos configurado.
- Un directorio de datos utiliza el mismo disco que otros directorios críticos del sistema.
- Varios directorios utilizan el mismo disco.

Esta alarma se borra cuando el directorio de datos DataNode está configurado correctamente y este DataNode se reinicia.

Atributo

ID de alarma	Severidad de la alarma	Borrar automáticamente
14011	Grave	Sí

Parámetros

Parámetro	Descripción
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

Si el directorio de datos de DataNode está montado en directorios críticos como el directorio raíz, el espacio en disco del directorio raíz se utilizará después de ejecutarse durante mucho tiempo. Esto provoca una falla del sistema.

Si el directorio de datos de DataNode no está configurado correctamente, el rendimiento de HDFS se deteriorará.

Causas posibles

- No se puede crear el directorio de datos de DataNode.
- El directorio de datos DataNode utiliza el mismo disco que los directorios críticos, como / o **/boot**.
- Varios directorios en el directorio de datos de DataNode utilizan el mismo disco.

Procedimiento

Paso 1 Compruebe la causa de la alarma y la información sobre el DataNode para el que se genera la alarma.

1. En la página de detalles del clúster MRS, haga clic en **Alarms**. En la lista de alarmas, haga clic en la alarma.
2. En el área **Alarm Details**, vea **Alarm Cause** para obtener la causa de la alarma. En el **HostName** de **Location**, se obtiene el nombre de host del DataNode para el que se genera la alarma.

Paso 2 Elimine los directorios que no cumplan con el plan de disco del directorio de datos de DataNode.

1. Elija **Components** >**HDFS** >**Instances**. En la lista de instancias, haga clic en la instancia DataNode en el nodo para el que se genera la alarma.
2. Haga clic en **Instance Configuration** y vea el valor del parámetro DataNode **dfs.datanode.data.dir**.
3. Compruebe si todos los directorios de datos de DataNode son coherentes con el plan de disco.
   - En caso afirmativo, vaya a **Paso 2.4**.
   - Si no, vaya a **Paso 2.7**.
4. Modifique el parámetro de DataNode **dfs.datanode.data.dir** y elimine los directorios incorrectos.
5. Elija **Components** > **HDFS** > **Instances** para reiniciar la instancia de DataNode.
6. Verifique si la alarma se ha borrado.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 2.7**.
7. Inicie sesión en el DataNode para el que se genera la alarma.
   - Si la causa de la alarma es "The DataNode data directory fails to be created", vaya a **Paso 3.1**.
   - Si la causa de la alarma es "The DataNode data directory uses the same disk as critical directories, such / or /**boot**", vaya a **Paso 4.1**.
   - Si la causa de la alarma es "Multiple directories in the DataNode data directory use the same disk", vaya a **Paso 5.1**.

Paso 3 Compruebe si el directorio de datos de DataNode no se puede crear.

1. Ejecute los siguientes comandos para cambiar el usuario:

   sudo su - root

   su - omm
2. Ejecute el comando **ls** para comprobar si los directorios existen en el directorio de datos de DataNode.
   - En caso afirmativo, vaya a **Paso 7**.
   - Si no, vaya a **Paso 3.3**.
3. Ejecute el comando **mkdir** *data directory* para crear un directorio y verifique si el directorio se ha creado correctamente.
   - En caso afirmativo, vaya a **Paso 6.1**.

- Si no, vaya a **Paso 3.4**.

4. Haga clic en **Alarms** para comprobar si existe una alarma ALM-12017 Capacidad de disco insuficiente.
   - En caso afirmativo, vaya a **Paso 3.5**.
   - Si no, vaya a **Paso 3.6**.
5. Ajuste la capacidad del disco y compruebe si la alarma ALM-12017 Capacidad insuficiente del disco está borrada. Para obtener más información, consulte **ALM-12017 Capacidad de disco insuficiente (para MRS 2.x o anterior)**.
   - En caso afirmativo, vaya a **ALM-12017 Capacidad de disco insuficiente (para MRS 2.x o anterior)**.
   - Si no, vaya a **Paso 7**.
6. Compruebe si el usuario **omm** tiene el permiso **rwx** o **x** de todos los directorios de capa superior del directorio. (Por ejemplo, para **/tmp/abc/**, el usuario **omm** tiene el permiso **x** para el directorio **tmp** y el permiso **rwx** para el directorio **abc**.)
   - En caso afirmativo, vaya a **Paso 6.1**.
   - Si no, vaya a **Paso 3.7**.
7. Ejecute el comando **chmod u+rwx** *path* o **chmod u+x** *path* como usuario **root** para agregar el permiso **rwx** o **x** a las rutas de acceso. A continuación, vaya a **Paso 3.3**.

Paso 4 Compruebe si el directorio de datos DataNode utiliza el mismo disco que otros directorios críticos del sistema.

1. Ejecute el comando **df** para obtener la información de montaje en disco de cada directorio en el directorio de datos de DataNode.
2. Compruebe si los directorios montados en el disco son directorios críticos, como / o /**boot**.
   - En caso afirmativo, vaya a **Paso 4.3**.
   - Si no, vaya a **Paso 6.1**.
3. Cambie el valor del parámetro DataNode **dfs.datanode.data.dir** y elimine los directorios que utilizan el mismo disco que los directorios críticos.
4. Vaya a **Paso 6.1**.

Paso 5 Compruebe si varios directorios del directorio de datos DataNode utilizan el mismo disco.

1. Ejecute el comando **df** para obtener la información de montaje en disco de cada directorio en el directorio de datos de DataNode. Registre el directorio montado en la salida del comando.
2. Modifique el parámetro de nodo de DataNode **dfs.DataNode.data.dir** para reservar uno de los directorios montados en el mismo directorio de disco.
3. Vaya a **Paso 6.1**.

Paso 6 Reinicie el DataNode y compruebe si la alarma está desactivada.

1. Elija **Components** > **HDFS** > **Instances** para reiniciar la instancia de DataNode.
2. Verifique si la alarma se ha borrado.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 7**.

Paso 7 Recopilar información de fallas.

1. En MRS Manager, seleccione **System** > **Export Log**.
2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Referencia

Ninguna

8.5.56 ALM-14012 Los datos de Journalnode de HDFS no están sincronizados (Para MRS 2.*x* o anterior)

Descripción

En el NameNode activo, el sistema comprueba la sincronización de datos en todos los JournalNodes del clúster cada 5 minutos. Esta alarma se genera cuando los datos de un JournalNode no están sincronizados con los de otro JournalNodes.

Esta alarma se borra en 5 minutos después de sincronizar los datos de JournalNodes.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
14012	Grave	Sí

Parámetros

Parámetro	Descripción
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
IP	Especifica la dirección IP del servicio de la instancia de JournalNode para la que se genera la alarma.

Impacto en el sistema

Cuando un JournalNode funciona incorrectamente, los datos del nodo no se sincronizan con los de otro JournalNodes. Si los datos de más de la mitad de JournalNodes no están sincronizados, el NameNode no puede funcionar correctamente, lo que hace que el servicio HDFS no esté disponible.

Causas posibles

- La instancia de JournalNode no se ha iniciado o se ha detenido.
- La instancia de JournalNode funciona incorrectamente.
- La red del JournalNode es inalcanzable.

Procedimiento

Paso 1 Compruebe si se ha iniciado la instancia de JournalNode.

1. En la página de detalles del clúster MRS, haga clic en **Alarms**. En la lista de alarmas, haga clic en la alarma.
2. En el área **Alarm Details**, compruebe **Location** y obtenga la dirección IP del JournalNode para el que se genera la alarma.
3. Elija **Components** > **HDFS** > **Instances**. En la lista de instancias, haga clic en el JournalNode para el que se genera la alarma y compruebe si **Operating Status** del nodo es **Started**.
   - En caso afirmativo, vaya a **Paso 2.1**.
   - Si no, vaya a **Paso 1.4**.
4. Seleccione la instancia JournalNode y elija **More** > **Start Instance** para iniciarla.
5. Espere 5 minutos y compruebe si la alarma está desactivada.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 4**.

Paso 2 Compruebe si la instancia de JournalNode funciona correctamente.

1. Comprueba si **Health Status** de la instancia de JournalNode es **Good**.
   - En caso afirmativo, vaya a **Paso 3.1**.
   - Si no, vaya a **Paso 2.2**.
2. Seleccione la instancia JournalNode y elija **More** > **Restart Instance** para reiniciarla.
3. Espere 5 minutos y compruebe si la alarma está desactivada.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 4**.

Paso 3 Compruebe si la red del JournalNode es accesible.

1. En la página de detalles del clúster MRS, elija **Components** > **HDFS** > **Instances** para comprobar la dirección IP del servicio del NameNode activo.
2. Inicie sesión en el NameNode activo.
3. Ejecute el comando **ping** para comprobar si se produce un tiempo de espera o si la red entre el NameNode activo y el JournalNode es inalcanzable.

   ping *service IP address of the JournalNode*
   - En caso afirmativo, vaya a **Paso 3.4**.
   - Si no, vaya a **Paso 4**.
4. Póngase en contacto con el personal de O&M para rectificar la falla de la red. Espere 5 minutos y compruebe si la alarma está desactivada.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 4**.

Paso 4 Recopilar información de fallas.

1. En MRS Manager, seleccione **System** > **Export Log**.
2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Referencia

Ninguna

8.5.57 ALM-16000 Porcentaje de sesiones conectadas al HiveServer al número máximo permitido supera el umbral (Para MRS 2.*x* o anterior)

Descripción

El sistema comprueba el porcentaje de sesiones conectadas al HiveServer hasta el número máximo permitido cada 30 segundos. Este indicador se puede ver en la página de monitoreo del servicio Hive. Esta alarma se genera cuando el porcentaje de sesiones conectadas al HiveServer al número máximo permitido supera el umbral especificado (90% por defecto).

Esta alarma se puede borrar automáticamente cuando el porcentaje es menor o igual al umbral.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
16000	Grave	Sí

Parámetros

Parámetro	Descripción
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger condition	Genera una alarma cuando el valor real del indicador excede el umbral especificado.

Impacto en el sistema

Si se genera una alarma de conexión, se conectan demasiadas sesiones al HiveServer y no se pueden crear nuevas conexiones.

Causas posibles

Hay demasiados clientes conectados al HiveServer.

Procedimiento

Paso 1 Aumente el número máximo de conexiones a Hive.

1. Vaya a la página de detalles del clúster MRS y haga clic en **Components**.
2. Elija **Hive** > **Service Configuration** y cambie **Basic** a **All**.
3. Aumente el valor del elemento de configuración **hive.server.session.control.maxconnections**. Supongamos que el valor del elemento de configuración es A, el umbral es B y las sesiones conectadas al HiveServer son C. Ajuste el valor del elemento de configuración según A x B > C. Las sesiones conectadas al HiveServer se pueden ver en la página de monitoreo de Hive.
4. Verifique si la alarma se ha borrado.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 2**.

Paso 2 Recopile información de fallas.

1. En MRS Manager, seleccione **System** > **Export Log**.
2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Referencia

Ninguna

8.5.58 ALM-16001 El uso del espacio de almacén de Hive supera el umbral (Para MRS 2.*x* o anterior)

Descripción

El sistema comprueba el uso del espacio del almacén de Hive cada 30 segundos. El indicador **Porcentaje de espacio de HDFS utilizado por Hive con respecto al espacio disponible** se puede ver en la página de supervisión del servicio Hive. Esta alarma se genera cuando el uso del espacio del almacén de Hive supera el umbral especificado (85% de forma predeterminada).

Esta alarma se borra cuando el uso del espacio del almacén de Hive es menor o igual que el umbral. Puede reducir el uso del espacio del almacén expandiendo la capacidad del almacén o liberando el espacio usado.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
16001	Grave	Sí

Parámetros

Parámetro	Descripción
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger condition	Genera una alarma cuando el valor real del indicador excede el umbral especificado.

Impacto en el sistema

El sistema no puede escribir datos, lo que causa la pérdida de datos.

Causas posibles

- El límite superior de la capacidad HDFS disponible para Hive es demasiado pequeño.
- El espacio en disco del sistema es insuficiente.
- Algunos nodos de datos se descomponen.

Procedimiento

Paso 1 Expanda la configuración del sistema.

1. Analice el uso de la capacidad HDFS del clúster y aumente el límite superior de la capacidad HDFS disponible para Hive.

   Vaya a la página de detalles del clúster MRS, elija **Components** > **Hive** > **Service Configuration**, establezca **Type** en **All**, busque **hive.metastore.warehouse.size.percent**, y aumente el valor de este parámetro. Supongamos que el valor del elemento de configuración es A, el espacio total de almacenamiento HDFS es B, el umbral es C y el espacio HDFS utilizado por Hive es D. Ajuste el valor del elemento de configuración según A x B x C > D. El espacio total de almacenamiento HDFS se puede ver en la página de monitorización de HDFS, y el espacio HDFS utilizado por Hive se puede ver en la página de monitorización de Hive.
2. Verifique si la alarma se ha borrado.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 2.1**.

Paso 2 Expanda el sistema.

1. Agregue nodos.
2. Verifique si la alarma se ha borrado.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 3.1**.

Paso 3 Compruebe si el nodo de datos es normal.

1. Vaya a la página de detalles del clúster y elija **Alarms**.
2. Compruebe si existe ALM-12006 Falla de nodo, ALM-12007 Falla de proceso o ALM-14002 Uso de disco de DataNode superior al umbral.
   - En caso afirmativo, vaya a **Paso 3.3**.
   - Si no, vaya a **Paso 4**.
3. Borre la alarma siguiendo los pasos indicados en ALM-12006 Falla de nodo, ALM-12007 Falla de proceso o ALM-14002 El uso de disco de DataNode supera el umbral.
4. Verifique si la alarma se ha borrado.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 4**.

Paso 4 Recopilar información de fallas.

1. En MRS Manager, seleccione **System** > **Export Log**.
2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Referencia

Ninguna

8.5.59 ALM-16002 La tasa de éxito de ejecución de Hive SQL es inferior al umbral (Para MRS 2.*x* o anterior)

Descripción

El sistema comprueba el porcentaje de las sentencias de HiveQL que se ejecutan correctamente cada 30 segundos. Porcentaje de sentencias HiveQL ejecutadas correctamente = Número de sentencias HiveQL ejecutadas correctamente por Hive en un periodo determinado/Número total de sentencias HiveQL ejecutadas por Hive. Este indicador se puede ver en la página de monitoreo del servicio Hive. Esta alarma se genera cuando el porcentaje de las sentencias HiveQL que se ejecutan correctamente excede el umbral especificado (90% de forma predeterminada). El nombre del host para el que se genera la alarma se puede obtener a partir de la información de ubicación de la alarma. La dirección IP del host es la dirección IP del nodo HiveServer.

Esta alarma se borra cuando el porcentaje de las sentencias HiveQL que se ejecutan correctamente en un período de prueba es menor o igual que el umbral.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
16002	Grave	Sí

Parámetros

Parámetro	Descripción
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger condition	Especifica el umbral para activar la alarma.

Impacto en el sistema

La configuración y el rendimiento del sistema no pueden cumplir los requisitos de procesamiento del servicio.

Causas posibles

- Se produce un error de sintaxis en los comandos HiveQL.
- El servicio HBase es anormal cuando se está realizando una tarea Hive on HBase.
- Los servicios básicos de los que depende son anormales, como HDFS, Yarn y ZooKeeper.

Procedimiento

Paso 1 Compruebe si los comandos HiveQL cumplen con la sintaxis.

1. Utilice el cliente Hive para iniciar sesión en el nodo HiveServer para el que se genera la alarma. Consulte el estándar de sintaxis HiveQL proporcionado por Apache y compruebe si los comandos HiveQL son correctos. Para obtener más información, consulte **https://cwiki.apache.org/confluence/display/hive/languagemanual**.
   - En caso afirmativo, vaya a **Paso 2.1**.
   - Si no, vaya a **Paso 1.2**.

   NOTA

   Para ver al usuario que ejecuta una sentencia incorrecta, descargue los registros de HiveServerAudit del nodo HiveServer para el que se genera esta alarma. Ajuste **Start time** y **End time** a 10 minutos antes y después del tiempo de generación de alarma respectivamente. Abra el archivo de registro y busque la palabra clave **Result=FAIL** para filtrar la información de registro sobre la sentencia incorrecta y, a continuación, vea el usuario que ejecuta la sentencia incorrecta según **UserName** en la información de registro.

2. Ingrese las sentencias HiveQL correctas y compruebe si el comando se puede ejecutar correctamente.
   - En caso afirmativo, vaya a **Paso 4.5**.
   - Si no, vaya a **Paso 2.1**.

Paso 2 Compruebe si el servicio HBase es anormal.

1. Compruebe si se realiza una tarea Hive on HBase.
   - En caso afirmativo, vaya a **Paso 2.2**.
   - Si no, vaya a **Paso 3.1**.
2. Compruebe si el servicio HBase es normal en la lista de servicios.
   - En caso afirmativo, vaya a **Paso 3.1**.
   - Si no, vaya a **Paso 2.3**.
3. Compruebe las alarmas mostradas en la página de alarmas y bórrelas según **Alarm Help**.
4. Ingrese las sentencias HiveQL correctas y compruebe si el comando se puede ejecutar correctamente.
   - En caso afirmativo, vaya a **Paso 4.5**.
   - Si no, vaya a **Paso 3.1**.

Paso 3 Compruebe si el servicio Spark es anormal.

1. Compruebe si el servicio Spark es normal en la lista de servicios.
   - En caso afirmativo, vaya a **Paso 4.1**.
   - Si no, vaya a **Paso 3.2**.
2. Compruebe las alarmas mostradas en la página de alarmas y bórrelas según **Alarm Help**.
3. Ingrese las sentencias HiveQL correctas y compruebe si el comando se puede ejecutar correctamente.
   - En caso afirmativo, vaya a **Paso 4.5**.
   - Si no, vaya a **Paso 4.1**.

Paso 4 Compruebe si HDFS, Yarn y ZooKeeper son normales.

1. Vaya a la página de detalles del clúster MRS y haga clic en **Components**.
2. En la lista de servicios, compruebe si los servicios, como HDFS, Yarn y ZooKeeper son normales.
   - En caso afirmativo, vaya a **Paso 4.5**.
   - Si no, vaya a **Paso 4.3**.
3. Compruebe las alarmas mostradas en la página de alarmas y bórrelas según **Alarm Help**.
4. Ingrese las sentencias HiveQL correctas y compruebe si el comando se puede ejecutar correctamente.
   - En caso afirmativo, vaya a **Paso 4.5**.
   - Si no, vaya a **Paso 5**.
5. Espere un minuto y compruebe si la alarma está desactivada.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 5**.

Paso 5 Recopilar información de fallas.

1. En MRS Manager, elija **System** > **Export Log**.
2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Referencia

Ninguna

8.5.60 ALM-16004 El servicio Hive no está disponible (Para MRS 2.*x* o anterior)

Descripción

El sistema comprueba el estado del servicio Hive cada 30 segundos. Esta alarma se genera cuando el servicio Hive no está disponible.

Esta alarma se borra cuando se recupera el servicio Hive.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
16004	Crítica	Sí

Parámetros

Parámetro	Descripción
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

El sistema no puede proporcionar servicios de carga, consulta y extracción de datos.

Causas posibles

- Los servicios básicos, como ZooKeeper HDFS, Yarn y DBService funcionan incorrectamente o el proceso Hive es defectuoso.
  - ZooKeeper es anormal.
  - HDFS es anormal.

  - Yarn es anormal.
  - DBService es anormal.
  - El proceso de servicio de Hive es defectuoso. Si la alarma es causada por una falla del proceso Hive, el informe de alarma tiene un retraso de aproximadamente 5 minutos.
- La comunicación de red entre el servicio Hive y los servicios básicos se interrumpe.

Procedimiento

Paso 1 Compruebe el estado del proceso HiveServer/MetaStore.

1. Vaya a la página de detalles del clúster MRS y haga clic en **Components**.
2. Elija **Hive** > **Instances**. En la lista de instancias de Hive, compruebe si el estado de todas las instancias de HiveSserver/MetaStore es **Unknown**.
   - En caso afirmativo, vaya a **Paso 1.3**.
   - Si no, vaya a **Paso 2**.
3. Encima de la lista de instancias de Hive, elija **More** > **Restart Instance** para reiniciar el proceso HiveServer/MetaStore.
4. En la lista de alarmas, compruebe si ALM-16004 Servicio Hive no disponible está desactivado.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 2**.

Paso 2 Compruebe el estado del ZooKeeper.

1. Vaya a la página de detalles del clúster y elija **Alarms**.
2. En MRS Manager, compruebe si se notifica la alarma ALM-12007 Falla de proceso.
   - En caso afirmativo, vaya a **Paso 2.3**.
   - Si no, vaya a **Paso 3**.
3. En el área **Alarm Details** de la falla de proceso ALM-12007, compruebe si **ServiceName** es **ZooKeeper**.
   - En caso afirmativo, vaya a **Paso 2.4**.
   - Si no, vaya a **Paso 3**.
4. Rectifique la falla siguiendo los pasos proporcionados en ALM-12007 Falla de proceso.
5. En la lista de alarmas, compruebe si ALM-16004 Servicio Hive no disponible está desactivado.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 3**.

Paso 3 Compruebe el estado de HDFS.

1. Vaya a la página de detalles del clúster y elija **Alarms**.
2. En la lista de alarmas, compruebe si existe la alarma ALM-14000 Servicio HDFS no disponible.
   - En caso afirmativo, vaya a **Paso 3.3**.
   - Si no, vaya a **Paso 4**.
3. Rectifique la falla siguiendo los pasos proporcionados en ALM-14000 El servicio HDFS no disponible.

4. En la lista de alarmas, compruebe si ALM-16004 Servicio Hive no disponible está desactivado.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 4**.

Paso 4 Compruebe el estado de Yarn.

1. Vaya a la página de detalles del clúster y elija **Alarms**.
2. En la lista de alarmas de MRS Manager, compruebe si se genera la alarma ALM-18000 Servicio Yarn no disponible.
   - En caso afirmativo, vaya a **Paso 4.3**.
   - Si no, vaya a **Paso 4**.
3. Rectifique la falla siguiendo los pasos proporcionados en ALM-18000 Servicio Yarn no disponible.
4. En la lista de alarmas, compruebe si ALM-16004 Servicio Hive no disponible está desactivado.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 4**.

Paso 5 Compruebe el estado de DBService.

1. Vaya a la página de detalles del clúster y elija **Alarms**.
2. En la lista de alarmas en MRS Manager, compruebe si se genera ALM-27001 DBService no disponible.
   - En caso afirmativo, vaya a **Paso 5.3**.
   - Si no, vaya a **Paso 6**.
3. Rectificar la falla siguiendo el procedimiento de tratamiento en **ALM-27001 DBService no disponible (Para MRS 2.x o anterior)**.
4. En la lista de alarmas, compruebe si ALM-16004 Servicio Hive no disponible está desactivado.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 6**.

Paso 6 Compruebe la conexión de red entre Hive y ZooKeeper, HDFS, Yarn y DBService.

1. Vaya a la página de detalles del clúster MRS y haga clic en **Components**.
2. Haga clic en **Hive**.
3. Haga clic en **Instances**.

   Se muestra la lista de instancias HiveServer.
4. Haga clic en **Host Name** en la fila de **HiveServer**.

   Se muestra la página de estado del host HiveServer.
5. Registre la dirección IP en **Summary**.
6. Utilice la dirección IP obtenida en el archivo **Paso 6.5** para iniciar sesión en el host donde se encuentra HiveServer.
7. Ejecute el comando **ping** para comprobar si la conexión de red entre el host que ejecuta HiveServer y los hosts que ejecutan los servicios ZooKeeper, HDFS, Yarn, y DBService es normal. Los métodos para obtener direcciones IP de los hosts que ejecutan servicios ZooKeeper, HDFS, Yarn, y DBService, así como la dirección IP HiveServer son los mismos.

- En caso afirmativo, vaya a **Paso 7**.
- Si no, vaya a **Paso 6.8**.

8. Póngase en contacto con el personal de O&M para restaurar la red.
9. En la lista de alarmas, compruebe si ALM-16004 Servicio Hive no disponible está desactivado.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 7**.

Paso 7 Recopilar información de fallas.

1. En MRS Manager, elija **System** > **Export Log**.
2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Referencia

Ninguna

8.5.61 ALM-16005 Número de ejecuciones de Hive SQL fallidas en el último período supera el umbral (para MRS 2.*x* o anterior)

Descripción

El sistema comprueba si el número de sentencias de Hive SQL que no se pueden ejecutar ha excedido el umbral en el último período de 10 minutos. Esta alarma se genera cuando el número de ejecuciones de sentencia SQL Hive fallidas en los últimos 10 minutos es mayor que el umbral. En los próximos 10 minutos, si el número de ejecuciones de sentencias SQL de Hive fallidas es menor que el umbral, la alarma se borra automáticamente.

Atributo

ID de alarma	Gravedad de alarma	Borrar automáticamente
16005	Grave	Sí

Parámetro

Parámetro	Descripción
ServiceName	Servicio para el que se genera la alarma.
RoleName	Rol para el que se genera la alarma.
HostName	Host para el que se genera la alarma.

Impacto en el sistema

Ninguna

Causas posibles

La sintaxis de Hive SQL es incorrecta. Como resultado, no se pueden ejecutar las sentencias de Hive SQL.

Procedimiento

Compruebe las sentencias de Hive SQL que no se pueden ejecutar, corrija la sintaxis y ejecute las sentencias de SQL de nuevo.

Referencia

Ninguna

8.5.62 ALM-18000 Servicio de Yarn no disponible (Para MRS 2.*x* o anterior)

Descripción

El módulo de alarma comprueba el estado del servicio de Yarn cada 30 segundos. Esta alarma se genera cuando el servicio Yarn no está disponible.

Esta alarma se borra cuando se recupera el servicio Yarn.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
18000	Crítica	Sí

Parámetros

Parámetro	Descripción
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

El clúster no puede proporcionar el servicio Yarn. Los usuarios no pueden ejecutar aplicaciones nuevas. Las aplicaciones enviadas no se pueden ejecutar.

Causas posibles

- ZooKeeper es anormal.
- HDFS es anormal.
- No hay ningún nodo de ResourceManager activo en el clúster de Yarn.
- Todos los nodos de NodeManager en el clúster de Yarn son anormales.

Procedimiento

Paso 1 Compruebe el estado del ZooKeeper.

1. Vaya a la página de detalles del clúster y elija **Alarms**.
2. En la lista de alarmas, compruebe si existe la alarma ALM-13000 El servicio ZooKeeper no disponible.
   - En caso afirmativo, vaya a **Paso 1.3**.
   - Si no, vaya a **Paso 2.2**.
3. Rectificar la falla siguiendo el procedimiento de tratamiento en **ALM-13000 El servicio ZooKeeper no está disponible (Para MRS 2.x o anterior)**. A continuación, compruebe si esta alarma está desactivada.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 2.2**.

Paso 2 Compruebe el estado de HDFS.

1. Vaya a la página de detalles del clúster y elija **Alarms**.
2. En la lista de alarmas, compruebe si se genera una alarma de HDFS.
   - En caso afirmativo, vaya a **Paso 2.3**.
   - Si no, vaya a **Paso 3.2**.
3. Haga clic en **Alarms** y maneje las alarmas HDFS de acuerdo con la norma **Alarm Help**. Verifique si la alarma se ha borrado.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 3.2**.

Paso 3 Compruebe el estado del ResorceManager en el clúster de Yarn.

1. Vaya a la página de detalles del clúster MRS y haga clic en **Components**.
2. Haga clic en **Yarn**.
3. En el clúster de **Yarn Summary**, compruebe si hay un nodo de ResourceManager activo en el clúster de Yarn.
   - En caso afirmativo, vaya a **Paso 4.2**.
   - Si no, vaya a **Paso 5**.

Paso 4 Compruebe el estado del nodo NodeManager en el clúster de Yarn.

1. Vaya a la página de detalles del clúster MRS y haga clic en **Components**.
2. Elija **Yarn** > **Instances**.
3. Verifique **Health Status** de NodeManager y verifique si hay nodos no saludables.
   - En caso afirmativo, vaya a **Paso 4.4**.
   - Si no, vaya a **Paso 5**.

4. Rectificar la falta siguiendo el procedimiento previsto en **ALM-18002 Pérdida de latido de NodeManager (Para MRS 2.x o anterior)** o **ALM-18003 NodeManager de mal funcionamiento (para MRS 2.x o anterior)**. A continuación, compruebe si esta alarma está desactivada.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 5**.

Paso 5 Recopilar información de fallas.

1. En MRS Manager, elija **System** > **Export Log**.
2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Referencia

Ninguna

8.5.63 ALM-18002 Pérdida de latido de NodeManager (Para MRS 2.*x* o anterior)

Descripción

El sistema comprueba el número de nodos de NodeManager perdidos cada 30 segundos, y compara el número de nodos perdidos con el umbral. El indicador **Lost Nodes** tiene un umbral predeterminado. Esta alarma se genera cuando el valor del indicador **Lost Nodes** excede el umbral.

Esta alarma se borra cuando el valor de **Lost Nodes** es menor o igual que el umbral.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
18002	Grave	Sí

Parámetros

Parámetro	Descripción
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger condition	Genera una alarma cuando el valor real del indicador excede el umbral especificado.

Impacto en el sistema

- El nodo NodeManager perdido no puede proporcionar el servicio Yarn.
- El número de contenedores disminuye, por lo que el rendimiento del clúster se deteriora.

Causas posibles

- NodeManager se elimina por la fuerza sin darse de baja.
- Todas las instancias de NodeManager se detienen o el proceso NodeManager es defectuoso.
- El host donde reside el nodo NodeManager es defectuoso.
- La red entre el NodeManager y el ResourceManager está desconectada u ocupada.

Procedimiento

Paso 1 Recopile información de fallas.

1. En MRS Manager, elija **System** > **Export Log**.
2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Referencia

Ninguna

8.5.64 ALM-18003 NodeManager de mal funcionamiento (para MRS 2.*x* o anterior)

Descripción

El sistema comprueba el número de nodos anormales de NodeManager cada 30 segundos y compara el número de nodos anormales con el umbral. El indicador **Unhealthy Nodes** tiene un umbral predeterminado. Esta alarma se genera cuando el valor del indicador **Unhealthy Nodes** excede el umbral.

Esta alarma se borra cuando el valor de **Unhealthy Nodes** es menor o igual que el umbral.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
18003	Grave	Sí

Parámetros

Parámetro	Descripción
ServiceName	Especifica el servicio para el que se genera la alarma.

Parámetro	Descripción
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger condition	Genera una alarma cuando el valor real del indicador excede el umbral especificado.

Impacto en el sistema

- El nodo de NodeManager defectuoso no puede proporcionar el servicio Yarn.
- El número de contenedores disminuye, por lo que el rendimiento del clúster se deteriora.

Causas posibles

- El espacio en disco del host donde reside el nodo NodeManager es insuficiente.
- El usuario **omm** no tiene permiso para acceder a un directorio local en el nodo de NodeManager.

Procedimiento

Paso 1 Recopile información de fallas.

1. En MRS Manager, elija **System** > **Export Log**.
2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Referencia

Ninguna

8.5.65 ALM-18004 La relación de usabilidad del disco NodeManager es inferior al umbral (para MRS 2.*x* o anterior)

Descripción

El sistema comprueba el espacio disponible en disco de cada nodo NodeManager cada 30 segundos y compara la tasa de disponibilidad del disco con el umbral. Se proporciona un rango de umbral predeterminado para el **NodeManager Disk Usability Ratio**. Esta alarma se genera cuando el sistema detecta que el **NodeManager Disk Usability Ratio** real es menor que el umbral.

Esta alarma se borra automáticamente cuando el valor de **NodeManager Disk Usability Ratio** es mayor que el umbral.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
18004	Grave	Sí

Parámetros

Parámetro	Descripción
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger condition	Especifica el umbral para activar la alarma.

Impacto en el sistema

- El nodo NodeManager cuya tasa de disponibilidad de disco es inferior al umbral puede no proporcionar el servicio Yarn.
- El número de contenedores disminuye, por lo que el rendimiento del clúster puede deteriorarse.

Causas posibles

- El espacio en disco del host donde reside el nodo NodeManager es insuficiente.
- El usuario **omm** no tiene permiso para acceder a un directorio local en el nodo de NodeManager.

Procedimiento

Paso 1 Recopile información de fallas.

1. En MRS Manager, seleccione **System** > **Export Log**.
2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Referencia

Ninguna

8.5.66 ALM-18006 Tiempo de espera de ejecución de trabajos de MapReduce (Para MRS 2.*x* o anterior)

Descripción

El módulo de alarma comprueba la ejecución del trabajo de MapReduce cada 30 segundos. Esta alarma se genera cuando se agota el tiempo de ejecución de un trabajo de MapReduce enviado.

Esta alarma debe borrarse manualmente.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
18006	Grave	No

Parámetros

Parámetro	Descripción
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger condition	Genera una alarma cuando el valor real del indicador excede el umbral especificado.

Impacto en el sistema

Se agota el tiempo de ejecución del trabajo de MapReduce enviado, por lo que no se puede obtener ningún resultado de ejecución. Ejecute el trabajo de nuevo después de rectificar la falla.

Causas posibles

Lleva mucho tiempo ejecutar un trabajo de MapReduce. Sin embargo, el tiempo especificado es menor que el tiempo de ejecución requerido.

Procedimiento

Paso 1 Comprueba si el tiempo está ajustado incorrectamente.

Establezca **-Dapplication.timeout.interval** en un valor mayor o no establezca el parámetro. Compruebe si el trabajo de MapReduce se puede ejecutar.

- En caso afirmativo, vaya a **Paso 2.5**.
- Si no, vaya a **Paso 2.2**.

Paso 2 Compruebe el estado de Yarn.

1. Vaya a la página de detalles del clúster y elija **Alarms**.
2. En la lista de alarmas de MRS Manager, compruebe si se genera la alarma ALM-18000 servicio Yarn no disponible.
   - En caso afirmativo, vaya a **Paso 2.3**.
   - Si no, vaya a **Paso 3**.
3. Rectificar la falla siguiendo el procedimiento de tratamiento de **ALM-18000 Servicio de Yarn no disponible (Para MRS 2.x o anterior)**.
4. Vuelva a ejecutar el comando de trabajo de MapReduce para comprobar si se puede ejecutar el trabajo de MapReduce.
   - En caso afirmativo, vaya a **Paso 2.5**.
   - Si no, vaya a **Paso 4**.
5. En la lista de alarmas, haga clic en  en la columna **Operation** de la alarma para borrarla manualmente. No se requiere ninguna otra acción.

Paso 3 Ajuste el umbral de tiempo de espera.

En MRS Manager, elija **System** > **Threshold Configuration** > **Services** > **Yarn** > **Timed out Applications** y aumente el número máximo de tareas de tiempo de espera permitidas por la regla de umbral actual. Verifique si la alarma se ha borrado.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 4**.

Paso 4 Recopile información de fallas.

1. En MRS Manager, seleccione **System** > **Export Log**.
2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Referencia

Ninguna

8.5.67 ALM-18008 Uso de memoria de Heap de Yarn ResourceManager supera el umbral (Para MRS 2.*x* o anterior)

Descripción

El sistema comprueba el uso de memoria heap de ResourceManager de Yarn cada 30 segundos y compara el uso real con el umbral. La alarma se genera cuando el uso de memoria heap de Yarn ResourceManager excede el umbral (80% de la memoria máxima por defecto).

Para cambiar el umbral, elija **System** > **Threshold Configuration** > **Service** > **Yarn**. La alarma se borra cuando el uso de memoria heap es menor o igual que el umbral.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
18008	Grave	Sí

Parámetros

Parámetro	Descripción
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger Condition	Especifica el umbral para activar la alarma.

Impacto en el sistema

Cuando el uso de memoria heap de Yarn ResourceManager es demasiado alto, el rendimiento del envío y la operación de la tarea de Yarn se ve afectado. Además, se produce un desbordamiento de memoria de modo que el servicio Yarn no está disponible.

Causas posibles

La memoria heap de la instancia de Yarn ResourceManager en el nodo se utiliza en exceso o la memoria heap se asigna de forma inapropiada. Como resultado, el uso excede el umbral.

Procedimiento

Paso 1 Compruebe el uso de la memoria heap.

1. Vaya a la página de detalles del clúster de MRS y elija **Alarms**.
2. Seleccione la alarma cuyo **Alarm ID** sea **18008** y vea la dirección IP y el nombre del rol de la instancia en **Location**.
3. Elija **Components** > **Yarn** > **Instances** > **ResourceManager** (dirección IP de la instancia para la que se genera la alarma) > **Customize** > **Percentage of Used Heap Memory of the ResourceManager**. Compruebe el uso de la memoria heap.
4. Compruebe si el uso de memoria heap de ResourceManager ha alcanzado el umbral (80% de la memoria máxima).
   - En caso afirmativo, vaya a **Paso 1.5**.
   - Si no, vaya a **Paso 2**.
5. Elija **Components** >**Yarn** >**Service Configuration**. Establezca **Type** en **All** y elija **ResourceManager** >**System**. Cambie los valores de **-Xmx** y **-Xms** en el parámetro **GC_OPTS** según los requisitos del sitio para asegurarse de que el valor de **-Xms** es

menor que el de **-Xmx**. Haga clic en **Save Configuration** y seleccione **Restart Role Instance**. Haga clic en **OK**.

6. Verifique si la alarma se ha borrado.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 2**.

Paso 2 Recopilar información de fallas.

1. En MRS Manager, seleccione **System** > **Export Log**.
2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Referencia

Ninguna

8.5.68 ALM-18009 El uso de memoria heap de MapReduce JobHistoryServer supera el umbral (Para MRS 2.*x* o anterior)

Descripción

El sistema comprueba el uso de memoria de pila de MapReduce JobHistoryServer cada 30 segundos y compara el uso real con el umbral. La alarma se genera cuando el uso de memoria heap de MapReduce JobHistoryServer excede el umbral (80% de la memoria máxima por defecto).

Para cambiar el umbral, elija **System** > **Threshold Configuration** > **Service** > **MapReduce**. La alarma se borra cuando el uso de memoria heap es menor o igual que el umbral.

Atributo

ID de alarma	Severidad de alarma	Borrado automáticamente
18009	Grave	Sí

Parámetros

Parámetro	Descripción
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger Condition	Especifica el umbral para activar la alarma.

Impacto en el sistema

Cuando el uso de memoria heap de JobHistoryServer de MapReduce es excesivo, el rendimiento del archivo de registros de MapReduce se ve afectado. Además, se produce un desbordamiento de memoria de modo que el servicio Yarn no está disponible.

Causas posibles

La memoria heap de la instancia de JobHistoryServer de MapReduce en el nodo se utiliza en exceso o la memoria heap se asigna de forma inadecuada. Como resultado, el uso excede el umbral.

Procedimiento

Paso 1 Compruebe el uso de la memoria heap.

1. Vaya a la página de detalles del clúster y elija **Alarms**.
2. Seleccione la alarma cuyo **Alarm ID** sea **18009** y vea la dirección IP y el nombre del rol de la instancia de **Location**.
3. Elija **Components** > **MapReduce** > **Instance** > **JobHistoryServer** (dirección IP de la instancia para la que se genera la alarma) > **Customize** > **JobHistoryServer Heap Memory Usage Statistics**. Compruebe el uso de la memoria heap.
4. Compruebe si el uso de memoria heap de JobHistoryServer ha alcanzado el umbral (80% de la memoria heap máxima).
   - En caso afirmativo, vaya a **Paso 1.5**.
   - Si no, vaya a **Paso 2**.
5. Elija **Components** >**MapReduce** >**Service Configuration**. Establezca **Type** en **All** y elija **JobHistoryServer** >**System**. Aumente el valor de **-Xmx** en el parámetro **GC_OPTS** según sea necesario, haga clic en **Save Configuration** y seleccione **Restart the affected services or instances.** Haga clic en **OK**.
6. Verifique si la alarma se ha borrado.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 2**.

Paso 2 Recopilar información de fallas.

1. En MRS Manager, seleccione **System** > **Export Log**.
2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Referencia

Ninguna

8.5.69 ALM-18010 Número de tareas pendientes de Yarn excede el umbral (Para MRS 2.*x* o anterior)

Descripción

El sistema comprueba el número de tareas pendientes de Yarn cada 30 segundos y compara el número de tareas con el umbral. Esta alarma se genera cuando el número de tareas pendientes excede el umbral.

Puede cambiar el umbral seleccionando **System** > **Configure Alarm Threshold** > **Service** > **Yarn** > **Queue Root Pending Applications** > **Queue Root Pending Applications** en MRS Manager.

Esta alarma se borra cuando el número de tareas pendientes es menor o igual que el umbral.

Atributo

ID de alarma	Severidad de alarma	Borrado automáticamente
18010	Grave	Sí

Parámetros

Parámetro	Descripción
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger Condition	Especifica el umbral para activar la alarma.

Impacto en el sistema

Las tareas se pueden apilar y no se pueden procesar de manera oportuna.

Causas posibles

La capacidad de cálculo del clúster es inferior a la tasa de envío de tareas. Como resultado, la tarea no puede procesarse de manera oportuna después de haber sido enviada.

Procedimiento

Paso 1 Compruebe el uso de la memoria y los vCores en la página Yarn.

Compruebe si los valores de **Memory Used|Memory Total** y **VCores Used|VCores Total** en la página nativa de Yarn alcanzan o se acercan a los valores máximos.

- En caso afirmativo, vaya a **Paso 2**.
- Si no, vaya a **Paso 5**.

Paso 2 Compruebe el número de tareas enviadas.

Compruebe si las tareas en ejecución se envían con una frecuencia normal.

- En caso afirmativo, vaya a **Paso 3**.
- Si no, vaya a **Paso 5**.

Paso 3 Escale horizontal el clúster.

El escalamiento horizontal se basa en los requisitos del sitio. Para obtener más información, consulte **Escalamiento horizontal manual de un clúster**.

Paso 4 Una vez completado el escalamiento horizontal, compruebe si la alarma está desactivada.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 5**.

Paso 5 Recopilar información de fallas.

1. En MRS Manager, seleccione **System** > **Export Log**.
2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Referencia

Ninguna

8.5.70 ALM-18011 Memoria de tareas pendientes de Yarn excede el umbral (Para MRS 2.*x* o anterior)

Descripción

El sistema comprueba la memoria de las tareas pendientes de Yarn cada 30 segundos y compara la memoria con el umbral. Esta alarma se genera cuando la memoria de tareas pendientes excede el umbral.

Puede cambiar el umbral seleccionando **System** > **Configure Alarm Threshold** > **Service** > **Yarn** > **Queue Root Pending Memory** > **Queue Root Pending Memory** en MRS Manager.

Esta alarma se borra cuando la memoria de las tareas pendientes es menor o igual que el umbral.

Atributo

ID de alarma	Gravedad de la alarma	Borrado automáticamente
18011	Grave	Sí

Parámetros

Parámetro	Descripción
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger Condition	Especifica el umbral para activar la alarma.

Impacto en el sistema

Las tareas se pueden apilar y no se pueden procesar de manera oportuna.

Causas posibles

La capacidad de cálculo del clúster es inferior a la tasa de envío de tareas. Como resultado, la tarea no puede procesarse de manera oportuna después de haber sido enviada.

Procedimiento

Paso 1 Compruebe el uso de la memoria y los vCores en la página Yarn.

Compruebe si los valores de **Memory Used|Memory Total** y **VCores Used|VCores Total** en la página nativa de Yarn alcanzan o se acercan a los valores máximos.

- En caso afirmativo, vaya a **Paso 2**.
- Si no, vaya a **Paso 5**.

Paso 2 Compruebe el número de tareas enviadas.

Compruebe si las tareas en ejecución se envían con una frecuencia normal.

- En caso afirmativo, vaya a **Paso 3**.
- Si no, vaya a **Paso 5**.

Paso 3 Escale horizontal el clúster.

El escalamiento horizontal se basa en los requisitos del sitio. Para obtener más información, consulte **Escalamiento manual de un clúster.**

Paso 4 Una vez completado el escalamiento horizontal, compruebe si la alarma está desactivada.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 5**.

Paso 5 Recopilar información de fallas.

1. En MRS Manager, seleccione **System** > **Export Log**.

2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Referencia

Ninguna

8.5.71 ALM-18012 El número de tareas de Yarn terminadas en el último período supera el umbral (Para MRS 2.*x* o anterior)

Descripción

El sistema comprueba el número de tareas de Yarn terminadas cada 10 minutos. Esta alarma se genera cuando el número de tareas de Yarn terminadas en los últimos 10 minutos es mayor que el umbral. Esta alarma se borra automáticamente cuando el número de tareas de Yarn terminadas es menor que el umbral en los próximos 10 minutos.

Atributo

ID de alarma	Gravedad de alarma	Borrar automáticamente
18012	Grave	Sí

Parámetro

Parámetro	Descripción
ServiceName	Servicio para el que se genera la alarma.
RoleName	Rol para el que se genera la alarma.
HostName	Host para el que se genera la alarma.

Impacto en el sistema

Ninguna

Causas posibles

Un usuario detiene manualmente una tarea de Yarn en ejecución.

Procedimiento

Compruebe el operador de terminación de tareas en los registros de Yarn y los registros de auditoría, y determine la causa de la terminación de la tarea.

Referencia

Ninguna

8.5.72 ALM-18013 El número de tareas de Yarn fallidas en el último período supera el umbral (Para MRS 2.*x* o anterior)

Descripción

El sistema comprueba el número de tareas de Yarn fallidas cada 10 minutos. Esta alarma se genera cuando el número de tareas de Yarn fallidas en los últimos 10 minutos es mayor que el umbral. Esta alarma se borra automáticamente cuando el número de tareas de Yarn fallidas es menor que el umbral en los próximos 10 minutos.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
18013	Grave	Sí

Parámetro

Parámetro	Descripción
ServiceName	Servicio para el que se genera la alarma.
RoleName	Rol para el que se genera la alarma.
HostName	Host para el que se genera la alarma.

Impacto en el sistema

Ninguna

Causas posibles

El programa de trabajo de Yarn enviado es incorrecto. Por ejemplo, el parámetro para que Spark envíe un trabajo es incorrecto.

Procedimiento

Compruebe el registro del trabajo fallido, busque la causa de la falla, modifique el trabajo y vuelva a enviarlo.

Referencia

Ninguna

8.5.73 ALM-19000 Servicio HBase no disponible (para MRS 2.*x* o anterior)

Descripción

El módulo de alarma comprueba el estado del servicio de HBase cada 30 segundos. Esta alarma se genera cuando el servicio HBase no está disponible.

Esta alarma se borra cuando se recupera el servicio HBase.

Atributo

ID de alarma	Gravedad de alarma	Borrar automáticamente
19000	Crítica	Sí

Parámetros

Parámetro	Descripción
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

No se pueden realizar operaciones, como leer o escribir datos y crear tablas.

Causas posibles

- ZooKeeper es anormal.
- HDFS es anormal.
- HBase es anormal.
- Estado anormal de la red.

Procedimiento

Paso 1 Compruebe el estado del ZooKeeper.

1. Vaya a la página de detalles del clúster MRS y haga clic en **Components**.
2. En la lista de servicios, compruebe si el estado de salud de ZooKeeper es de tipo **Good**.
   - En caso afirmativo, vaya a **Paso 2.1**.
   - Si no, vaya a **Paso 1.3**.

3. En la lista de alarmas, compruebe si existe la alarma ALM-13000 El servicio ZooKeeper no disponible.
   - En caso afirmativo, vaya a **Paso 1.4**.
   - Si no, vaya a **Paso 2.1**.
4. Rectifique la falla siguiendo los pasos proporcionados en ALM-13000 El servicio ZooKeeper no disponible.
5. Espere varios minutos y compruebe si la alarma está desactivada.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 2.1**.

Paso 2 Compruebe el estado de HDFS.

1. En MRS Manager, compruebe si se notifica la alarma ALM-14000 El servicio HDFS no disponible.
   - En caso afirmativo, vaya a **Paso 2.2**.
   - Si no, vaya a **Paso 3**.
2. Rectifique la falla siguiendo los pasos proporcionados en ALM-14000 El servicio HDFS no disponible.
3. Espere varios minutos y compruebe si la alarma está desactivada.

Paso 3 Recopilar información de fallas.

1. En MRS Manager, seleccione **System** > **Export Log**.
2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Referencia

Ninguna

8.5.74 ALM-19006 Error de sincronización de replicación de HBase (Para MRS 2.*x* o anterior)

Descripción

Esta alarma se genera cuando los datos de recuperación ante desastres (DR) no se sincronizan con un clúster en espera.

Esta alarma se borra cuando la sincronización de datos de DR se realiza correctamente.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
19006	Grave	Sí

Parámetros

Parámetro	Descripción
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

Los datos de HBase en un clúster no se sincronizan con el clúster en espera, lo que provoca incoherencia de datos entre los clústeres activos y en espera.

Causas posibles

- El servicio HBase en el clúster en espera es anormal.
- Estado anormal de la red.

Procedimiento

Paso 1 Observe si el sistema borra automáticamente la alarma.

1. Vaya a la página de detalles del clúster y elija **Alarms**.
2. En la lista de alarmas, haga clic en la alarma para obtener el tiempo de generación de alarma a partir de **Generated Time** en **Alarm Details**. Compruebe si la alarma ha existido durante más de 5 minutos.
   - En caso afirmativo, vaya a **Paso 2.1**.
   - Si no, vaya a **Paso 1.3**.
3. Espere 5 minutos y compruebe si la alarma se borra automáticamente.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 2.1**.

Paso 2 Compruebe el estado del servicio HBase del clúster en espera.

1. Vaya a la página de detalles del clúster y elija **Alarms**.
2. En la lista de alarmas, haga clic en la alarma y obtenga **HostName** de **Location** en **Alarm Details**.
3. Inicie sesión en el nodo donde se encuentra el cliente HBase del clúster activo. Ejecute los siguientes comandos para cambiar el usuario:

   sudo su - root

   su - omm
4. Ejecute el comando **status 'replication', 'source'** para comprobar el estado de sincronización del nodo defectuoso.

   El estado de sincronización de un nodo es el siguiente.


```
10-10-10-153:
 SOURCE: PeerID=abc, SizeOfLogQueue=0, ShippedBatches=2, ShippedOps=2,
ShippedBytes=320, LogReadInBytes=1636, LogEditsRead=5, LogEditsFiltered=3,
SizeOfLogToReplicate=0, TimeForLogToReplicate=0, ShippedHFiles=0,
SizeOfHFileRefsQueue=0, AgeOfLastShippedOp=0, TimeStampsOfLastShippedOp=Mon
Jul 18 09:53:28 CST 2016, Replication Lag=0, FailedReplicationAttempts=0
 SOURCE: PeerID=abc1, SizeOfLogQueue=0, ShippedBatches=1, ShippedOps=1,
ShippedBytes=160, LogReadInBytes=1636, LogEditsRead=5, LogEditsFiltered=3,
SizeOfLogToReplicate=0, TimeForLogToReplicate=0, ShippedHFiles=0,
SizeOfHFileRefsQueue=0, AgeOfLastShippedOp=16788,
TimeStampsOfLastShippedOp=Sat Jul 16 13:19:00 CST 2016, Replication
Lag=16788, FailedReplicationAttempts=5
```

5. Obtenga **PeerID** correspondiente a un registro cuyo valor **FailedReplicationAttempts** es mayor que 0.

   En la etapa anterior, los datos en el nodo defectuoso **10-10-10-153** no pueden sincronizarse con un clúster en espera cuyo **PeerID** es de **abc1**.

6. Ejecute el comando **list_peers** para encontrar el clúster y la instancia de HBase correspondiente a **PeerID**.

   ```
   PEER_ID CLUSTER_KEY STATE TABLE_CFS
    abc1 10.10.10.110,10.10.10.119,10.10.10.133:24002:/hbase2 ENABLED
    abc 10.10.10.110,10.10.10.119,10.10.10.133:24002:/hbase ENABLED
   ```

   En la información anterior, **/hbase2** indica que los datos están sincronizados con la instancia HBase2 del clúster en espera.

7. En la lista de servicios del clúster en espera, compruebe si el estado de salud de la instancia HBase obtenida en **Paso 2.6** es **Good**.
   - En caso afirmativo, vaya a **Paso 3.1**.
   - Si no, vaya a **Paso 2.8**.
8. En la lista de alarmas, compruebe si existe la alarma ALM-19000 Servicio HBase no disponible.
   - En caso afirmativo, vaya a **Paso 2.9**.
   - Si no, vaya a **Paso 3.1**.
9. Rectifique la falla siguiendo los pasos proporcionados en ALM-19000 Servicio HBase no disponible.
10. Espere varios minutos y compruebe si la alarma está desactivada.
    - En caso afirmativo, no es necesario hacer nada más.
    - Si no, vaya a **Paso 3.1**.

Paso 3 Compruebe la conexión de red entre RegionServers en clústeres activos y en espera.

1. Vaya a la página de detalles del clúster y elija **Alarms**.
2. En la lista de alarmas, haga clic en la alarma y obtenga **HostName** de **Location** en **Alarm Details**.
3. Inicie sesión en el nodo RegionServer defectuoso.
4. Ejecute el comando **ping** para comprobar si la conexión de red entre el nodo RegionServer defectuoso y el host donde reside el RegionServer del clúster en espera es normal.
   - En caso afirmativo, vaya a **Paso 4**.
   - Si no, vaya a **Paso 3.5**.
5. Póngase en contacto con el personal de O&M para restaurar la red.
6. Después de que la red se recupere, compruebe si la alarma está borrada.

– En caso afirmativo, no es necesario hacer nada más.
– Si no, vaya a **Paso 4**.

Paso 4 Recopilar información de fallas.

1. En MRS Manager, seleccione **System** > **Export Log**.
2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Referencia

Ninguna

8.5.75 ALM-19007 HBase Merge Queue Exceeds the Threshold (for 2.x and Earlier Versions)

Description

The system checks the HBase compaction queue size every 30 seconds. This alarm is generated when the compaction queue size exceeds the alarm threshold (**100** by default) for three consecutive times. This alarm is cleared when the compaction queue size is less than the threshold.

Attribute

Alarm ID	Alarm Severity	Auto Clear
19007	Minor	Yes

Parameters

Name	Meaning
ServiceName	Specifies the service for which the alarm is generated.
RoleName	Specifies the role for which the alarm is generated.
Host Name	Specifies the host for which the alarm is generated.

Impact on the System

The cluster performance may deteriorate, affecting data read and write.

Possible Causes

- The number of HBase RegionServers is too small.
- There are too many regions on a RegionServer of HBase.
- The HBase RegionServer heap size is small.
- Resources are insufficient.
- Related parameters are not configured properly.

Procedure

Paso 1 Check whether related HBase parameters are properly configured.

1. Log in to the MRS cluster details page, choose **Components** > **HBase** > **Service Configuration**, switch **Basic Configuration** to **All Configurations**, and search for **hbase.hstore.compaction.min** and **hbase.hstore.compaction.max**, and increase the values of **hbase.regionserver.thread.compaction.small** and **hbase.regionserver.thread.compaction.throttle**.

   NOTA

   If you did not synchronize IAM users, perform synchronization first. (In the **Dashboard** tab, click **Synchronize** next to **IAM User Sync**.)
2. Save the configuration, and restart the HBase service during off-peak hours or perform a rolling restart to make the configuration take effect.
3. Check whether the alarm is cleared.
   - If yes, no further action is required.
   - If no, go to **Paso 2**.

Paso 2 Collect fault information.

1. On MRS Manager, choose **System** > **Export Log**.
2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Alarm Clearing

This alarm is automatically cleared after the fault is rectified.

Related Information

None

8.5.76 ALM-20002 Servicio Hue no disponible (para MRS 2.*x* o anterior)

Descripción

El sistema comprueba el estado del servicio Hue cada 60 segundos. Esta alarma se genera si el servicio Hue no está disponible.

Esta alarma se borra cuando el servicio Hue es normal.

Atributo

ID de alarma	Severidad de alarma	Borrado automáticamente
20002	Crítica	Sí

Parámetros

Parámetro	Descripción
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

El sistema no puede proporcionar servicios de carga, consulta y extracción de datos.

Causas posibles

- El servicio KrbServer del que depende Hue es anormal.
- El servicio DBService del que depende Hue es anormal.
- La conexión de red a DBService es anormal.

Procedimiento

Comprobar si el servicio KrbServer es normal.

Paso 1 Vaya a la página de detalles del clúster MRS y haga clic en **Components**.

Paso 2 En la lista de servicios, compruebe si el **Health Status** de **KrbServer** es **Good**.

- En caso afirmativo, vaya a **Paso 5**.
- Si no, vaya a **Paso 3**.

Paso 3 Haga clic en **Restart** en la columna **Operation** del servicio KrbServer para reiniciar el servicio.

Paso 4 Espere unos minutos. Compruebe si ALM-20002 Servicio Hue no disponible está borrado.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 5**.

Comprobar si DBService es normal.

Paso 5 Vaya a la página de detalles del clúster MRS y haga clic en **Components**.

Paso 6 En la lista de servicios, compruebe si **Health Status** de **DBService** es **Good**.

- En caso afirmativo, vaya a **Paso 9**.
- Si no, vaya a **Paso 7**.

Paso 7 Haga clic en **Restart** en la columna **Operation** del servicio DBService para reiniciar el servicio.

NOTA

Para reiniciar el servicio, debe ingresar la contraseña del administrador de MRS Manager y seleccionar **Start or restart related services**.

Paso 8 Espere unos minutos. Compruebe si ALM-20002 Servicio Hue no disponible está borrado.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 9**.

Comprobar si la red conectada a DBService es normal.

Paso 9 Elija **Components** > **Hue** > **Instance** y registre la dirección IP del nodo de Hue activo.

Paso 10 Use PuTTY para iniciar sesión en el Hue activo.

Paso 11 Ejecute el comando **ping** para comprobar si la conexión de red entre el host donde se encuentra el Hue activo y el host donde se encuentra DBService es normal. (El método para obtener la dirección IP del servicio DBService es el mismo que el de obtener la dirección IP de Hue activa.)

- En caso afirmativo, vaya a **Paso 17**.
- Si no, vaya a **Paso 12**.

Paso 12 Póngase en contacto con el administrador de red para reparar la red.

Paso 13 Espere unos minutos. Compruebe si ALM-20002 Servicio Hue no disponible está borrado.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 17**.

Recopilar información de fallas.

Paso 14 En MRS Manager, seleccione **System** > **Export Log**.

Paso 15 Seleccione los siguientes nodos de la lista desplegable **Services** y haga clic en **OK**.

- Hue
- Controller

Paso 16 Configure **Start Time** y **End Time** para la recopilación de registros en 10 minutos antes y después de que se genere la alarma, seleccione un tipo de exportación y haga clic en **OK** para recopilar la información de registro de fallas correspondiente.

Reiniciar Hue.

Paso 17 Elija **Components** > **Hue**.

Paso 18 Elija **More** > **Restart Service** y haga clic en **OK**.

Paso 19 Verifique si la alarma se ha borrado.

- En caso afirmativo, no es necesario hacer nada más.

- Si no, vaya a **Paso 20**.

Paso 20 Recopile información de fallas.

1. En MRS Manager, elija **System** > **Export Log**.
2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Referencia

Ninguna

8.5.77 ALM-23001 Servicio Loader no disponible (Para MRS 2.*x* o anterior)

Descripción

El sistema comprueba la disponibilidad del servicio del Loader cada 60 segundos. Esta alarma se genera si el servicio Loader no está disponible y se borra después de que se recupere el servicio Loader.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
23001	Crítica	Sí

Parámetros

Parámetro	Descripción
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

La carga, la importación y la conversión de datos no están disponibles.

Causas posibles

- Los servicios de los que depende Loader son anormales.
  - ZooKeeper es anormal.

  - HDFS es anormal.
  - DBService es anormal.
  - Yarn es anormal.
  - MapReduce es anormal.
- La red está defectuosa. Loader no puede comunicarse con sus servicios dependientes.
- Loader está funcionando incorrectamente.

Procedimiento

Paso 1 Compruebe el estado del ZooKeeper.

1. Vaya a la página de detalles del clúster MRS y haga clic en **Components**.
2. Elija **ZooKeeper** y compruebe si el estado de salud de ZooKeeper es normal.
   - En caso afirmativo, vaya a **Paso 1.4**.
   - Si no, vaya a **Paso 1.3**.
3. Haga clic en **More > Restart Service** para reiniciar ZooKeeper. Después de iniciar el ZooKeeper, compruebe si la alarma "ALM-23001 Servicio Loader no disponible" está desactivada.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 1.4**.
4. En MRS Manager, compruebe si se notifica la alarma ALM-12007 Falla de proceso.
   - En caso afirmativo, vaya a **Paso 1.5**.
   - Si no, vaya a **Paso 2.1**.
5. En **Alarm Details** de la alarma "ALM-12007 Fallo de proceso", compruebe si **ServiceName** es **ZooKeeper**.
   - En caso afirmativo, vaya a **Paso 1.6**.
   - Si no, vaya a **Paso 2.1**.
6. Desactive la alarma de acuerdo con las sugerencias de manejo de "ALM-12007 Falla de proceso".
7. Compruebe si la alarma "ALM-23001 Servicio Loader no disponible" está desactivada.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 2.1**.

Paso 2 Compruebe el estado de HDFS.

1. Vaya a la página de detalles del clúster de MRS y elija **Alarms**.
2. En MRS Manager, compruebe si se notifica la "ALM-14000 Alarma de servicio HDFS no disponible".
   - En caso afirmativo, vaya a **Paso 2.3**.
   - Si no, vaya a **Paso 3.1**.
3. Borre la alarma de acuerdo con las sugerencias de manejo de "ALM-14000 Servicio HDFS no disponible".
4. Compruebe si la alarma "ALM-23001 Servicio Loader no disponible" está desactivada.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 3.1**.

Paso 3 Compruebe el estado de DBService.

1. Vaya a la página de detalles del clúster MRS y haga clic en **Components**.
2. Elija **DBService** para comprobar si el estado de mantenimiento de DBService es normal.
   - En caso afirmativo, vaya a **Paso 4.1**.
   - Si no, vaya a **Paso 3.3**.
3. Elija **More > Restart Service** para reiniciar DBService. Después de iniciar DBService, compruebe si la alarma "ALM-23001 Servicio Loader no disponible" está desactivada.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 4.1**.

Paso 4 Compruebe el estado del MapReduce.

1. Vaya a la página de detalles del clúster MRS y haga clic en **Components**.
2. Elija **MapReduce** y compruebe si el estado de salud de MapReduce es normal.
   - En caso afirmativo, vaya a **Paso 5.1**.
   - Si no, vaya a **Paso 4.3**.
3. Haga clic en **More > Restart Service** para reiniciar MapReduce. Después de iniciar el MapReduce, compruebe si la alarma "ALM-23001 Servicio Loader no disponible" está desactivada.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 5.1**.

Paso 5 Compruebe el estado de Yarn.

1. Vaya a la página de detalles del clúster MRS y haga clic en **Components**.
2. Elija **Yarn** y compruebe si el estado de salud de Yarn es normal.
   - En caso afirmativo, vaya a **Paso 5.4**.
   - Si no, vaya a **Paso 5.3**.
3. Elija **More > Restart Service** para reiniciar Yarn. Después de iniciar Yarn, compruebe si la alarma "ALM-23001 Servicio Loader no disponible" está desactivada.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 5.4**.
4. En MRS Manager, compruebe si se notifica la alarma "ALM-18000 Servicio Yarn no disponible".
   - En caso afirmativo, vaya a **Paso 5.5**.
   - Si no, vaya a **Paso 6.1**.
5. Borre la alarma de acuerdo con las sugerencias de manejo de "ALM-18000 Servicio Yarn no disponible".
6. Compruebe si la alarma "ALM-23001 Servicio Loader no disponible" está desactivada.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 6.1**.

Paso 6 Compruebe las conexiones de red entre Loader y sus componentes dependientes.

1. Vaya a la página de detalles del clúster MRS y haga clic en **Components**.
2. Haga clic en **Loader**.

3. Haga clic en **Instance**. Se muestra la lista de instancias de Sqoop.
4. Registre las direcciones IP de gestión de todas las instancias de Sqoop.
5. Inicie sesión en los hosts utilizando las direcciones IP obtenidas en **Paso 6.4**. Ejecute los siguientes comandos para cambiar el usuario:

   sudo su - root

   su - omm
6. Ejecute el comando **ping** para comprobar si la conexión de red entre los hosts donde residen las instancias Sqoop y los componentes dependientes es normal. (Los componentes dependientes incluyen ZooKeeper, DBService, HDFS, MapReduce e Yarn. El método para obtener las direcciones IP de los componentes dependientes es el mismo que el utilizado para obtener las direcciones IP de las instancias Sqoop.)
   - En caso afirmativo, vaya a **Paso 7**.
   - Si no, vaya a **Paso 6.7**.
7. Póngase en contacto con el administrador de red para reparar la red.
8. Compruebe si la alarma "ALM-23001 Servicio Loader no disponible" está desactivada.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 7**.

Paso 7 Recopilar información de fallas.

1. En MRS Manager, seleccione **System** > **Export Log**.
2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

8.5.78 ALM-24000 Servicio de Flume no disponible (Para MRS 2.*x* o anterior)

Descripción

El módulo de alarma comprueba el estado de servicio de Flume cada 180 segundos. Esta alarma se genera si el servicio Flume es anormal.

Esta alarma se borra después de que se recupere el servicio Flume.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
24000	Crítica	Sí

Parámetros

Parámetro	Descripción
ServiceName	Especifica el servicio para el que se genera la alarma.

Parámetro	Descripción
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impact on the System

Flume no puede funcionar y la transmisión de datos se interrumpe.

Causas posibles

- HDFS no está disponible.
- LdapServer no está disponible.

Procedimiento

Paso 1 Compruebe el estado de HDFS.

1. Vaya a la página de detalles del clúster de MRS y elija **Alarms**.
2. Compruebe si se genera la alarma ALM-14000 Servicio HDFS no disponible.
   - En caso afirmativo, borre la alarma de acuerdo con las sugerencias de manejo de "ALM-14000 Servicio HDFS no disponible".
   - Si no, vaya a **Paso 2**.

Paso 2 Compruebe el estado del LdapServer.

Compruebe si se genera la alarma ALM-25000 Servicio LdapServer no disponible.

- En caso afirmativo, borre la alarma de acuerdo con las sugerencias de manejo de "ALM-25000 Servicio LdapServer no disponible".
- Si no, vaya a **Paso 3.2**.

Paso 3 Compruebe si los servicios HDFS y LdapServer están detenidos.

1. Vaya a la página de detalles del clúster MRS y haga clic en **Components**.
2. En la lista de servicios en MRS Manager, compruebe si los servicios HDFS y LdapServer están detenidos.
   - En caso afirmativo, inicie los servicios HDFS y LdapServer y vaya a **Paso 3.3**.
   - Si no, vaya a **Paso 4**.
3. Compruebe si la alarma "ALM-24000 Servicio Flume no disponible" está desactivada.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 4**.

Paso 4 Recopilar información de fallas.

1. En MRS Manager, seleccione **System** > **Export Log**.
2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Información relacionada

N/A

8.5.79 ALM-24001 El agente de Flume es anormal (Para MRS 2.*x* o anterior)

Descripción

Esta alarma se genera si el módulo de monitorización del agente de Flume detecta que el proceso del agente de Flume es anormal.

Esta alarma se borra después de que se recupera el proceso del agente de Flume.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
24001	Menor	Sí

Parámetros

Parámetro	Descripción
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

Las funciones de la instancia de agente de Flume alarmada son anormales. Las tareas de transmisión de datos de la instancia se suspenden. En la transmisión de datos en tiempo real, los datos se perderán.

Causas posibles

- El directorio **JAVA_HOME** no existe o el permiso Java es incorrecto.
- El permiso del directorio del agente de Flume es incorrecto.

Procedimiento

Paso 1 Compruebe el archivo de configuración del agente de Flume.

1. Inicie sesión en el host donde reside el nodo defectuoso. Ejecute el siguiente comando para cambiar a usuario **root**:

sudo su - root

2. Ejecute el comando **cd** *Flume installation directory*/**fusioninsight-flume-1.6.0/conf/** para ir al directorio de configuración de Flume.
3. Ejecute el comando **cat ENV_VARS**. Compruebe si el directorio **JAVA_HOME** existe y si el usuario del agente de Flume tiene permiso de ejecución de Java.
   - En caso afirmativo, vaya a **Paso 2.1**.
   - Si no, vaya a **Paso 1.4**.
4. Especifique el directorio JAVA_HOME correcto y conceda al usuario del agente de Flume el permiso de ejecución de Java. Entonces vaya a **Paso 2.4**.

Paso 2 Compruebe el permiso del directorio del agente de Flume.

1. Inicie sesión en el host donde reside el nodo defectuoso. Ejecute el siguiente comando para cambiar a usuario **root**:

   sudo su - root
2. Ejecute el siguiente comando para acceder al directorio de instalación del agente de Flume:

   cd *Flume agent installation directory*
3. Ejecute el comando **ls -al * -R**. Compruebe si el propietario de todos los archivos es el usuario del agente de Flume.
   - En caso afirmativo, vaya a **Paso 3**.
   - Si no, ejecute el comando **chown** y cambie el propietario de los archivos al usuario del agente de Flume. Entonces vaya a **Paso 2.4**.
4. Verifique si la alarma se ha borrado.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 3**.

Paso 3 Recopilar información de fallas.

1. En MRS Manager, seleccione **System** > **Export Log**.
2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Información relacionada

N/A

8.5.80 ALM-24003 Conexión de Flume Client interrumpida (Para MRS 2.*x* o anterior)

Descripción

El módulo de alarma monitorea el estado de la conexión del puerto en el Flume server. Esta alarma se genera si el Flume server no recibe un mensaje de conexión del Flume client en 3 minutos consecutivos.

Esta alarma se borra después de que el Flume server recibe un mensaje de conexión del Flume client.

Atributo

ID de alarma	Gravedad de alarma	Borrar automáticamente
24003	Grave	Sí

Parámetros

Parámetro	Descripción
ClientIP	Especifica la dirección IP del cliente de Flume.
ServerIP	Especifica la dirección IP del servidor de Flume.
ServerPort	Especifica el puerto del servidor de Flume.

Impacto en el sistema

La comunicación entre Flume client y server falla. El Flume client no puede enviar datos al Flume server.

Causas posibles

- La red entre el Flume client y server es defectuosa.
- El proceso del Flume client es anormal.
- El Flume client está configurado incorrectamente.

Procedimiento

Paso 1 Compruebe la red entre el Flume client y server.

1. Inicie sesión en el host donde reside Flume client alarmado. Ejecute el siguiente comando para cambiar a usuario **root**:

   sudo su - root

2. Ejecute el comando **ping** *Flume server IP address* para comprobar si la red entre Flume client y server es normal.
   - En caso afirmativo, vaya a **Paso 2.1**.
   - Si no, vaya a **Paso 4**.

Paso 2 Compruebe si el proceso de Flume client es normal.

1. Inicie sesión en el host donde reside Flume client alarmado. Ejecute el siguiente comando para cambiar a usuario **root**:

   sudo su - root

2. Ejecute el comando **ps -ef|grep flume |grep client** para comprobar si existe el proceso Flume client.
   - En caso afirmativo, vaya a **Paso 3.1**.

– Si no, vaya a **Paso 4**.

Paso 3 Compruebe la configuración del Flume client.

1. Inicie sesión en el host donde reside Flume client alarmado. Ejecute el siguiente comando para cambiar a usuario **root**:

   sudo su - root

2. Ejecute el comando **cd** *Flume installation directory*/**fusioninsight-flume-1.6.0/conf/** para ir al directorio de configuración de Flume.
3. Ejecute el comando **cat properties.properties** para consultar el archivo de configuración actual del Flume client.
4. Compruebe si el archivo **properties.properties** está configurado correctamente de acuerdo con la descripción de configuración del Flume agent.
   – En caso afirmativo, vaya a **Paso 3.5**.
   – Si no, vaya a **Paso 4**.
5. Modifique el archivo de configuración **properties.properties**.
6. Verifique si la alarma se ha borrado.
   – En caso afirmativo, no es necesario hacer nada más.
   – Si no, vaya a **Paso 4**.

Paso 4 Recopilar información de fallas.

1. En MRS Manager, seleccione **System** > **Export Log**.
2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Información relacionada

N/A

8.5.81 ALM-24004 Flume no puede leer datos (para MRS 2.*x* o anterior)

Descripción

El módulo de alarma monitorea el estado de Flume source. Esta alarma se genera si la duración en la que Flume Source no puede leer los datos excede el umbral.

Los usuarios pueden modificar el umbral según sea necesario.

Esta alarma se borra si Source lee los datos correctamente.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
24004	Grave	Sí

Parámetros

Parámetro	Descripción
ServiceName	Especifica el servicio para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
ComponentType	Especifica el tipo de componente para el que se genera la alarma.
ComponentName	Especifica el nombre del componente para el que se genera la alarma.

Impacto en el sistema

Se detiene la recopilación de datos.

Causas posibles

- Flume source está defectuosa.
- La red está defectuosa.

Procedimiento

Paso 1 Compruebe si Flume Source es normal.

1. Compruebe si Flume Source es el tipo spoolDir.
   - En caso afirmativo, vaya a **Paso 1.2**.
   - Si no, vaya a **Paso 1.3**.
2. Consulte el directorio **spoolDir** y compruebe si se han enviado todos los archivos.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 1.5**.
3. Compruebe si la fuente de Flume es el tipo Kafka.
   - En caso afirmativo, vaya a **Paso 1.4**.
   - Si no, vaya a **Paso 1.5**.
4. Inicie sesión en el cliente de Kafka y ejecute los siguientes comandos para comprobar si se han consumido todos los datos del topic configurados para Kafka Source.

   cd /opt/client/Kafka/kafka/bin

   ./kafka-consumer-groups.sh --bootstrap-server *Kafka cluster IP address*:**21007 --new-consumer --describe --group example-group1 --command-config**

   ../config/consumer.properties
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 1.5**.
5. Vaya a la página de detalles del clúster y haga clic en **Components**.

6. Elija **Flume** > **Instances**.
7. Haga clic en la instancia Flume del nodo defectuoso y compruebe si el valor del **Source Speed Metrics** es 0.
   - En caso afirmativo, vaya a **Paso 2.1**.
   - En caso negativo, no se requiere ninguna otra acción.

Paso 2 Compruebe el estado de la red entre la fuente de Flume y el nodo defectuoso.

1. Compruebe si la fuente de Flume es el tipo avro.
   - En caso afirmativo, vaya a **Paso 2.3**.
   - Si no, vaya a **Paso 3**.
2. Inicie sesión en el host donde reside el nodo defectuoso. Ejecute el siguiente comando para cambiar a usuario **root**:

   sudo su - root
3. Ejecute el comando **ping** *Flume source IP address* para comprobar si se puede hacer un ping al Flume Source.
   - En caso afirmativo, vaya a **Paso 3**.
   - Si no, vaya a **Paso 2.4**.
4. Póngase en contacto con el administrador de red para reparar la red.
5. Espere un rato y compruebe si la alarma está desactivada.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 3**.

Paso 3 Recopile información de fallas.

1. En MRS Manager, seleccione **System** > **Export Log**.
2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Información relacionada

N/A

8.5.82 ALM-24005 La transmisión de datos por Flume es anormal (Para MRS 2.*x* o anterior)

Descripción

El módulo de alarma monitoriza la capacidad de los canales de Flume. Esta alarma se genera si la duración en la que un canal está lleno o el número de veces que una fuente no envía datos al canal excede el umbral.

Los usuarios pueden establecer el umbral según sea necesario modificando el parámetro **channelfullcount**.

Esta alarma se borra después de que se suelte el espacio del canal Flume.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
24005	Grave	Sí

Parámetros

Parámetro	Descripción
ServiceName	Especifica el servicio para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
ComponentType	Especifica el tipo de componente para el que se genera la alarma.
ComponentName	Especifica el nombre del componente para el que se genera la alarma.

Impacto en el sistema

Si el uso del Flume Channel continúa creciendo, el tiempo de transmisión de datos aumenta. Cuando el uso alcanza el 100%, se suspende el proceso del agente de Flume.

Causas posibles

- El Flume sink está defectuoso.
- La red está defectuosa.

Procedimiento

Paso 1 Compruebe si el Flume sink es normal.

1. Compruebe si el Flume sink es el tipo de HDFS.
   - En caso afirmativo, vaya a **Paso 1.2**.
   - Si no, vaya a **Paso 1.3**.
2. En MRS Manager, compruebe si se informa de la alarma ALM-14000 Servicio HDFS no disponible y si se detiene el servicio HDFS.
   - Si se informa de la alarma, bórrela de acuerdo con las sugerencias de manejo de ALM-14000 Servicio HDFS no disponible; si el servicio HDFS está detenido, inícielo. Entonces vaya a **Paso 1.7**.
   - Si no, vaya a **Paso 1.7**.
3. Compruebe si el Flume sink es el tipo de HBase.
   - En caso afirmativo, vaya a **Paso 1.4**.
   - Si no, vaya a **Paso 1.7**.

4. En MRS Manager, compruebe si se informa de la alarma ALM-19000 Servicio HBase no disponible y si se detiene el servicio HBase.
   - Si se informa de la alarma, bórrela de acuerdo con las sugerencias de manejo de "ALM-19000 Servicio HBase no disponible"; si el servicio HBase está detenido, inícielo. Entonces vaya a **Paso 1.7**.
   - Si no, vaya a **Paso 1.7**.
5. Compruebe si el Flume sink es del tipo de Kafka.
   - En caso afirmativo, vaya a **Paso 1.6**.
   - Si no, vaya a **Paso 1.7**.
6. En MRS Manager, compruebe si se informa de la alarma ALM-38000 Servicio Kafka no disponible y si se detiene el servicio Kafka.
   - Si se informa de la alarma, bórrela de acuerdo con las sugerencias de manejo de "ALM-38000 Servicio Kafka no disponible"; si el servicio Kafka está detenido, inícielo. Entonces vaya a **Paso 1.7**.
   - Si no, vaya a **Paso 1.7**.
7. Vaya a la página de detalles del clúster MRS y haga clic en **Components**.
8. Elija **Flume** > **Instances**.
9. Haga clic en la instancia Flume del nodo defectuoso y compruebe si el valor del **Sink Speed Metrics** es 0.
   - En caso afirmativo, vaya a **Paso 2.1**.
   - En caso negativo, no se requiere ninguna otra acción.

Paso 2 Compruebe el estado de la red entre el Flume sink y el nodo defectuoso.

1. Compruebe si el Flume sink es del tipo de Avro.
   - En caso afirmativo, vaya a **Paso 2.3**.
   - Si no, vaya a **Paso 3**.
2. Inicie sesión en el host donde reside el nodo defectuoso. Ejecute el siguiente comando para cambiar a usuario **root**:

   sudo su - root
3. Ejecute el comando **ping** *Flume sink IP address* para comprobar si se puede hacer un ping al Flume sink.
   - En caso afirmativo, vaya a **Paso 3**.
   - Si no, vaya a **Paso 2.4**.
4. Póngase en contacto con el administrador de red para reparar la red.
5. Espere un rato y compruebe si la alarma está desactivada.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 3**.

Paso 3 Recopilar información de fallas.

1. En MRS Manager, seleccione **System** > **Export Log**.
2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Información relacionada

N/A

8.5.83 ALM-25000 El servicio LdapServer no está disponible (Para MRS 2.*x* o anterior)

Descripción

El sistema comprueba el estado del servicio LdapServer cada 30 segundos. Esta alarma se genera cuando los servicios de LdapServer activo y en espera son anormales.

Esta alarma se borra cuando se restaura cualquiera de los servicios LdapServer.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
25000	Crítica	Sí

Parámetros

Parámetro	Descripción
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

Cuando se genera esta alarma, no se puede realizar ninguna operación para los usuarios KrbServer y LdapServer en el clúster. Por ejemplo, los usuarios, grupos de usuarios o roles no se pueden agregar, eliminar o modificar, y las contraseñas de usuario no se pueden cambiar en MRS Manager. La autenticación de los usuarios existentes en el clúster no se ve afectada.

Causas posibles

- El nodo donde se encuentra el servicio LdapServer es defectuoso.
- El proceso LdapServer es anormal.

Procedimiento

Paso 1 Compruebe si los nodos donde se encuentran las dos instancias de SlapdServer del servicio LdapServer son defectuosos.

1. Vaya a la página de detalles del clúster MRS y haga clic en **Components**.
2. Elija **LdapServer** > **Instances**. Vaya a la página de instancia LdapServer para obtener el nombre de host del nodo donde residen las dos instancias de SlapdServer.
3. En la página **Alarms** del MRS Manager, compruebe si se genera la alarma ALM-12006 Falla de nodo.
   - En caso afirmativo, vaya a **Paso 1.4**.
   - Si no, vaya a **Paso 2.1**.
4. Compruebe si el nombre de host en la información de alarma es el mismo que el nombre de host real en **Paso 1.2**.
   - En caso afirmativo, vaya a **Paso 1.5**.
   - Si no, vaya a **Paso 2.1**.
5. Rectifique la falla siguiendo los pasos proporcionados en ALM-12006 Falla de nodo.
6. En la lista de alarmas, compruebe si la alarma ALM-25000 Servicio LdapServer no disponible está borrado.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 3**.

Paso 2 Compruebe si el proceso LdapServer está en estado normal.

1. Vaya a la página de detalles del clúster y elija **Alarms**.
2. Compruebe si se genera ALM-12007 Falla de proceso.
   - En caso afirmativo, vaya a **Paso 2.3**.
   - Si no, vaya a **Paso 3**.
3. Compruebe si el nombre de servicio y el nombre de host en la alarma son consistentes con el servicio LdapServer y los nombres del host.
   - En caso afirmativo, vaya a **Paso 2.4**.
   - Si no, vaya a **Paso 3**.
4. Rectifique la falla siguiendo los pasos proporcionados en ALM-12007 Falla de proceso.
5. En la lista de alarmas, compruebe si la alarma ALM-25000 Servicio LdapServer no disponible está borrado.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 3**.

Paso 3 Recopilar información de fallas.

1. En MRS Manager, seleccione **System** > **Export Log**.
2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Referencia

Ninguna

8.5.84 ALM-25004 Sincronización anormal de datos de LdapServer (Para MRS 2.*x* o anterior)

Descripción

Esta alarma se genera cuando los datos de LdapServer en Manager son inconsistentes. Esta alarma se borra cuando los datos se vuelven consistentes.

Esta alarma se genera cuando los datos de LdapServer en el clúster son incompatibles con los datos de LdapServer en Manager. Esta alarma se borra cuando los datos se vuelven consistentes.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
25004	Crítica	Sí

Parámetros

Parámetro	Descripción
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Host para el que se genera la alarma.

Impacto en el sistema

La incoherencia de datos de LdapServer se produce porque los datos de LdapServer en Manager o en el clúster están dañados. El proceso LdapServer con datos dañados no puede proporcionar servicios externamente, y las funciones de autenticación de Manager y del clúster se ven afectadas.

Causas posibles

- El proceso LdapServer con datos dañados no puede proporcionar servicios externamente, y las funciones de autenticación de Manager y del clúster se ven afectadas.
- El proceso LdapServer es anormal.
- El reinicio del sistema operativo daña los datos de LdapServer.

Procedimiento

Paso 1 Compruebe si la red donde residen los nodos LdapServer es defectuosa.

1. Vaya a la página de detalles del clúster y elija **Alarms**.

2. Registre la dirección IP de **HostName** en **Location** de la alarma como **IP1** (si existen varias alarmas, registre las direcciones IP como **IP1**, **IP2** y **IP3** respectivamente).
3. Póngase en contacto con el personal de O&M y utilice PuTTY para iniciar sesión en el nodo correspondiente a **IP1**. Ejecute el comando **ping** en el nodo para comprobar si se puede hacer ping a la dirección IP del plano de gestión del nodo OMS activo.
   - En caso afirmativo, vaya a **Paso 1.4**.
   - Si no, vaya a **Paso 2.1**.
4. Póngase en contacto con el personal de O&M para recuperar la red y comprobar si la alarma **ALM-25004 Sincronización anormal de datos de LdapServer** está borrada.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 2.1**.

Paso 2 Compruebe si el proceso LdapServer está en estado normal.

1. Vaya a la página de detalles del clúster y elija **Alarms**.
2. Comprobar si ALM-12004 Recurso OLdap es anormal se genera para LdapServer.
   - En caso afirmativo, vaya a **Paso 2.3**.
   - Si no, vaya a **Paso 2.5**.
3. Rectifique la falla siguiendo los pasos indicados en **ALM-12004 Recurso OLdap es anormal**.
4. Compruebe si la alarma ALM-25004 Sincronización anormal de datos de LdapServer está borrada.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 2.5**.
5. En la página **Alarms** del MRS Manager, compruebe si se genera la alarma ALM-12007 Falla de proceso de LdapServer.
   - En caso afirmativo, vaya a **Paso 2.6**.
   - Si no, vaya a **Paso 3.1**.
6. Rectifique la falla siguiendo los pasos proporcionados en ALM-12007 Falla de proceso.
7. Compruebe si la alarma ALM-25004 Sincronización anormal de datos de LdapServer está borrada.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 3.1**.

Paso 3 Comprueba si el reinicio del sistema operativo daña los datos de LdapServer.

1. Vaya a la página de detalles del clúster y elija **Alarms**.
2. Registre la dirección IP de **HostName** en **Location** de la alarma como **IP1** (si existen varias alarmas, registre las direcciones IP como **IP1**, **IP2** y **IP3** respectivamente). Seleccione **Services** > **LdapServer** > **Service Configuration** y registre el número de puerto LdapServer como **PORT**. (Si la dirección IP en la información de ubicación de alarma es la dirección IP del nodo OMS en espera, el número de puerto predeterminado es 21750.)
3. Inicie sesión en el nodo **IP1** como usuario **omm** y ejecute el comando **ldapsearch -H ldaps://IP1:PORT -x -LLL -b dc=hadoop,dc=com** (si la dirección IP es la dirección IP del nodo OMS en espera, ejecute el comando **ldapsearch -H ldaps://IP1:PORT -x -LLL -b dc=hadoop,dc=com** antes de ejecutar este comando). Compruebe si la información de error se muestra en la salida del comando.

– En caso afirmativo, vaya a **Paso 3.4**.
– Si no, vaya a **Paso 4**.

4. Recupere los nodos LdapServer y OMS utilizando datos de respaldo antes de generar la alarma. Para obtener más información, consulte la sección "Recuperación de datos de Manager" en el *Guía de administrador*.

   NOTA

   Utilice los datos de OMS y los datos de LdapServer respaldados al mismo tiempo para restaurar los datos. De lo contrario, el servicio y la operación pueden fallar. Para recuperar datos cuando los servicios se ejecutan correctamente, se le aconseja hacer una copia de respaldo manual de los últimos datos de gestión y luego recuperar los datos. De lo contrario, se perderán los datos del Manager generados entre el punto de copia de respaldo y el punto de recuperación.

5. Compruebe si la alarma ALM-25004 Sincronización anormal de datos de LdapServer está borrada.
   – En caso afirmativo, no es necesario hacer nada más.
   – Si no, vaya a **Paso 4**.

Paso 4 Recopile información de fallas.

1. En MRS Manager, seleccione **System** > **Export Log**.
2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Referencia

Ninguna

8.5.85 ALM-25500 El servicio KrbServer no está disponible (Para MRS 2.*x* o anterior)

Descripción

El sistema comprueba el estado del servicio KrbServer cada 30 segundos. Esta alarma se genera cuando el servicio KrbServer es anormal.

Esta alarma se borra cuando el servicio KrbServer está en estado normal.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
25500	Crítica	Sí

Parámetros

Parámetro	Descripción
ServiceName	Especifica el servicio para el que se genera la alarma.

Parámetro	Descripción
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

Cuando se genera esta alarma, no se puede realizar ninguna operación para el componente KrbServer en el clúster. La autenticación de KrbServer en otros componentes se verá afectada. El estado de los componentes que dependen de KrbServer en el clúster es **Bad**.

Causas posibles

- El nodo donde se encuentra el servicio KrbServer es defectuoso.
- El servicio OLdap no está disponible.

Procedimiento

Paso 1 Compruebe si el nodo donde se encuentra el servicio KrbServer es defectuoso.

1. Vaya a la página de detalles del clúster MRS y haga clic en **Components**.
2. Elija **KrbServer** > **Instances**. Vaya a la página de instancia KrbServer y vea el nombre de host del nodo donde se despliega el servicio KrbServer.
3. En la página **Alarms** del MRS Manager, compruebe si se genera la alarma ALM-12006 Falla de nodo.
   - En caso afirmativo, vaya a **Paso 1.4**.
   - Si no, vaya a **Paso 2.1**.
4. Compruebe si el nombre de host en la información de alarma es el mismo que el nombre de host real en **Paso 1.2**.
   - En caso afirmativo, vaya a **Paso 1.5**.
   - Si no, vaya a **Paso 2.1**.
5. Rectifique la falla siguiendo los pasos proporcionados en ALM-12006 Falla de nodo.
6. En la lista de alarmas, compruebe si la alarma ALM-25500 Servicio KrbServer no disponible está borrado.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 3**.

Paso 2 Compruebe si el servicio OLdap no está disponible.

1. Vaya a la página de detalles del clúster y elija **Alarms**.
2. Compruebe si se genera ALM-12004 Recurso OLdap es anormal.
   - En caso afirmativo, vaya a **Paso 2.3**.
   - Si no, vaya a **Paso 3**.
3. Rectifique la falla siguiendo los pasos proporcionados en ALM-12004 Recurso OLdap es anormal.

4. En la lista de alarmas, compruebe si la alarma ALM-25500 Servicio KrbServer no disponible está borrado.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 3**.

Paso 3 Recopile información de fallas.

1. En MRS Manager, elija **System** > **Export Log**.
2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Referencia

Ninguna

8.5.86 ALM-26051 Servicio de Storm no disponible (Para MRS 2.*x* o anterior)

Descripción

El sistema comprueba la disponibilidad del servicio Storm cada 30 segundos. Esta alarma se genera si el servicio Storm no está disponible después de que todos los nodos Nimbus de un clúster se vuelven anormales.

Esta alarma se borra después de que el servicio Storm se recupere.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
26051	Crítica	Sí

Parámetros

Parámetro	Descripción
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

- El clúster no puede proporcionar el servicio Storm.

- Los usuarios no pueden ejecutar tareas nuevas de Storm.

Causas posibles

- El componente de Kerberos es defectuoso.
- ZooKeeper está defectuoso o suspendido.
- Los nodos de Nimbus activos y en espera en el clúster Storm son anormales.

Procedimiento

Paso 1 Compruebe el estado del componente de Kerberos. Para los clústeres sin autenticación de Kerberos, omita este paso y vaya a **Paso 2**.

1. Vaya a la página de detalles del clúster MRS y haga clic en **Components**.
2. Compruebe si el estado del servicio de Kerberos es de **Good**.
   - En caso afirmativo, vaya a **Paso 2.1**.
   - Si no, vaya a **Paso 1.3**.
3. Rectifique la falla siguiendo las instrucciones en ALM-25500 Servicio de KrbServer no disponible.
4. Realice **Paso 1.2** de nuevo.

Paso 2 Compruebe el estado del componente de ZooKeeper.

1. Compruebe si el estado de salud del servicio ZooKeeper es **Good**.
   - En caso afirmativo, vaya a **Paso 3.1**.
   - Si no, vaya a **Paso 2.2**.
2. Si se detiene el servicio de ZooKeeper, inícielo. Para otros problemas, siga las instrucciones en ALM-13000 Servicio de ZooKeeper no disponible.
3. Realice **Paso 2.1** de nuevo.

Paso 3 Compruebe el estado de los nodos de Nimbus activos y en espera.

1. Elija **Components** > **Storm** > **Nimbus**.
2. En **Role**, compruebe si solo existe un nodo de Nimbus activo.
   - En caso afirmativo, vaya a **Paso 4**.
   - Si no, vaya a **Paso 3.3**.
3. Seleccione las dos instancias de Nimbus y elija **More** > **Restart Instance**. Compruebe si el reinicio se realiza correctamente.
   - En caso afirmativo, vaya a **Paso 3.4**.
   - Si no, vaya a **Paso 4**.
4. Inicie sesión de nuevo en MRS Manager y elija **Components** > **Storm** > **Nimbus**. Comprueba si el estado de salud de Nimbus es **Good**.
   - En caso afirmativo, vaya a **Paso 3.5**.
   - Si no, vaya a **Paso 4**.
5. Espere 30 segundos y compruebe si la alarma está desactivada.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 4**.

Paso 4 Recopilar información de fallas.

1. En MRS Manager, seleccione **System** > **Export Log**.
2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Información relacionada

N/A

8.5.87 ALM-26052 El número de supervisores disponibles en Storm es inferior al umbral (Para MRS 2.*x* o anterior)

Descripción

El sistema comprueba el número de supervisores cada 60 segundos y lo compara con el umbral. Esta alarma se genera si el número de supervisores es inferior al umbral.

Para modificar el umbral, los usuarios pueden elegir **System** > **Threshold Configuration** en MRS Manager.

Esta alarma se borra si el número de supervisores es mayor o igual que el umbral.

Atributo

ID de alarma	Gravedad de alarma	Borrar automáticamente
26052	Grave	Sí

Parámetros

Parámetro	Descripción
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger Condition	Genera una alarma cuando el valor real del indicador excede el umbral especificado.

Impacto en el sistema

- Las tareas existentes en el clúster no se pueden ejecutar.
- El clúster puede recibir nuevas tareas de Storm pero no puede ejecutarlas.

Causas posibles

Los supervisores son anormales en el clúster.

Procedimiento

Paso 1 Verifique el estado del supervisor.

1. Vaya a la página de detalles del clúster y haga clic en **Components**.
2. Elija **Storm** > **Supervisor**.
3. En el caso de **Role**, compruebe si el clúster tiene instancias de supervisor que estén en estado **Faulty** o **Recovering**.
   - En caso afirmativo, vaya a **Paso 1.4**.
   - Si no, vaya a **Paso 2**.
4. Seleccione las instancias de supervisor que se encuentran en el estado **Faulty** o **Recovering** y elija **More** > **Restart Instance**.
   - En caso afirmativo, vaya a **Paso 1.5**.
   - Si el reinicio falla, vaya a **Paso 2**.
5. Espere 30 segundos y compruebe si la alarma está desactivada.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 2**.

Paso 2 Recopilar información de fallas.

1. En MRS Manager, seleccione **System** > **Export Log**.
2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Información relacionada

N/A

8.5.88 ALM-26053 El uso de la ranura de la Storm supera el umbral (Para MRS 2.*x* o anterior)

Descripción

El sistema comprueba el uso de la ranura de Storm cada 60 segundos y lo compara con el umbral. Esta alarma se genera si el uso de ranura excede el umbral.

Para modificar el umbral, los usuarios pueden elegir **System** > **Threshold Configuration** en MRS Manager.

Esta alarma se borra si el uso de ranura es inferior o igual al umbral.

Atributo

ID de alarma	Gravedad de alarma	Borrar automáticamente
26053	Grave	Sí

Parámetros

Parámetro	Descripción
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger condition	Genera una alarma cuando el valor real del indicador excede el umbral especificado.

Impacto en el sistema

Los usuarios no pueden ejecutar tareas nuevas de Storm.

Causas posibles

- Los supervisores son anormales en el clúster.
- Los supervisores son normales pero tienen una capacidad de procesamiento deficiente.

Procedimiento

Paso 1 Verifique el estado del supervisor.

1. Vaya a la página de detalles del clúster y haga clic en **Components**.
2. Elija **Storm** > **Supervisor**.
3. En el caso de **Role**, compruebe si el clúster tiene instancias de supervisor que estén en estado **Faulty** o **Recovering**.
   - En caso afirmativo, vaya a **Paso 1.4**.
   - Si no es así, vaya a **Paso 2.1** o **Paso 3.1**.
4. Seleccione las instancias de supervisor que se encuentran en el estado **Faulty** o **Recovering** y elija **More** > **Restart Instance**.
   - En caso afirmativo, vaya a **Paso 1.5**.
   - Si el reinicio falla, vaya a **Paso 4**.
5. Espere un momento y compruebe si la alarma está desactivada.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no es así, vaya a **Paso 2.1** o **Paso 3.1**.

Paso 2 Aumentar el número de ranuras para los supervisores.

1. Vaya a la página de detalles del clúster y haga clic en **Components**.
2. Elija **Storm** > **Supervisor** > **Service Configuration**, y establezca **Type** en **All**.

3. Aumente el valor de **supervisor.slots.ports** para aumentar el número de espacios para cada supervisor. A continuación, reinicie las instancias.
4. Espere un momento y compruebe si la alarma está desactivada.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 4**.

Paso 3 Ampliar la capacidad de los supervisores.

1. Agregue nodos.
2. Espere un momento y compruebe si la alarma está desactivada.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si el reinicio falla, vaya a **Paso 4**.

Paso 4 Recopilar información de fallas.

1. En MRS Manager, seleccione **System** > **Export Log**.
2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Información relacionada

N/A

8.5.89 ALM-26054 El uso de memoria heap de Storm Nimbus supera el umbral (Para MRS 2.*x* o anterior)

Descripción

El sistema comprueba el uso de memoria heap de Storm Nimbus cada 30 segundos y lo compara con el umbral. Esta alarma se genera si el uso de memoria heap excede el umbral (80% de forma predeterminada).

Para modificar el umbral, los usuarios pueden elegir **System** > **Threshold Configuration** > **Service** > **Storm** en MRS Manager.

Esta alarma se borra si el uso de memoria heap es inferior o igual al umbral.

Atributo

ID de alarma	Gravedad de alarma	Borrar automáticamente
26054	Grave	Sí

Parámetros

Parámetro	Descripción
ServiceName	Especifica el servicio para el que se genera la alarma.

Parámetro	Descripción
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger Condition	Genera una alarma cuando el valor real del indicador excede el umbral especificado.

Impacto en el sistema

Es posible que se produzca una recolección frecuente de basura de memoria o un desbordamiento de memoria, lo que afecta al envío de los servicios de Storm.

Causas posibles

El uso de la memoria heap es alto o la memoria heap está asignada incorrectamente.

Procedimiento

Paso 1 Compruebe el uso de la memoria heap.

1. Vaya a la página de detalles del clúster y elija **Alarms**.
2. Elija **ALM-26054 Heap Memory Usage of Storm Nimbus Exceeds the Threshold > Location**. Consulte el **HostName** de la instancia con alarma.
3. Elija **Components > Storm > Instances > Nimbus (corresponding to the HostName of the alarmed instance) > Customize > Heap Memory Usage of Nimbus**.
4. Compruebe si el uso de memoria heap de Nimbus ha alcanzado el umbral (80%).
   - En caso afirmativo, vaya a **Paso 1.5**.
   - Si no, vaya a **Paso 2**.
5. Ajuste la memoria heap.

   Elija **Components > Storm > Service Configuration** y establezca **Type** en **All**. Elija **Nimbus** > **System**. Aumente el valor de **-Xmx** en **NIMBUS_GC_OPTS**. Haga clic en **Save Configuration**. Seleccione **Restart the affected services or instances** y haga clic en **OK**.
6. Verifique si la alarma se ha borrado.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 2**.

Paso 2 Recopilar información de fallas.

1. En MRS Manager, seleccione **System** > **Export Log**.
2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Información relacionada

N/A

8.5.90 ALM-27001 DBService no disponible (Para MRS 2.*x* o anterior)

Descripción

El módulo de alarma comprueba el estado de DBService cada 30 segundos. Esta alarma se genera cuando el sistema detecta que DBService no está disponible.

Esta alarma se borra cuando DBService se recupera.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
27001	Crítica	Sí

Parámetros

Parámetro	Descripción
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

El servicio de base de datos no está disponible y no puede proporcionar funciones de importación y consulta de datos para los servicios de capa superior, lo que da como resultado excepciones de servicio.

Causas posibles

- La dirección IP flotante no existe.
- No hay una instancia de DBServer activa.
- Los procesos DBServer activo y en espera son anormales.

Procedimiento

Paso 1 Compruebe si la dirección IP flotante existe en el entorno del clúster.

1. Vaya a la página de detalles del clúster MRS y haga clic en **Components**.
2. Elija **DBService** > **Instances**.
3. Compruebe si existe la instancia activa.
   - En caso afirmativo, vaya a **Paso 1.4**.
   - Si no, vaya a **Paso 2.1**.
4. Seleccione la instancia de DBServer activa y registre la dirección IP.
5. Inicie sesión en el host con la dirección IP anterior y ejecute el comando **ifconfig** para comprobar si la dirección IP flotante DBService existe en el nodo.
   - En caso afirmativo, vaya a **Paso 1.6**.
   - Si no, vaya a **Paso 2.1**.
6. Ejecute el comando **ping** *floating IP address* para comprobar si la dirección IP flotante DBService se puede hacer ping.
   - En caso afirmativo, vaya a **Paso 1.7**.
   - Si no, vaya a **Paso 2.1**.
7. Inicie sesión en el host donde se encuentra la dirección IP flotante DBService y ejecute el comando **ifconfig** *interface* **down** para eliminar la dirección IP flotante.
8. Elija **Components** > **DBService** > **More** > **Restart Service** para reiniciar DBService y compruebe si DBService se ha iniciado correctamente.
   - En caso afirmativo, vaya a **Paso 1.9**.
   - Si no, vaya a **Paso 2.1**.
9. Espere unos 2 minutos y compruebe si la alarma está borrada en la lista de alarmas.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 13**.

Paso 2 Compruebe el estado de la instancia de DBServer activa.

1. Seleccione la instancia de DBServer cuyo estado de rol es anormal y registre la dirección IP.
2. En la página **Alarms**, compruebe si ALM-12007 Falla de proceso produce en la instancia de DBServer en el host que corresponde a la dirección IP.
   - En caso afirmativo, vaya a **Paso 2.3**.
   - Si no, vaya a **Paso 4**.
3. Rectifique la falla siguiendo los pasos proporcionados en ALM-12007 Falla de proceso.
4. Espere unos 5 minutos y compruebe si la alarma está borrada en la lista de alarmas.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 4**.

Paso 3 Compruebe el estado de los DBServers activo y en espera.

1. Inicie sesión en el host donde se encuentra la dirección IP flotante de DBService, ejecute los comandos **sudo su - root** y **su - omm** para cambiar a usuario **omm** y ejecute el comando **cd ${BIGDATA_HOME}/FusionInsight/dbservice/** para ir al directorio de instalación de DBService.
2. Ejecute el comando **sh sbin/status-dbserver.sh** para ver el estado de los procesos de HA activos y en espera de DBService. Determine si el estado se puede ver correctamente.
   - En caso afirmativo, vaya a **Paso 3.3**.

- Si no, vaya a **Paso 4**.

3. Compruebe si los procesos de HA activo y en espera son anormales.
   - En caso afirmativo, vaya a **Paso 3.4**.
   - Si no, vaya a **Paso 4**.
4. Elija **Components** > **DBService** > **More** > **Restart Service** para reiniciar DBService y compruebe si DBService se ha iniciado correctamente.
   - En caso afirmativo, vaya a **Paso 3.5**.
   - Si no, vaya a **Paso 4**.
5. Espere unos 2 minutos y compruebe si la alarma está borrada en la lista de alarmas.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 4**.

Paso 4 Recopilar información de fallas.

1. En MRS Manager, seleccione **System** > **Export Log**.
2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Referencia

Ninguna

8.5.91 ALM-27003 Interrupción del latido del corazón entre los nodos activo y en espera de DBService (Para MRS 2.*x* o anterior)

Descripción

Esta alarma se genera cuando el nodo DBService activo o en espera no recibe mensajes de latidos del nodo par.

Esta alarma se borra cuando se recupera el latido del corazón.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
27003	Grave	Sí

Parámetros

Parámetro	Descripción
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.

Parámetro	Descripción
HostName	Especifica el host para el que se genera la alarma.
Local DBService HA Name	Especifica un HA de DBService local.
Peer DBService HA Name	Especifica un HA de DBService del mismo nivel.

Impacto en el sistema

Durante la interrupción del latido de DBService, solo un nodo puede proporcionar el servicio. Si este nodo es defectuoso, no hay ningún nodo en espera disponible para la conmutación por error y el servicio no está disponible.

Causas posibles

El vínculo entre los nodos DBService activo y en espera es anormal.

Procedimiento

Paso 1 Compruebe si la red entre los servidores de DBService activo y en espera está en estado normal.

1. Vaya a la página de detalles del clúster y elija **Alarms**.
2. En la lista de alarmas, busque la fila que contiene la alarma y vea la dirección IP del servidor DBService en espera en los detalles de la alarma.
3. Inicie sesión en el servidor de DBService activo.
4. Ejecute el comando **ping** *heartbeat IP address of the standby DBService* para comprobar si el servidor DBService en espera es accesible.
   - En caso afirmativo, vaya a **Paso 2**.
   - Si no, vaya a **Paso 1.5**.
5. Póngase en contacto con el administrador de la red para comprobar si la red es defectuosa.
   - En caso afirmativo, vaya a **Paso 1.6**.
   - Si no, vaya a **Paso 2**.
6. Rectifique la falla de la red y compruebe si la alarma está borrada de la lista de alarmas.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 2**.

Paso 2 Recopilar información de fallas.

1. En MRS Manager, seleccione **System** > **Export Log**.
2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Referencia

Ninguna

8.5.92 ALM-27004 Incoherencia de datos entre DBServices activos y en espera (Para MRS 2.*x* o anterior)

Descripción

El sistema comprueba el estado de sincronización de datos entre los DBServices activo y en espera cada 10 segundos. Esta alarma se genera cuando el estado de sincronización no se puede consultar durante seis veces consecutivas o cuando el estado de sincronización es anormal.

Esta alarma se borra cuando la sincronización está en estado normal.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
27004	Crítica	Sí

Parámetros

Parámetro	Descripción
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Local DBService HA Name	Especifica un HA de DBService local.
Peer DBService HA Name	Especifica un HA de DBService del mismo nivel.
SYNC_PERSENT	Porcentaje de sincronización.

Impacto en el sistema

Cuando los datos no están sincronizados entre los DBServices activo y en espera, los datos pueden perderse o ser anormales si la instancia activa se vuelve anormal.

Causas posibles

- La red entre los nodos activos y en espera es inestable.

- El DBService en espera es anormal.
- El espacio de disco del nodo en espera está lleno.

Procedimiento

Paso 1 Compruebe si la red entre los nodos activos y en espera está en estado normal.

1. Vaya a la página de detalles del clúster y elija **Alarms**.
2. En la lista de alarmas, localice la fila que contiene la alarma y vea la dirección IP del nodo DBService en espera en los detalles de la alarma.
3. Inicie sesión en el nodo DBService activo.
4. Ejecute el comando **ping** *heartbeat IP address of the standby DBService* para comprobar si el nodo de DBService en espera es accesible.
   - En caso afirmativo, vaya a **Paso 2.1**.
   - Si no, vaya a **Paso 1.5**.
5. Póngase en contacto con el personal de O&M para comprobar si la red es defectuosa.
   - En caso afirmativo, vaya a **Paso 1.6**.
   - Si no, vaya a **Paso 2.1**.
6. Rectifique la falla de la red y compruebe si la alarma está borrada de la lista de alarmas.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 2.1**.

Paso 2 Compruebe si el DBService en espera está en estado normal.

1. Inicie sesión en el nodo de DBService en espera.
2. Ejecute los siguientes comandos para cambiar el usuario:

   sudo su - root

   su - omm
3. Vaya al directorio **${DBSERVER_HOME}/sbin** y ejecute el comando **./status-dbserver.sh** para comprobar si el estado del recurso de GaussDB del DBService en espera está en estado normal. En la salida del comando, compruebe si se muestra la siguiente información en la fila donde **ResName** es **gaussDB**:

   Ejemplo:

   ```
   10_10_10_231 gaussDB Standby_normal Normal Active_standby
   ```
   - En caso afirmativo, vaya a **Paso 3.1**.
   - Si no, vaya a **Paso 4**.

Paso 3 Compruebe si el espacio en disco del nodo en espera es insuficiente.

1. Inicie sesión en el nodo de DBService en espera.
2. Ejecute los siguientes comandos para cambiar el usuario:

   sudo su - root

   su - omm
3. Vaya al directorio **${DBSERVER_HOME}** y ejecute los siguientes comandos para obtener el directorio de datos de DBService:

   cd ${DBSERVER_HOME}

   source .dbservice_profile

echo ${DBSERVICE_DATA_DIR}

4. Ejecute el comando **df -h** para comprobar el uso de la partición del disco del sistema.
5. Compruebe si el espacio de directorio de datos de DBService está lleno.
   - En caso afirmativo, vaya a **Paso 3.6**.
   - Si no, vaya a **Paso 4**.
6. Realice la actualización y amplíe la capacidad.
7. Después de la ampliación de la capacidad, espere 2 minutos y compruebe si la alarma está desactivada.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 4**.

Paso 4 Recopilar información de fallas.

1. En MRS Manager, seleccione **System** > **Export Log**.
2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Referencia

Ninguna

8.5.93 ALM-28001 Servicio de Spark no disponible (Para MRS 2.*x* o anterior)

Descripción

El sistema comprueba el estado del servicio Spark cada 30 segundos. Esta alarma se genera cuando el servicio Spark no está disponible.

Esta alarma se borra cuando el servicio Spark se recupera.

Atributo

ID de alarma	Gravedad de alarma	Borrar automáticamente
28001	Crítica	Sí

Parámetros

Parámetro	Descripción
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.

Parámetro	Descripción
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

Las tareas de Spark enviadas por los usuarios no se pueden ejecutar.

Causas posibles

- El servicio KrbServer es anormal.
- El servicio LdapServer es anormal.
- El servicio ZooKeeper es anormal.
- El servicio HDFS es anormal.
- El servicio Yarn es anormal.
- El servicio Hive correspondiente es anormal.

Procedimiento

Paso 1 Compruebe si existen alarmas de indisponibilidad de servicio en los servicios de los que depende Spark.

1. Vaya a la página de detalles del clúster de MRS y elija **Alarms**.
2. Compruebe si existen las siguientes alarmas en la lista de alarmas:
   a. ALM-25500 Servicio KrbServer no disponible
   b. ALM-25000 Servicio LdapServer no disponible
   c. ALM-13000 Servicio ZooKeeper no disponible
   d. ALM-14000 Servicio HDFS no disponible
   e. ALM-18000 Servicio Yarn no disponible
   f. ALM-16004 Servicio Hive no disponible
   – En caso afirmativo, vaya a **Paso 1.3**.
   – Si no, vaya a **Paso 2**.
3. Manejar las alarmas basándose en los métodos de solución de problemas proporcionados en la ayuda de alarma.

   Después de que la alarma esté desactivada, espere unos minutos y compruebe si la alarma Servicio HetuServer no disponible está borrada.
   – En caso afirmativo, no es necesario hacer nada más.
   – Si no, vaya a **Paso 2**.

Paso 2 Recopilar información de fallas.

1. En MRS Manager, seleccione **System** > **Export Log**.
2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Referencia

Ninguna

8.5.94 ALM-38000 Servicio Kafka no disponible (Para MRS 2.*x* o anterior)

Descripción

El sistema comprueba la disponibilidad del servicio Kafka cada 30 segundos. Esta alarma se genera si el servicio Kafka no está disponible.

Esta alarma se borra después de que se recupere el servicio Kafka.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
38000	Crítica	Sí

Parámetros

Parámetro	Descripción
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

El clúster no puede proporcionar el servicio de Kafka y los usuarios no pueden ejecutar nuevas tareas de Kafka.

Causas posibles

- El componente KrbServer está defectuoso.
- El componente ZooKeeper está defectuoso o no responde.
- El nodo Broker en el clúster de Kafka es anormal.

Procedimiento

Paso 1 Compruebe el estado del componente KrbServer. Para los clústeres sin autenticación de Kerberos, omita este paso y vaya a **Paso 2**.

1. Vaya a la página de detalles del clúster MRS y haga clic en **Components**.
2. Compruebe si el estado de salud del servicio KrbServer es de tipo **Good**.
   - En caso afirmativo, vaya a **Paso 2.1**.
   - Si no, vaya a **Paso 1.3**.
3. Rectifique la falla siguiendo las instrucciones en ALM-25500 Servicio de KrbServer no disponible.
4. Realice **Paso 1.2** de nuevo.

Paso 2 Compruebe el estado del componente de ZooKeeper.

1. Compruebe si el estado de salud del servicio ZooKeeper es **Good**.
   - En caso afirmativo, vaya a **Paso 3.1**.
   - Si no, vaya a **Paso 2.2**.
2. Si se detiene el servicio de ZooKeeper, inícielo. Para otros problemas, siga las instrucciones en ALM-13000 Servicio de ZooKeeper no disponible.
3. Realice **Paso 2.1** de nuevo.

Paso 3 Compruebe el estado del Broker.

1. Elija **Components** > **Kafka** > **Broker**.
2. En el **Role**, compruebe si todas las instancias son normales.
   - En caso afirmativo, vaya a **Paso 3.4**.
   - Si no, vaya a **Paso 3.3**.
3. Seleccione todas las instancias de Broker y elija **More** > **Restart Instance**.
   - Si el reinicio se realiza correctamente, vaya a **Paso 3.4**.
   - Si el reinicio falla, vaya a **Paso 4**.
4. Elija **Components > Kafka**. Compruebe si el estado de salud de Kafka es **Good**.
   - En caso afirmativo, vaya a **Paso 3.5**.
   - Si no, vaya a **Paso 4**.
5. Espere 30 segundos y compruebe si la alarma está desactivada.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 4**.

Paso 4 Recopilar información de fallas.

1. En MRS Manager, seleccione **System** > **Export Log**.
2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Información relacionada

N/A

8.5.95 ALM-38001 Capacidad de disco de Kafka insuficiente (para MRS 2.*x* o anterior)

Descripción

El sistema comprueba el uso del disco de Kafka cada 60 segundos y lo compara con el umbral. Esta alarma se genera si el uso del disco excede el umbral.

Para modificar el umbral, los usuarios pueden elegir **System** > **Threshold Configuration** en MRS Manager.

Esta alarma se borra si el uso del disco de Kafka es inferior o igual al umbral.

Atributo

ID de alarma	Gravedad de alarma	Borrar automáticamente
38001	Grave	Sí

Parámetros

Parámetro	Descripción
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
PartitionName	Especifica la partición de disco donde se genera la alarma.
Trigger Condition	Genera una alarma cuando el valor real del indicador excede el umbral especificado.

Impacto en el sistema

Kafka no puede escribir datos en los discos.

Causas posibles

- Las configuraciones de disco de Kafka (como el número de discos y el tamaño del disco) son insuficientes para el volumen de datos.
- El período de retención de datos es largo y los datos históricos ocupan un gran espacio.
- Los servicios están mal planeados. Como resultado, los datos se distribuyen de manera desigual y algunos discos están llenos.

Procedimiento

Paso 1 Vaya a la página de detalles del clúster de MRS y elija **Alarms**.

Paso 2 En la lista de alarmas, haga clic en la alarma y vea el **HostName** y **PartitionName** de la alarma en **Location** de **Alarm Details**.

Paso 3 En la página **Hosts**, haga clic en el nombre de host obtenido en **Paso 2**.

Paso 4 Compruebe si el área **Disk** contiene el **PartitionName** de la alarma.

- En caso afirmativo, vaya a **Paso 5**.
- En caso negativo, borre manualmente la alarma y no se requiere ninguna acción adicional.

Paso 5 En el área **Disk**, compruebe si el uso de la partición alarmada ha alcanzado el 100%.

- En caso afirmativo, vaya a **Paso 6**.
- Si no, vaya a **Paso 8**.

Paso 6 En **Instance**, seleccione **Broker > Instance Configuration**. En la página **Instance Configuration** que se muestra, establezca **Type** en **All** y consulte el parámetro **log.dirs** del directorio de datos.

Paso 7 Elija **Components > Kafka > Instances**. En la página **Kafka Instance** que se muestra, detenga la instancia del Broker correspondiente a **Paso 2**. A continuación, inicie sesión en el nodo alarmado y elimine manualmente el directorio de datos en **Paso 6**. Una vez completadas todas las operaciones posteriores, inicie la instancia del Broker.

Paso 8 Elija **Components > Kafka > Service Configuration**. Se muestra la página **Kafka Configuration**.

Paso 9 Comprueba si **disk.adapter.enable** es **true**.

- En caso afirmativo, vaya a **Paso 11**.
- Si no, cambie el valor a **true** y vaya a **Paso 10**.

Paso 10 Compruebe si el parámetro **adapter.topic.min.retention.hours**, que indica el período mínimo de retención de datos, está configurado correctamente.

- En caso afirmativo, vaya a **Paso 12**.
- Si no, configúrelo en un valor adecuado y vaya a **Paso 12**.

NOTA

Si el período de retención no se puede ajustar para ciertos temas, los temas se pueden agregar a **disk.adapter.topic.blacklist**.

Paso 11 Espere 10 minutos y compruebe si se reduce el uso del disco.

- En caso afirmativo, espere hasta que se borre la alarma.
- Si no, vaya a **Paso 12**.

Paso 12 Vaya a la página **Kafka Topic Monitor** y consulte el período de retención de datos configurado para Kafka. Determine si es necesario acortar el período de retención en función de los requisitos de servicio y el volumen de datos.

- En caso afirmativo, vaya a **Paso 13**.
- Si no, vaya a **Paso 14**.

Paso 13 Encuentre los temas con grandes volúmenes de datos basados en la partición de disco obtenida en **Paso 2**. Inicie sesión en el cliente de Kafka y acorte manualmente el período de retención de datos para estos temas mediante el siguiente comando:

kafka-topics.sh --zookeeper *ZooKeeper address:24002/kafka* **--alter --topic** *Topic name* **--config retention.ms=***Retention period*

Paso 14 Compruebe si las particiones están configuradas correctamente para los temas. Por ejemplo, si el número de particiones para un tema con un volumen de datos grande es menor que el número de discos, los datos pueden distribuirse de manera desigual a los discos y el uso de algunos discos alcanzará el límite superior.

NOTA

Para identificar temas con grandes volúmenes de datos, inicie sesión en los nodos relevantes que se obtienen en **Paso 2**, vaya al directorio de datos (el directorio antes de modificar **log.dirs** en **Paso 6**) y compruebe el espacio en disco ocupado por las particiones de los temas.

- Si las particiones no están configuradas correctamente, vaya a **Paso 15**.
- Si las particiones están configuradas correctamente, vaya a **Paso 16**.

Paso 15 En el cliente de Kafka, agregue particiones a los temas.

kafka-topics.sh --zookeeper *ZooKeeper address:24002/kafka* **--alter --topic** *Topic name* **--partitions=***Number of new partitions*

NOTA

Se recomienda establecer el número de particiones nuevas en un múltiplo del número de discos Kafka.

Esta operación puede no borrar rápidamente la alarma. Los datos se equilibrarán gradualmente entre los discos.

Paso 16 Compruebe si es necesario ampliar la capacidad del clúster.

- En caso afirmativo, agregue nodos al clúster y vaya a **Paso 17**.
- Si no, vaya a **Paso 17**.

Paso 17 Espere un momento y compruebe si la alarma está desactivada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 18**.

Paso 18 Recopile información de fallas.

1. En MRS Manager, seleccione **System** > **Export Log**.
2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Información relacionada

N/A

8.5.96 ALM-38002 El uso de memoria heap de Kafka supera el umbral (para MRS 2.*x* o anterior)

Descripción

El sistema comprueba el uso de memoria heap de Kafka cada 30 segundos. Esta alarma se genera si el uso de memoria heap de Kafka excede el umbral (80%).

Esta alarma se borra si el uso de memoria heap es menor que el umbral.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
38002	Grave	Sí

Parámetros

Parámetro	Descripción
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger Condition	Genera una alarma cuando el valor real del indicador excede el umbral especificado.

Impacto en el sistema

Es posible que se produzca un desbordamiento de memoria, lo que causa fallos en el servicio.

Causas posibles

El uso de la memoria heap es alto o la memoria heap está asignada incorrectamente.

Procedimiento

Paso 1 Compruebe el uso de la memoria heap.

1. Vaya a la página de detalles del clúster de MRS y elija **Alarms**.
2. Elija **ALM-38002 Kafka Heap Memory Usage Exceeds the Threshold** > **Location**. Consulte la dirección IP de la instancia con alarma.
3. Elija **Components > Kafka > Instance > Broker (corresponding to the IP address of the alarmed instance) > Customize > Kafka Heap Memory Resource Percentage** para comprobar el uso de la memoria heap.

4. Compruebe si el uso de memoria heap de Kafka ha alcanzado el umbral (80%).
   - En caso afirmativo, vaya a **Paso 1.5**.
   - Si no, vaya a **Paso 2**.
5. Elija **Components** > **Kafka** > **Service Configuration** > **All** > **Broker** > **Environment Variables**. Aumente el valor de **KAFKA_HEAP_OPTS** según sea necesario.
6. Verifique si la alarma se ha borrado.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 2**.

Paso 2 Recopile información de fallas.

1. En MRS Manager, seleccione **System** > **Export Log**.
2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Información relacionada

N/A

8.5.97 ALM-43001 Servicio Spark no disponible (Para MRS 2.*x* o anterior)

Descripción

El sistema comprueba el estado del servicio Spark cada 60 segundos. Esta alarma se genera cuando el servicio Spark no está disponible.

Esta alarma se borra cuando el servicio Spark se recupera.

Atributo

ID de alarma	Severidad de alarma	Borrado automáticamente
43001	Crítica	Sí

Parámetros

Parámetro	Descripción
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

Las tareas de Spark enviadas por los usuarios no se pueden ejecutar.

Causas posibles

- El servicio KrbServer es anormal.
- El servicio LdapServer es anormal.
- ZooKeeper es anormal.
- El servicio HDFS es anormal.
- El servicio Yarn es anormal.
- El servicio Hive correspondiente es anormal.

Procedimiento

Paso 1 Compruebe si existen alarmas de indisponibilidad de servicio en los servicios de los que depende Spark.

1. Vaya a la página de detalles del clúster y elija **Alarms**.
2. Compruebe si existen las siguientes alarmas en la lista de alarmas:
   a. ALM-25500 Servicio KrbServer no disponible
   b. ALM-25000 Servicio LdapServer no disponible
   c. ALM-13000 Servicio ZooKeeper no disponible
   d. ALM-14000 Servicio HDFS no disponible
   e. ALM-18000 Servicio Yarn no disponible
   f. ALM-16004 Servicio Hive no disponible

   – En caso afirmativo, vaya a **Paso 1.3**.
   – Si no, vaya a **Paso 2**.
3. Maneje la alarma de acuerdo con la ayuda de alarma.

   Después de que la alarma esté desactivada, espere unos minutos y compruebe si la alarma Servicio HetuServer no disponible está borrada.

   – En caso afirmativo, no es necesario hacer nada más.
   – Si no, vaya a **Paso 2**.

Paso 2 Recopilar información de fallas.

1. En MRS Manager, seleccione **System** > **Export Log**.
2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Referencia

Ninguna

8.5.98 ALM-43006 El uso de memoria de Heap del proceso de JobHistory supera el umbral (Para MRS 2.*x* o anterior)

Descripción

El sistema comprueba el estado del proceso de JobHistory cada 30 segundos. La alarma se genera cuando el uso de memoria de heap del proceso de JobHistory excede el umbral (90% de la memoria máxima).

Atributo

ID de alarma	Gravedad de la alarma	Borrado automáticamente
43006	Grave	Sí

Parámetros

Parámetro	Descripción
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

Si la memoria de heap de proceso de JobHistory disponible es insuficiente, se produce un desbordamiento de memoria y el servicio se interrumpe.

Causas posibles

La memoria de heap del proceso de JobHistory se utiliza en exceso o la memoria de heap se asigna de forma inadecuada.

Procedimiento

Paso 1 Compruebe el uso de la memoria heap.

1. Vaya a la página de detalles del clúster y elija **Alarms**.
2. Seleccione la alarma cuyo **Alarm ID** sea **43006** y vea la dirección IP y el nombre del rol de la instancia en **Location**.
3. Elija **Components** > **Spark** > **Instance** > **JobHistory** (dirección IP de la instancia para la que se genera la alarma) > **Customize** > **Heap Memory Statistics of the JobHistory Process**. Haga clic en **OK** para ver el uso de memoria de heap.

4. Compruebe si la memoria de heap utilizada de JobHistory alcanza el 90% de la memoria de heap máxima especificada para JobHistory.
   - En caso afirmativo, vaya a **Paso 1.5**.
   - Si no, vaya a **Paso 2**.
5. Elija **Components** >**Spark** >**Service Configuration**. Establezca **Type** en **All** y elija **JobHistory** >**Default**. Aumente el valor de **SPARK_DAEMON_MEMORY** según sea necesario.
6. Haga clic en **Save Configuration** y seleccione **Restart the affected services or instances**. Haga clic en **OK**.
7. Verifique si la alarma se ha borrado.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 2**.

Paso 2 Recopilar información de fallas.

1. En MRS Manager, seleccione **System** > **Export Log**.
2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Referencia

Ninguna

8.5.99 ALM-43007 El uso de memoria no heap del proceso de JobHistory supera el umbral (Para MRS 2.*x* o anterior)

Descripción

El sistema comprueba el estado del proceso de JobHistory cada 30 segundos. La alarma se genera cuando el uso de memoria no heap del proceso de JobHistory excede el umbral (90% de la memoria máxima).

Atributo

ID de alarma	Gravedad de alarma	Borrado automáticamente
43007	Grave	Sí

Parámetros

Parámetro	Descripción
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.

Parámetro	Descripción
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

Si la memoria no heap del proceso de JobHistory disponible es insuficiente, se produce un desbordamiento de memoria y el servicio se interrumpe.

Causas posibles

La memoria no heap del proceso de JobHistory se utiliza en exceso o la memoria no heap se asigna de forma inadecuada.

Procedimiento

Paso 1 Comprueba el uso de memoria no heap.

1. Vaya a la página de detalles del clúster y elija **Alarms**.
2. Seleccione la alarma cuyo **Alarm ID** sea **43007** y vea la dirección IP y el nombre del rol de la instancia en **Location**.
3. Elija **Components** > **Spark** > **Instance** > **JobHistory** (Dirección IP de la instancia para la que se genera la alarma) > **Customize** > **Non-Heap Memory Statistics of the JobHistory Process**. Haga clic en **OK** para ver el uso de memoria no heap.
4. Compruebe si el uso de memoria no heap de JobHistory ha alcanzado el umbral (90% de la memoria máxima).
   - En caso afirmativo, vaya a **Paso 1.5**.
   - Si no, vaya a **Paso 2**.
5. Elija **Components** >**Spark** >**Service Configuration**. Establezca **Type** en **All** y elija **JobHistory** >**Default**. Aumente el valor de **-XX:MaxMetaspaceSize** en **SPARK_DAEMON_JAVA_OPTS** según sea necesario.
6. Verifique si la alarma se ha borrado.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 2**.

Paso 2 Recopilar información de fallas.

1. En MRS Manager, seleccione **System** > **Export Log**.
2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Referencia

Ninguna

8.5.100 ALM-43008 El uso de memoria directa del proceso JobHistory supera el umbral (Para MRS 2.*x* o anterior)

Descripción

El sistema comprueba el estado del proceso de JobHistory cada 30 segundos. La alarma se genera cuando el uso de memoria directa del proceso JobHistory excede el umbral (90% de la memoria máxima).

Atributo

ID de alarma	Severidad de alarma	Borrado automáticamente
43008	Grave	Sí

Parámetros

Parámetro	Descripción
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

Si la memoria directa del proceso JobHistory disponible es insuficiente, se produce un desbordamiento de memoria y el servicio se interrumpe.

Causas posibles

La memoria directa del proceso JobHistory se utiliza en exceso o la memoria directa se asigna de forma inapropiada.

Procedimiento

Paso 1 Compruebe el uso de la memoria directa.

1. Vaya a la página de detalles del clúster y elija **Alarms**.
2. Seleccione la alarma cuyo **Alarm ID** sea **43008** y vea la dirección IP y el nombre del rol de la instancia de **Location**.
3. Elija **Components** > **Spark** > **Instance** > **JobHistory** (dirección IP de la instancia para la que se genera la alarma) > **Customize** > **Direct Memory Statistics of the JobHistory Process**. Haga clic en **OK** para ver el uso de la memoria directa.

4. Compruebe si el uso de memoria directa del proceso JobHistory ha alcanzado el umbral (90% de la memoria directa máxima).
   - En caso afirmativo, vaya a **Paso 1.5**.
   - Si no, vaya a **Paso 2**.
5. Elija **Components** >**Spark** >**Service Configuration**. Establezca **Type** en **All** y elija **JobHistory** >**Default**. Aumente el valor de **-XX:MaxDirectMemorySize** en el **SPARK_DAEMON_JAVA_OPTS** según sea necesario.
6. Verifique si la alarma se ha borrado.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 2**.

Paso 2 Recopilar información de fallas.

1. En MRS Manager, seleccione **System** > **Export Log**.
2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Referencia

Ninguna

8.5.101 ALM-43009 El tiempo de GC de JobHistory supera el umbral (Para MRS 2.*x* o anterior)

Descripción

El sistema comprueba el tiempo de GC del proceso de JobHistory cada 60 segundos. Esta alarma se genera cuando el tiempo GC detectado excede el umbral (12 segundos) durante tres veces consecutivas. Puede cambiar el umbral seleccionando **System** > **Threshold Configuration** > **Service** > **Spark** > **JobHistory GC Time** > **Total JobHistory GC Time**. Esta alarma se borra cuando el tiempo de GC de JobHistory es menor o igual que el umbral.

Atributo

ID de alarma	Severidad de alarma	Borrado automáticamente
43009	Grave	Sí

Parámetros

Parámetro	Descripción
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.

Parámetro	Descripción
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

Si el tiempo de GC excede el umbral, el JobHistory puede funcionar con bajo rendimiento.

Causas posibles

La memoria heap del proceso de JobHistory se usa en exceso o se asigna de forma inapropiada, lo que causa GC frecuente.

Procedimiento

Paso 1 Comprueba la hora del GC.

1. Vaya a la página de detalles del clúster y elija **Alarms**.
2. Seleccione la alarma cuyo **Alarm ID** sea **43009** y vea la dirección IP y el nombre del rol de la instancia de **Location**.
3. Elija **Components** > **Spark** > **Instance** > **JobHistory** (dirección IP de la instancia para la que se genera la alarma) > **Customize** > **GC Time of the JobHistory Process**. Haga clic en **OK** para ver la hora de GC.
4. Compruebe si el tiempo de GC del proceso de JobHistory es superior a 12 segundos.
   - En caso afirmativo, vaya a **Paso 1.5**.
   - Si no, vaya a **Paso 2**.
5. Elija **Components** >**Spark** >**Service Configuration**. Establezca **Type** en **All** y elija **JobHistory** >**Default**. Aumente el valor del parámetro **SPARK_DAEMON_MEMORY** según sea necesario.
6. Verifique si la alarma se ha borrado.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 2**.

Paso 2 Recopilar información de fallas.

1. En MRS Manager, seleccione **System** > **Export Log**.
2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Referencia

Ninguna

8.5.102 ALM-43010 El uso de memoria heap del proceso de JDBCServer supera el umbral (Para MRS 2.*x* o anterior)

Descripción

El sistema comprueba el estado del proceso de JDBCServer cada 30 segundos. La alarma se genera cuando el uso de memoria heap del proceso de JDBCServer excede el umbral (90% de la memoria máxima).

Atributo

ID de alarma	Gravedad de alarma	Borrado automáticamente
43010	Grave	Sí

Parámetros

Parámetro	Descripción
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

Si la memoria heap de procesos de JDBCServer disponible es insuficiente, se produce un desbordamiento de memoria y el servicio se interrumpe.

Causas posibles

La memoria heap del proceso de JDBCServer se utiliza en exceso o la memoria heap se asigna de forma inadecuada.

Procedimiento

Paso 1 Compruebe el uso de la memoria heap.

1. Vaya a la página de detalles del clúster y elija **Alarms**.
2. Seleccione la alarma cuyo **Alarm ID** sea **43010** y vea la dirección IP y el nombre del rol de la instancia de **Location**.
3. Elija **Components** > **Spark** > **Instance** > **JDBCServer** (dirección IP de la instancia para la que se genera la alarma) > **Customize** > **Heap Memory Statistics of the JDBCServer Process**. Haga clic en **OK** para ver el uso de memoria de heap.

4. Compruebe si el uso de memoria heap de JDBCServer ha alcanzado el umbral (90% de la memoria heap máxima).
   - En caso afirmativo, vaya a **Paso 1.5**.
   - Si no, vaya a **Paso 2**.
5. Elija **Components** >**Spark** >**Service Configuration**. Establezca **Type** en **All** y elija **JDBCServer** >**Tuning**. Aumente el valor del parámetro **SPARK_DRIVER_MEMORY** según sea necesario.
6. Verifique si la alarma se ha borrado.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 2**.

Paso 2 Recopilar información de fallas.

1. En MRS Manager, seleccione **System** > **Export Log**.
2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Referencia

Ninguna

8.5.103 ALM-43011 El uso de memoria no heap del proceso de JDBCServer supera el umbral (Para MRS 2.*x* o anterior)

Descripción

El sistema comprueba el estado del proceso de JDBCServer cada 30 segundos. La alarma se genera cuando el uso de memoria no heap del proceso de JDBCServer excede el umbral (90% de la memoria máxima).

Atributo

ID de alarma	Severidad de alarma	Borrado automáticamente
43011	Grave	Sí

Parámetros

Parámetro	Descripción
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.

Parámetro	Descripción
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

Si la memoria no heap del proceso de JDBCServer disponible es insuficiente, se produce un desbordamiento de memoria y el servicio se interrumpe.

Causas posibles

La memoria no heap del proceso de JDBCServer se utiliza en exceso o la memoria no heap se asigna de forma inapropiada.

Procedimiento

Paso 1 Comprueba el uso de memoria no heap.

1. Vaya a la página de detalles del clúster y elija **Alarms**.
2. Seleccione la alarma cuyo **Alarm ID** sea **43011** y vea la dirección IP y el nombre del rol de la instancia de **Location**.
3. Elija **Components** > **Spark** > **Instance** > **JDBCServer** (dirección IP de la instancia para la que se genera la alarma) > **Customize** > **Non-heap Memory Statistics of the JDBCServer Process**. Haga clic en **OK** para ver el uso de memoria no heap.
4. Compruebe si el uso de memoria no-heap de JDBCServer ha alcanzado el umbral (90% de la memoria máxima no-heap).
   - En caso afirmativo, vaya a **Paso 1.5**.
   - Si no, vaya a **Paso 2**.
5. Elija **Components** >**Spark** >**Service Configuration**. Establezca **Type** en **All** y elija **JDBCServer** >**Tuning**. Aumente el valor de **-XX:MaxMetaspaceSize** en **spark.driver.extraJavaOptions** según sea necesario.
6. Verifique si la alarma se ha borrado.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 2**.

Paso 2 Recopilar información de fallas.

1. En MRS Manager, seleccione **System** > **Export Log**.
2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Referencia

Ninguna

8.5.104 ALM-43012 El uso de memoria directa del proceso de JDBCServer supera el umbral (Para MRS 2.*x* o anterior)

Descripción

El sistema comprueba el estado del proceso de JDBCServer cada 30 segundos. La alarma se genera cuando el uso de memoria directa del proceso de JDBCServer excede el umbral (90% de la memoria máxima).

Atributo

ID de alarma	Gravedad de alarma	Borrado automáticamente
43012	Grave	Sí

Parámetros

Parámetro	Descripción
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

Si la memoria directa del proceso de JDBCServer disponible es insuficiente, se produce un desbordamiento de memoria y el servicio se interrumpe.

Causas posibles

La memoria directa del proceso JDBCServer se utiliza en exceso o la memoria directa se asigna de forma inadecuada.

Procedimiento

Paso 1 Compruebe el uso de la memoria directa.

1. Vaya a la página de detalles del clúster y elija **Alarms**.
2. Seleccione la alarma cuyo **Alarm ID** sea **43012** y vea la dirección IP y el nombre del rol de la instancia de **Location**.
3. Elija **Components** > **Spark** > **Instance** > **JDBCServer** (dirección IP de la instancia para la que se genera la alarma) > **Customize** > **Direct Memory Statistics of the JDBCServer Process**. Haga clic en **OK** para ver el uso de la memoria directa.

4. Compruebe si el uso de memoria directa del proceso de JDBCServer ha alcanzado el umbral (90% de la memoria directa máxima).
   - En caso afirmativo, vaya a **Paso 1.5**.
   - Si no, vaya a **Paso 2**.
5. Elija **Components** >**Spark** >**Service Configuration**. Establezca **Type** en **All** y elija **JDBCServer** >**Tuning**. Aumente el valor de **-XX:MaxDirectMemorySize** en el **spark.driver.extraJavaOptions** según sea necesario.
6. Verifique si la alarma se ha borrado.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 2**.

Paso 2 Recopilar información de fallas.

1. En MRS Manager, seleccione **System** > **Export Log**.
2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Referencia

Ninguna

8.5.105 ALM-43013 Tiempo de JDBCServer GC excede el umbral (Para MRS 2.*x* o anterior)

Descripción

El sistema comprueba el tiempo de GC del proceso JDBCServer cada 60 segundos. Esta alarma se genera cuando el tiempo GC detectado excede el umbral (12 segundos) durante tres veces consecutivas. Puede cambiar el umbral seleccionando **System** > **Threshold Configuration** > **Service** > **Spark** > **JDBCServer GC Time** > **Total JDBCServer GC Time**. Esta alarma se borra cuando el tiempo GC de JDBCServer es menor o igual que el umbral.

Atributo

ID de alarma	Severidad de alarma	Borrado automáticamente
43013	Grave	Sí

Parámetros

Parámetro	Descripción
ServiceName	Especifica el servicio para el que se genera la alarma.

Parámetro	Descripción
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

Si el tiempo GC excede el umbral, JDBCServer puede ejecutarse con bajo rendimiento.

Causas posibles

La memoria heap del proceso JDBCServer se usa en exceso o se asigna de forma inapropiada, lo que causa GC frecuente.

Procedimiento

Paso 1 Comprueba la hora del GC.

1. Vaya a la página de detalles del clúster y elija **Alarms**.
2. Seleccione la alarma cuyo **Alarm ID** sea **43013** y vea la dirección IP y el nombre del rol de la instancia de **Location**.
3. Elija **Components** > **Spark** > **Instance** > **JDBCServer** (Dirección IP de la instancia para la que se genera la alarma) > **Customize** > **GC Time of the JDBCServer Process**. Haga clic en **OK** para ver la hora de GC.
4. Compruebe si el tiempo de GC del proceso JDBCServer es superior a 12 segundos.
   - En caso afirmativo, vaya a **Paso 1.5**.
   - Si no, vaya a **Paso 2**.
5. Elija **Components** >**Spark** >**Service Configuration**. Establezca **Type** en **All** y elija **JDBCServer** >**Tuning**. Aumente el valor del parámetro **SPARK_DRIVER_MEMORY** según sea necesario.
6. Verifique si la alarma se ha borrado.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 2**.

Paso 2 Recopilar información de fallas.

1. En MRS Manager, seleccione **System** > **Export Log**.
2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Referencia

Ninguna

8.5.106 ALM-44004 Las tareas de cola de grupo de recursos de coordinador de Presto superan el umbral (Para MRS 2.*x* o anterior)

Descripción

Esta alarma se genera cuando el sistema detecta que el número de tareas de cola en un grupo de recursos excede el umbral. El sistema consulta el número de tareas de cola en un grupo de recursos a través de la interfaz JMX. Puede elegir **Components** > **Presto** > **Service Configuration** (cambiar **Basic** a **All**) > **Presto** > **resource-groups** para configurar un grupo de recursos. Puede elegir **Components** > **Presto** > **Service Configuration** (cambiar **Basic** a **All**) > **Coordinator** > **Customize** > **resourceGroupAlarm** para configurar el umbral de cada grupo de recursos.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
44004	Grave	Sí

Parámetro

Parámetro	Descripción
ServiceName	Servicio para el que se genera la alarma.
RoleName	Rol para el que se genera la alarma.
HostName	Host para el que se genera la alarma.

Impacto en el sistema

Si el número de tareas de cola en un grupo de recursos excede el umbral, un gran número de tareas puede estar en el estado de cola. El tiempo de tarea de Presto supera el valor esperado. Cuando el número de tareas de cola en un grupo de recursos excede el número máximo (**maxQueued**) de tareas de cola en el grupo de recursos, no se pueden ejecutar nuevas tareas.

Causas posibles

La configuración del grupo de recursos es incorrecta o se envían demasiadas tareas en el grupo de recursos.

Procedimiento

Paso 1 Seleccione **Components** > **Presto** > **Service Configuration** (cambiar **Basic** a **All**) > **Presto** > **resource-groups** para ajustar la configuración del grupo de recursos.

Paso 2 Puede elegir **Components** > **Presto** > **Service Configuration** (cambiar **Basic** a **All**) > **Coordinator** > **Customize** > **resourceGroupAlarm** para modificar el umbral de cada grupo de recursos.

Paso 3 Recopilar información de fallas.

1. Inicie sesión en el nodo del clúster según el nombre del host en la información de error y consulte el número de tareas de cola según **Resource Group** en la información adicional del cliente de Presto.
2. Inicie sesión en el nodo del clúster basándose en el nombre del host en la información de errores, vea el archivo **/var/log/Bigdata/nodeagent/monitorlog/monitor.log** y busque información del grupo de recursos para ver la información de recopilación de supervisión del grupo de recursos.
3. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Referencia

Ninguna

8.5.107 ALM-44005 El tiempo de GC del proceso del Presto Coordinator supera el umbral (Para MRS 2.*x* o anterior)

Descripción

El sistema recoge el tiempo de GC del proceso de Presto Coordinator cada 30 segundos. Esta alarma se genera cuando el tiempo de GC excede el umbral (excede 5 segundos durante tres veces consecutivas). Puede cambiar el umbral seleccionando **System** > **Configure Alarm Threshold** > **Service** > **Presto** > **Coordinator** > **Presto Process Garbage Collection Time** > **Garbage Collection Time of the Coordinator Process** en MRS Manager. Esta alarma se borra cuando el tiempo de proceso de GC del Coordinator es menor o igual que el umbral.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
44005	Grave	Sí

Parámetro

Parámetro	Descripción
ServiceName	Servicio para el que se genera la alarma.
RoleName	Rol para el que se genera la alarma.
HostName	Host para el que se genera la alarma.

Impacto en el sistema

Si el tiempo de GC del proceso del Coordinator es demasiado largo, el proceso del Coordinator se verá afectado y el proceso del Coordinator incluso no estará disponible.

Causas posibles

La memoria heap del proceso del Coordinator se utiliza en exceso o se asigna de manera inadecuada, lo que provoca la ocurrencia frecuente del proceso de GC.

Procedimiento

Paso 1 Comprueba el tiempo de GC.

1. Vaya a la página de detalles del clúster y elija **Alarms**.
2. Seleccione la alarma cuyo **Alarm ID** sea **44005** y vea la dirección IP y el nombre del rol de la instancia de **Location**.
3. Seleccione **Components** > **Presto** > **Instances** > **Coordinator** (dirección IP del negocio de la instancia para la que se genera la alarma) > **Customize** > **Presto Garbage Collection Time**. Haga clic en **OK** para ver la hora de GC.
4. Compruebe si el tiempo de GC del proceso de Coordinator es superior a 5 segundos.
   - En caso afirmativo, vaya a **Paso 1.5**.
   - Si no, vaya a **Paso 2**.
5. Seleccione **Components** > **Presto** > **Service Configuration**, y cambie **Basic** a **All**. Elija **Presto** > **Coordinator**. Aumente el valor de **-Xmx** en el parámetro **JAVA_OPTS** según los requisitos del sitio.
6. Verifique si la alarma se ha borrado.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 2**.

Paso 2 Recopile información de fallas.

1. En MRS Manager, seleccione **System** > **Export Log**.
2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Referencia

Ninguna

8.5.108 ALM-44006 El tiempo de GC de proceso de Presto Worker excede el umbral (Para MRS 2.*x* o anterior)

Descripción

El sistema recoge el tiempo de GC del proceso de Presto Worker cada 30 segundos. Esta alarma se genera cuando el tiempo de GC excede el umbral (excede 5 segundos durante tres veces consecutivas). Puede cambiar el umbral seleccionando **System** > **Configure Alarm Threshold** > **Service** > **Presto** > **Worker** > **Presto Garbage Collection Time** > **Garbage**

Collection Time of the Worker Process en MRS Manager. Esta alarma se borra cuando el tiempo de GC del proceso del trabajador es más corto que o igual al umbral.

Atributo

ID de alarma	Gravedad de alarma	Borrar automáticamente
44006	Grave	Sí

Parámetro

Parámetro	Descripción
ServiceName	Servicio para el que se genera la alarma.
RoleName	Rol para el que se genera la alarma.
HostName	Host para el que se genera la alarma.

Impacto en el sistema

Si el tiempo de GC del proceso de Worker es demasiado largo, el rendimiento de ejecución del proceso de Worker se verá afectado y el proceso de Worker incluso no estará disponible.

Causas posibles

La memoria de pila del proceso de Worker se usa en exceso o se asigna de forma inadecuada, lo que provoca la ocurrencia frecuente del proceso de GC.

Procedimiento

Paso 1 Comprueba la hora del GC.

1. Vaya a la página de detalles del clúster y elija **Alarms**.
2. Seleccione la alarma cuyo **Alarm ID** sea **44006**. A continuación, compruebe la dirección IP y el nombre del rol de la instancia de **Location**.
3. Elija **Components** > **Presto** > **Instances** > **Worker** (dirección IP del negocio de la instancia para la que se genera la alarma) > **Customize** > **Presto Garbage Collection Time**. Haga clic en **OK** para ver la hora de GC.
4. Compruebe si el tiempo de GC del proceso de Worker es superior a 5 segundos.
   - En caso afirmativo, vaya a **Paso 1.5**.
   - Si no, vaya a **Paso 2**.
5. Elija **Components** > **Presto** > **Service Configuration**, y cambie **Basic** a **All**, y elija **Presto** > **Worker** Aumente el valor de **-Xmx** (memoria heap máxima) en el parámetro **JAVA_OPTS** en función de los requisitos del sitio.
6. Verifique si la alarma se ha borrado.
   - En caso afirmativo, no es necesario hacer nada más.

– Si no, vaya a **Paso 2**.

Paso 2 Recopilar información de fallas.

1. En MRS Manager, seleccione **System** > **Export Log**.
2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Referencia

Ninguna

8.5.109 ALM-45325 Servicio Presto no disponible (Para MRS 2.*x* o anterior)

Descripción

El sistema comprueba el estado del servicio Presto cada 60 segundos. Esta alarma se genera cuando el sistema detecta que Presto no está disponible.

Esta alarma se borra cuando el servicio Presto se recupera.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
45325	Crítica	Sí

Parámetros

Nombre	Significado
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

Presto no puede ejecutar consultas SQL.

Causas posibles

- El proceso de Coordinator o worker de Presto es defectuoso.
- Se interrumpe la comunicación de red entre las instancias del Presto coordinator y del worker.

Procedimiento

Paso 1 **Comprobar el estado de los procesos de coordinator y worker.**

1. Inicie sesión en FusionInsight Manager y elija **Cluster** > **Services** > **Presto**. En la página que se muestra, haga clic en la pestaña **Instance**. En la lista de instancias de Presto, compruebe si el estado de todas las instancias de coordinator o de worker es **Unknown**.
   - En caso afirmativo, vaya a **2**.
   - Si no, vaya a **1**.
2. En la parte superior de la lista de instancias de Presto, elija **More** > **Restart Service** para reiniciar los procesos de coordinator y worker.
3. En la lista de alarmas, compruebe si ALM-45325 Servicio Presto no disponible está desactivado.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **1** en **Paso 2**.

Paso 2 Recopile información de fallas.

1. En FusionInsight Manager, seleccione **O&M**. En el panel de navegación de la izquierda, elija **Log** > **Download**.
2. Seleccione **Presto** para **Service**.
3. Haga clic en  en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.
4. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

8.6 Gestión de objeto

8.6.1 Gestionar objetos

El MRS contiene diferentes tipos de objetos básicos como se describe en **Tabla 8-16**.

Tabla 8-16 Descripción del objeto básico de MRS

Objeto	Descripción	Ejemplo
Servicio	Conjunto de funciones que puede completar un negocio específico.	Servicio de KrbServer y servicio de LdapServer
Instancia del servicio	Ejemplo específico de un servicio, generalmente llamado servicio.	Servicio de KrbServer

Objeto	Descripción	Ejemplo
Rol de servicio	Entidad de función que forma un servicio completo, generalmente llamado rol.	KrbServer está compuesto por el rol KerberosAdmin y el rol KerberosServer.
Instancia de rol	Ejemplo específico de un rol de servicio que se ejecuta en un host.	KerberosAdmin que se ejecuta en Host2 y KerberosServer que se ejecuta en Host3
Host	Un ECS que ejecuta el sistema operativo de Linux.	Host1 a Host5
Rack	Entidad física que contiene varios hosts que se conectan al mismo switch.	Rack1 contiene Host1 a Host5.
Clúster	Entidad lógica que consta de varios hosts y proporciona varios servicios.	Nombres de clúster **Cluster1** consta de cinco hosts (de Host1 a Host5) y proporciona servicios como KrbServer y LdapServer.

8.6.2 Consulta de configuraciones

En MRS Manager, los usuarios pueden ver las configuraciones de los servicios (incluidos los roles) y las instancias de rol.

Procedimiento

- Consultar configuraciones de servicio.
  a. En la página MRS Manager, haga clic en **Services**.
  b. Seleccione el servicio de destino en la lista de servicios.
  c. Haga clic en **Service Configuration**.
  d. Ajusta **Type** a **All**. Todos los parámetros de configuración del servicio se muestran en el árbol de navegación. Los nodos raíz de arriba hacia abajo en el árbol de navegación representan los nombres de servicio y de rol.
  e. En el árbol de navegación, seleccione un parámetro especificado y cambie su valor. También puede introducir el nombre del parámetro en el cuadro **Search** para buscar el parámetro y ver el resultado.

     Los parámetros bajo los nodos de servicio y los nodos de rol son parámetros de configuración de servicio y parámetros de configuración de rol respectivamente.
  f. En el parámetro **Non-default**, seleccione **Non-default**. Se mostrarán los parámetros cuyos valores no son valores predeterminados.
- Consultar configuraciones de instancia de rol.
  a. En la página MRS Manager, haga clic en **Services**.
  b. Seleccione el servicio de destino en la lista de servicios.
  c. Haga clic en la pestaña **Instances**.
  d. Haga clic en la instancia de rol de destino en la lista de instancias de rol.

e. Haga clic en **Instance Configuration**.

f. Ajusta **Type** a **All**. Se muestra el árbol de navegación de todos los parámetros de configuración de la instancia de rol.

g. En el árbol de navegación, seleccione un parámetro especificado y cambie su valor. También puede introducir el nombre del parámetro en el cuadro **Search** para buscar el parámetro y ver el resultado.

h. En el parámetro **Non-default**, seleccione **Non-default**. Se mostrarán los parámetros cuyos valores no son valores predeterminados.

8.6.3 Gestión de servicios

Puede realizar las siguientes operaciones en MRS Manager:

- Iniciar el servicio en el estado **Stopped**, **Stop Failed** o **Start Failed** para usar el servicio.
- Detener los servicios o detener los servicios anormales.
- Reiniciar servicios anormales o configurar servicios caducados para restaurar o habilitar los servicios.

Procedimiento

Paso 1 En la página MRS Manager, haga clic en **Services**.

Paso 2 Busque la fila que contiene el servicio de destino, **Start**, **Stop** o **Restart** para iniciar, detener o reiniciar el servicio.

Los servicios están interrelacionados. Si se inicia, se detiene y se reinicia un servicio, los servicios que dependen de él se verán afectados.

Los servicios se verán afectados de las siguientes maneras:

- Si se va a iniciar un servicio, los servicios de capa inferior que dependen de él deben iniciarse primero.
- Si se detiene un servicio, los servicios de capa superior que dependen de él no estarán disponibles.
- Si se reinicia un servicio, los servicios de capa superior en ejecución que dependen de él deben reiniciarse.

----Fin

8.6.4 Configuración de parámetros de servicio

En MRS Manager, puede ver y modificar las configuraciones de servicio predeterminadas según los requisitos del sitio y exportar o importar las configuraciones.

Impacto en el sistema

- Debe descargar y actualizar los archivos de configuración del cliente después de configurar las propiedades de servicio HBase, HDFS, Hive, Spark, Yarn y MapReduce.
- Los parámetros de DBService no se pueden modificar cuando solo existe una instancia de rol DBService en el clúster.

Procedimiento

- Modificar un servicio.
  a. Haga clic en **Services**.
  b. Seleccione el servicio de destino en la lista de servicios.
  c. Haga clic en **Service Configuration**.
  d. Ajusta **Type** a **All**. Todos los parámetros de configuración del servicio se muestran en el árbol de navegación. Los nodos raíz de arriba hacia abajo en el árbol de navegación representan los nombres de servicio y de rol.
  e. En el árbol de navegación, seleccione un parámetro especificado y cambie su valor. También puede introducir el nombre del parámetro en el cuadro **Search** para buscar el parámetro y ver el resultado.

     Para cancelar el cambio a un valor de parámetro, haga clic en  .

     NOTA

     También puede utilizar grupos de host para cambiar las configuraciones de instancia de rol en lotes. Seleccione un nombre de rol en la lista desplegable **Role** y elija **< Select Host >** en la lista desplegable **Host**. Escriba un nombre en el cuadro de texto **Host Group Name**, seleccione los hosts que se van a modificar en la lista **Host** y agréguelos al área **Selected hosts** y haga clic en **OK**. El grupo de host agregado se puede seleccionar de **Host** y solo es válido en la página actual. No se puede guardar la página después de actualizarla.
  f. Haga clic en **Save Configuration** y seleccione **Restart the affected services or instances**. Haga clic en **OK** para reiniciar los servicios.

     Después de que **Operation successful.** se muestra, haga clic en **Finish**. El servicio se inicia correctamente.

     NOTA

     Para actualizar la configuración de cola del servicio Yarn sin reiniciar el servicio, elija **More** > **Refresh Queue** para actualizar la cola para que la configuración surta efecto.
- Exportar parámetros de configuración del servicio.
  a. Haga clic en **Services**.
  b. Seleccione un servicio.
  c. Haga clic en **Service Configuration**.
  d. Haga clic en **Export Service Configuration**. Seleccione una ruta para guardar los archivos de configuración.
- Importar parámetros de configuración del servicio.
  a. Haga clic en **Services**.
  b. Seleccione un servicio.
  c. Haga clic en **Service Configuration**.
  d. Haga clic en **Import Service Configuration**.
  e. Seleccione el archivo de configuración de destino.
  f. Haga clic en **Save Configuration** y seleccione **Restart the affected services or instances**. Haga clic en **OK**.

     Después de que **Operation successful.** se muestra, haga clic en **Finish**. El servicio se inicia correctamente.

8.6.5 Configuración de parámetros de servicio personalizados

Cada componente de MRS soporta todos los parámetros de código abierto. Puede modificar algunos parámetros para escenarios de aplicación clave en MRS Manager. Algunos clientes de componentes pueden no incluir todos los parámetros con características de código abierto. Para los parámetros de componentes que no se pueden modificar directamente en Manager, los usuarios pueden agregar nuevos parámetros para los componentes mediante la función de personalización de configuración en Manager. Los parámetros recién agregados se guardan en los archivos de configuración de componentes y entran en vigor después del reinicio.

Impacto en el sistema

- Después de configurar los atributos de servicio, es necesario reiniciar el servicio y no se puede acceder a él.
- Debe descargar y actualizar los archivos de configuración del cliente después de configurar las propiedades de servicio HBase, HDFS, Hive, Spark, Yarn y MapReduce.

Prerrequisitos

Ha comprendido los significados de los parámetros a agregar, los archivos de configuración que han surtido efecto y el impacto en los componentes.

Procedimiento

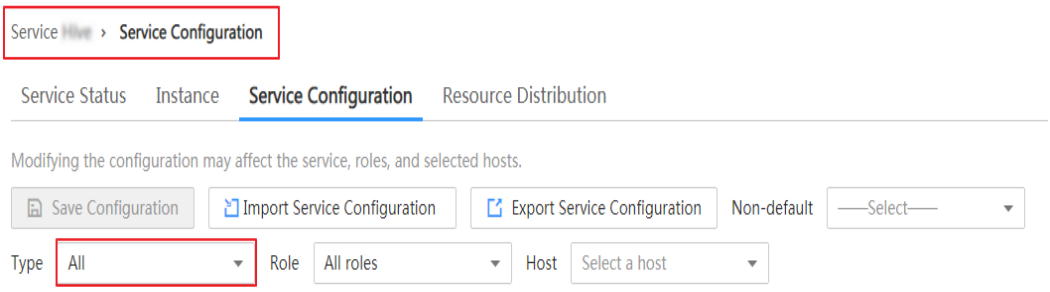
Paso 1 En MRS Manager, haga clic en **Services**.

Paso 2 Seleccione el servicio de destino en la lista de servicios.

Paso 3 Haga clic en **Service Configuration**.

Paso 4 Ajuste **Type** a **All**.

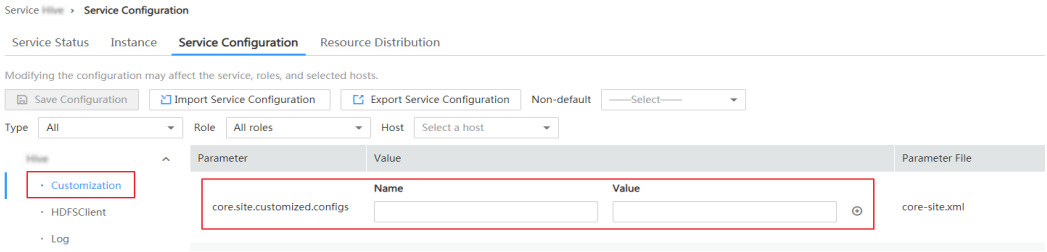
Figura 8-3 Configuración del servicio



Paso 5 En el árbol de navegación, seleccione **Customization**. Los parámetros personalizados del componente actual se muestran en Manager.

Los archivos de configuración que guardan los parámetros personalizados recién agregados se muestran en la columna **Parameter File**. Diferentes archivos de configuración pueden tener los mismos parámetros de código abierto. Después de que los parámetros en diferentes archivos se establecen en valores diferentes, si la configuración tiene efecto depende de la secuencia de carga de los archivos de configuración por componentes. Puede personalizar los parámetros para los servicios y roles según sea necesario. No se admite la adición de parámetros personalizados para una instancia de rol única.

Figura 8-4 Configuraciones de personalización



Paso 6 En función de los archivos de configuración y las funciones de parámetros, busque la fila donde reside un parámetro especificado, introduzca el nombre del parámetro admitido por el componente en la columna **Name** e introduzca el valor del parámetro en la columna **Value**.

- Puede hacer clic en  o  para agregar o eliminar un parámetro definido por el usuario. Puede eliminar un parámetro personalizado sólo después de hacer clic en  por primera vez.
- Si desea cancelar la modificación de un valor de parámetro, haga clic en  para restaurarlo.

Paso 7 Haga clic en **Save Configuration** y seleccione **Restart the affected services or instances**. Haga clic en **OK** para reiniciar los servicios.

Después de que **Operation successful.** se muestra, haga clic en **Finish**. El servicio se inicia correctamente.

----Fin

Ejemplo de tarea

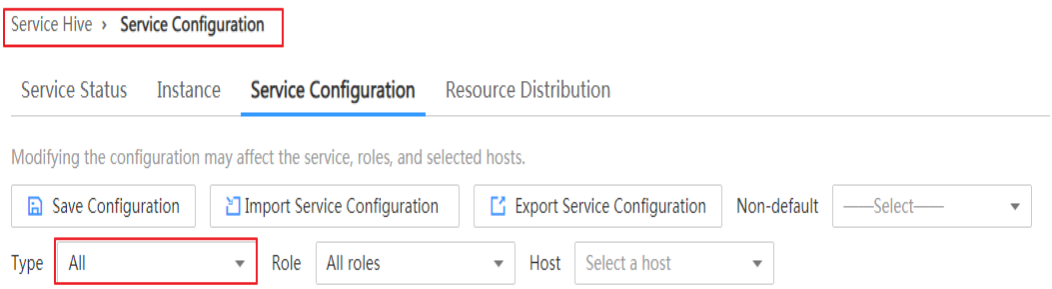
Configuración de parámetros de Hive personalizados

Hive depende de HDFS. De forma predeterminada, Hive accede al cliente de HDFS. Los parámetros de configuración que tienen efecto son controlados por HDFS de una manera unificada. Por ejemplo, el parámetro HDFS **ipc.client.rpc.timeout** afecta al período de tiempo de espera de RPC para que todos los clientes se conecten al servidor HDFS. Si necesita modificar el período de tiempo de espera para que Hive se conecte a HDFS, puede utilizar la función de personalización de configuración. Después de agregar este parámetro al archivo **core-site.xml** de Hive, este parámetro puede ser identificado por el servicio Hive y su configuración sobrescribe la configuración del parámetro en HDFS.

Paso 1 En MRS Manager, seleccione **Services** >**Hive** >**Service Configuration**.

Paso 2 Ajuste **Type** a **All**.

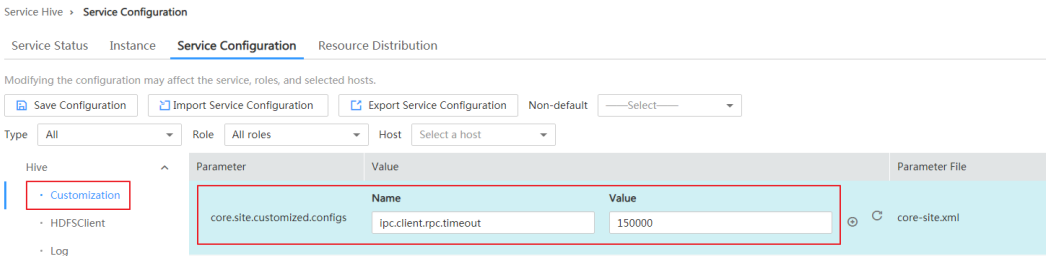
Figura 8-5 Configuración del servicio Hive



Paso 3 En el árbol de navegación de la izquierda, seleccione **Customization** para el servicio Hive. El sistema muestra los parámetros de servicio personalizados compatibles con Hive.

Paso 4 En **core-site.xml**, busque la fila que contiene el parámetro **core.site.customized.configs**, escriba **ipc.client.rpc.timeout** en la columna **Name** e introduzca un nuevo valor en la columna **Value**, por ejemplo, **150000**. La unidad es milisegundo.

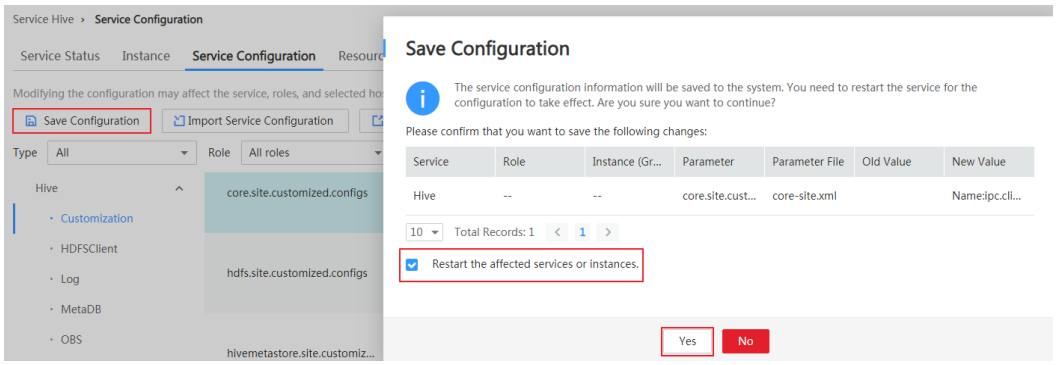
Figura 8-6 Configuraciones de personalización de Hive



Paso 5 Haga clic en **Save Configuration** y seleccione **Restart the affected services or instances**. Haga clic en **OK** para reiniciar el servicio.

Después de que **Operation successful.** se muestra, haga clic en **Finish**. El servicio se inicia correctamente.

Figura 8-7 Guardar configuraciones de Hive



----Fin

8.6.6 Sincronización de configuraciones de servicio

Escenario

Si **Configuration Status** de un servicio es **Expired** o **Failed**, sincronice las configuraciones del clúster o servicio para restaurar su estado de configuración. Si todos los servicios del clúster están en estado **Failed**, sincronice la configuración del clúster con la configuración en segundo plano.

Impacto en el sistema

Después de sincronizar las configuraciones de servicio, debe reiniciar los servicios cuyas configuraciones han caducado. Estos servicios no están disponibles durante el reinicio.

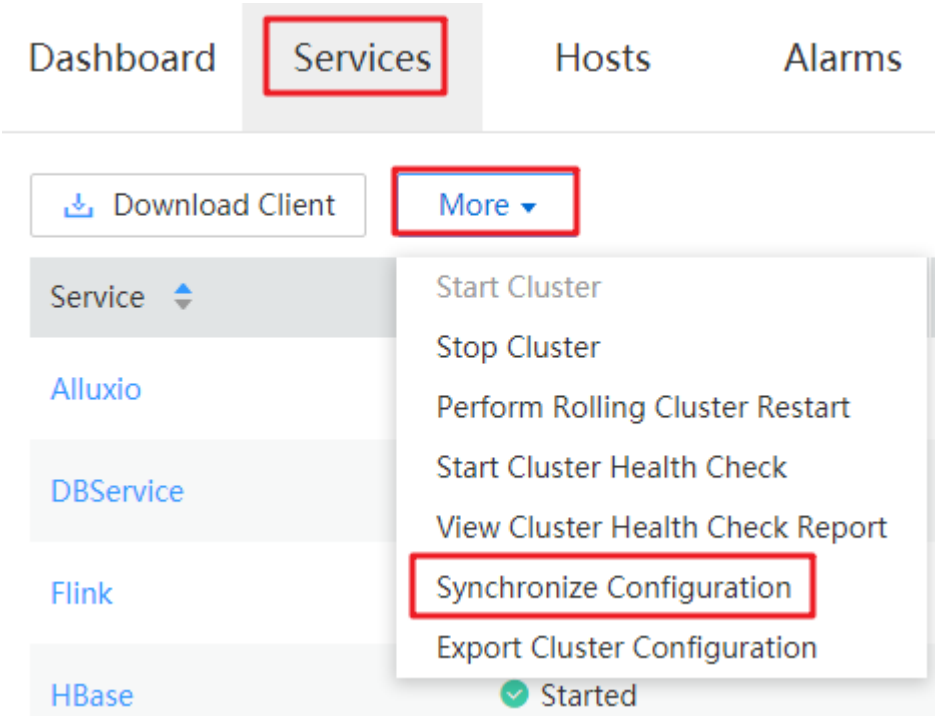
Procedimiento

Paso 1 En la página MRS Manager, haga clic en **Services**.

Paso 2 Seleccione el servicio de destino en la lista de servicios.

Paso 3 En la parte superior de la información del estado del servicio y de la métrica, seleccione **More** > **Synchronize Configuration**.

Figura 8-8 Configuraciones de sincronización



Paso 4 En el cuadro de diálogo que se muestra, escriba la contraseña como se le solicite y haga clic en **OK**. Una vez verificada su identidad, seleccione **Restart the service or instance whose configuration has expired**. y haga clic en **OK** para reiniciar el servicio cuya configuración ha caducado.

Cuando se muestre **Operation successful**, haga clic en **Finish**. El servicio se inicia correctamente.

----Fin

8.6.7 Gestión de instancias de rol

Escenario

Puede iniciar una instancia de rol que se encuentre en el estado **Stopped**, **Failed to stop** o **Failed to start**, detener una instancia de rol no utilizada o anormal o reiniciar una instancia de rol anormal para recuperar sus funciones.

Procedimiento

Paso 1 En la página MRS Manager, haga clic en **Services**.

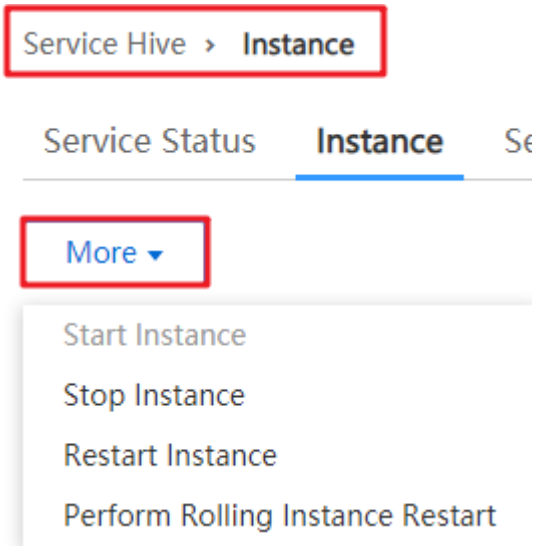
Paso 2 Seleccione el servicio de destino en la lista de servicios.

Paso 3 Haga clic en la pestaña **Instances**.

Paso 4 Seleccione la casilla de verificación situada a la izquierda de la instancia de rol de destino.

Paso 5 Elija **More** > **Start Instance**, **Stop Instance** o **Restart Instance** según corresponda.

Figura 8-9 Operaciones de instancias



----Fin

8.6.8 Configuración de parámetros de instancia de rol

Escenario

Puede ver y modificar las configuraciones de instancias de rol predeterminadas en MRS Manager según los requisitos del sitio. Las configuraciones se pueden importar y exportar.

Impacto en el sistema

Debe descargar y actualizar los archivos de configuración del cliente después de configurar las propiedades de servicio HBase, HDFS, Hive, Spark, Yarn y MapReduce.

Procedimiento

- Modificación de configuraciones de instancia de rol
  a. Haga clic en **Services**.
  b. Seleccione el servicio de destino en la lista de servicios.
  c. Haga clic en la pestaña **Instances**.
  d. Haga clic en la instancia de rol de destino en la lista de instancias de rol.
  e. Haga clic en **Instance Configuration**.
  f. Ajusta **Type** a **All**. Se muestra el árbol de navegación de todos los parámetros de configuración de la instancia de rol.

g. En el árbol de navegación, seleccione un parámetro especificado y cambie su valor. También puede introducir el nombre del parámetro en el cuadro **Search** para buscar el parámetro y ver el resultado.

   Si desea cancelar la modificación de un valor de parámetro, haga clic en  para restaurarlo.

h. Haga clic en **Save Configuration**, seleccione **Restart the role instance**, y haga clic en **OK**.

   Después de que **Operation successful.** se muestra, haga clic en **Finish**. La instancia de rol se inicia correctamente.

- Exportación de parámetros de configuración de una instancia de rol

  a. Haga clic en **Services**.

  b. Seleccione un servicio.

  c. Seleccione una instancia de rol o haga clic en la pestaña **Instances**.

  d. Seleccione una instancia de rol en un host especificado.

  e. Haga clic en **Instance Configuration**.

  f. Haga clic en **Export Instance Configuration** para exportar los datos de configuración de una instancia de rol especificada y elija una ruta para guardar el archivo de configuración.

- Importar datos de configuración de una instancia de rol.

  a. Haga clic en **Services**.

  b. Seleccione un servicio.

  c. Seleccione una instancia de rol o haga clic en la pestaña **Instances**.

  d. Seleccione una instancia de rol en un host especificado.

  e. Haga clic en **Instance Configuration**.

  f. Haga clic en **Import Instance Configuration** para importar los datos de configuración de la instancia de rol especificada.

  g. Haga clic en **Save Configuration** y seleccione **Restart the role instance**. Haga clic en **OK**.

     Después de que **Operation successful.** se muestra, haga clic en **Finish**. La instancia de rol se inicia correctamente.

8.6.9 Sincronización de configuración de instancia de rol

Escenario

Cuando **Configuration Status** de una instancia de rol es **Expired** o **Failed**, puede sincronizar los datos de configuración de la instancia de rol con la configuración en segundo plano.

Impacto en el sistema

Después de sincronizar una configuración de instancia de rol, debe reiniciar la instancia de rol cuya configuración ha caducado. La instancia de rol no está disponible durante el reinicio.

Procedimiento

Paso 1 En MRS Manager, haga clic en **Services** y seleccione un nombre de servicio.

Paso 2 Haga clic en la pestaña **Instances**.

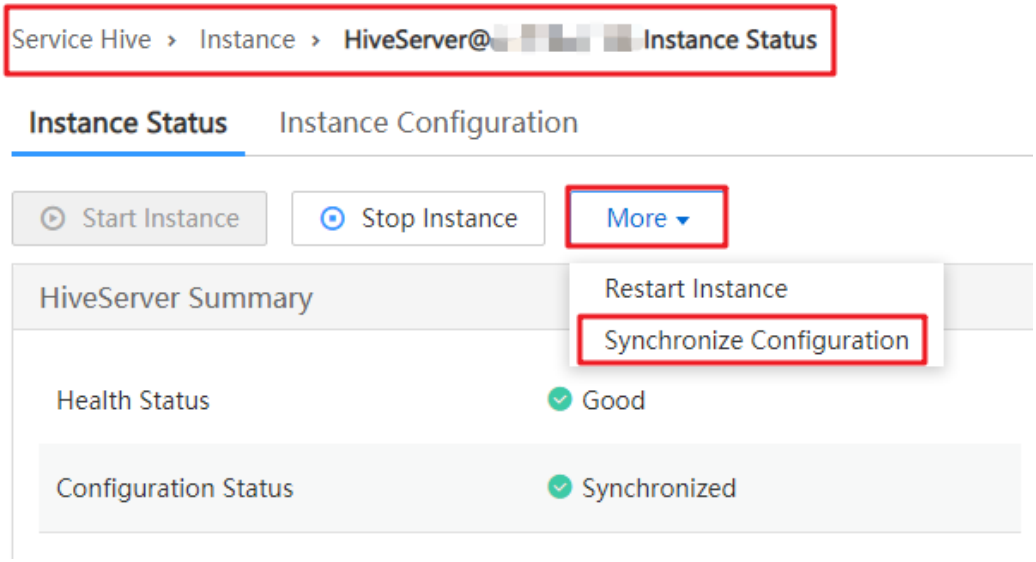
Paso 3 Haga clic en la instancia de rol de destino en la lista de instancias de rol.

Paso 4 Elija **More** > **Synchronize Configuration** encima del estado de la instancia de rol y la información del indicador.

Paso 5 En el cuadro de diálogo mostrado, seleccione **Restart services and instances whose configuration have expired** y haga clic en **OK** para reiniciar la instancia de rol.

Una vez que se muestre **Operation successful**, haga clic en **Finish**. La instancia de rol se inicia correctamente.

Figura 8-10 Sincronización de configuraciones de instancia de rol



----Fin

8.6.10 Desmantelar y volver a poner en servicio una instancia de rol

Escenario

Si un nodo Core o Task es defectuoso, el estado del clúster puede mostrarse como **Abnormal**. En un clúster de MRS, los datos se pueden almacenar en diferentes nodos de Core. Los usuarios pueden retirar la instancia de rol especificada en MRS Manager para impedir que la instancia de rol proporcione servicios. Después de la rectificación de errores, puede volver a poner en marcha la instancia de rol.

Las siguientes instancias de rol se pueden retirar y volver a poner en servicio.

- Instancia de rol de DataNode en HDFS
- Instancia de rol de NodeManager en Yarn

- Instancia de rol de RegionServer en HBase
- Instancia de rol de broker en Kafka

Restricciones:

- Si el número del DataNodes es menor o igual que el de las copias de HDFS, no se puede realizar el desmantelamiento. Si el número de copias de HDFS es tres y el número de DataNodes es inferior a cuatro en el sistema, no se puede realizar el desmantelamiento. En este caso, se informará de un error y el desmantelamiento se detendrá 30 minutos después de que se realice el intento de desmantelamiento en Manager.
- Si el número de instancias de Kafka Broker es menor o igual que el de las copias, no se puede realizar el desmantelamiento. Por ejemplo, si el número de copias de Kafka es dos y el número de nodos es inferior a tres en el sistema, no se puede realizar el desmantelamiento. El desmantelamiento de instancias fallará en Manager y se cerrará.
- Si una instancia de rol está fuera de servicio, debe volver a poner en servicio la instancia para iniciarla antes de volver a usarla.

Procedimiento

Paso 1 En la página MRS Manager, haga clic en **Services**.

Paso 2 Haga clic en un servicio en la lista de servicios.

Paso 3 Haga clic en la pestaña **Instances**.

Paso 4 Seleccione una instancia.

Paso 5 Elija **More** > **Decommission** o **Recommission** para realizar la operación correspondiente.

NOTA

Durante la retirada de la instancia, si el servicio correspondiente a la instancia se reinicia en el clúster mediante otro navegador, MRS Manager muestra un mensaje que indica que la retirada de la instancia se ha detenido, pero el **Operating Status** de la instancia se muestra como **Started**. En este caso, la instancia ha sido desmantelada en segundo plano. Para sincronizar el estado operativo, debe volver a desmantelar la instancia.

----Fin

8.6.11 Gestión de un host

Escenario

Cuando un host es anormal o defectuoso, debe detener todos los roles del host en MRS Manager para comprobar el host. Una vez que se corrija el error del host, inicie todos los roles que se ejecuten en el host para recuperar los servicios del host.

Procedimiento

Paso 1 Haga clic en **Hosts**.

Paso 2 Seleccione el cuadro de verificación del host de destino.

Paso 3 Elija **More** > **Start All Roles** o **Stop All Roles** en consecuencia.

----Fin

8.6.12 Aislamiento de un host

Escenario

Si se detecta que un host es anormal o defectuoso, que afecta al rendimiento del clúster o impide que se proporcionen servicios, puede excluir temporalmente ese host de los nodos disponibles en el clúster. De esta manera, el cliente puede acceder a otros nodos disponibles. En los escenarios en los que se van a instalar parches en un clúster, también puede excluir un nodo especificado de la instalación de parches.

Los usuarios pueden aislar un host manualmente en MRS Manager según los requisitos de servicio reales o el plan O&M. Solo se pueden aislar nodos que no sean de gestión.

Impacto en el sistema

- Después de aislar un host, se detendrán todas las instancias de rol en el host. No puede iniciar, detener ni configurar el host ni ninguna instancia del host.
- Después de aislar un host, no se pueden recopilar ni mostrar estadísticas sobre el estado de monitoreo y los datos indicadores del hardware y las instancias del host.

Procedimiento

Paso 1 En MRS Manager, haga clic en **Hosts**.

Paso 2 Seleccione la casilla de verificación del host que se va a aislar.

Paso 3 Elija **More** > **Isolate Host**,

Paso 4 y haga clic en **OK** en el cuadro de diálogo mostrado.

Después de que **Operation successful.** se muestra, haga clic en **Finish**. El host se aísla correctamente y el valor de **Operating Status** se convierte en **Isolated**.

NOTA

Para hosts aislados, puede cancelar el aislamiento y agregarlos de nuevo al clúster. Para obtener más información, consulte **Cancelación del aislamiento del host**.

----Fin

8.6.13 Cancelación del aislamiento del host

Escenario

Después de que se haya manejado la excepción o la falla de un host, debe cancelar el aislamiento del host para su uso correcto.

Los usuarios pueden cancelar el aislamiento de un host en MRS Manager.

Prerrequisitos

- El host se encuentra en el estado **Isolated**.
- Se ha rectificado la excepción o falla del host.

Procedimiento

Paso 1 En MRS Manager, haga clic en **Hosts**.

Paso 2 Seleccione la casilla de verificación del host que se va a desaislar.

Paso 3 Elija **More** > **Cancel Host Isolation**,

Paso 4 y haga clic en **OK** en el cuadro de diálogo mostrado.

Después de que **Operation successful.** se muestra, haga clic en **Finish**. El host se desaisla con éxito, y el valor de **Operating Status** se convierte en **Normal**.

Paso 5 Haga clic en el nombre del host desaislado para mostrar su estado y haga clic en **Start All Roles**.

----Fin

8.6.14 Inicio o detención de un clúster

Escenario

Un clúster es una colección de componentes de servicio. Puede iniciar o detener todos los servicios de un clúster.

Procedimiento

Paso 1 En la página MRS Manager, haga clic en **Services**.

Paso 2 En la parte superior de la lista de servicios, elija **More** > **Start Cluster** o **Stop Cluster** en consecuencia.

----Fin

8.6.15 Sincronización de configuraciones de clúster

Escenario

Si **Configuration Status** de todos los servicios o de algunos servicios es **Expired** o **Failed**, sincronice la configuración del clúster o del servicio para restaurar su estado de configuración.

- Si todos los servicios del clúster están en estado **Failed**, sincronice la configuración del clúster con la configuración en segundo plano.
- Si todos los servicios del clúster están en estado **Failed**, sincronice la configuración del servicio con la configuración en segundo plano.

Impacto en el sistema

Después de sincronizar las configuraciones de clúster, debe reiniciar los servicios cuyas configuraciones han caducado. Estos servicios no están disponibles durante el reinicio.

Procedimiento

Paso 1 En la página MRS Manager, haga clic en **Services**.

Paso 2 En la parte superior de la lista de servicios, elija **More** > **Synchronize Configuration**.

Paso 3 En el cuadro de diálogo que se muestra, introduzca la contraseña del usuario de inicio de sesión actual para la verificación de identidad. Una vez completada la verificación, seleccione **Restart the service or instance whose configuration has expired**. y haga clic en **OK** para reiniciar el servicio cuya configuración ha caducado.

Cuando **Operation successful.** se muestra, haga clic en **Finish**. El servicio se inicia correctamente.

----Fin

8.6.16 Exportación de datos de configuración de un clúster

Escenario

Puede exportar todos los datos de configuración de un clúster en MRS Manager para cumplir con los requisitos del sitio. Los datos de configuración exportados se utilizan para actualizar rápidamente la configuración del servicio.

Procedimiento

Paso 1 En la página MRS Manager, haga clic en **Services**.

Paso 2 Elija **More** > **Export Cluster Configuration**.

El archivo exportado se utiliza para actualizar las configuraciones de servicio. Para obtener más información, consulte **Importar parámetros de configuración del servicio** en **Configuración de parámetros de servicio**.

----Fin

8.7 Gestión de registros

8.7.1 Acerca de los registros

Descripción del registro

Los registros de clúster de MRS se almacenan en el directorio **/var/log/Bigdata**. En la siguiente tabla se enumeran los tipos de registro.

Tabla 8-17 Tipos de registro

Tipo	Descripción
Registro de instalación	Los registros de instalación registran información sobre FusionInsight Manager, el clúster y la instalación de servicios para ayudar a los usuarios a localizar errores de instalación.

Tipo	Descripción
Registros de ejecución	Los registros de ejecución registran la información de la pista de ejecución, la información de depuración, los cambios de estado, los problemas potenciales y la información de error generada durante la ejecución de los servicios.
Registros de auditoría	Los registros de auditoría registran información sobre las actividades de los usuarios y las instrucciones de operación, que se pueden utilizar para localizar las causas de errores en los eventos de seguridad y determinar quiénes son los responsables de estos errores.

En la siguiente tabla se enumeran los directorios de registro MRS.

Tabla 8-18 Directorios de registro

Directorio de archivo	Contenido de registro
/var/log/Bigdata/audit	Registro de auditoría de componentes.
/var/log/Bigdata/controller	Registro de script de recolección de registro. Registro de proceso de controller. Registro de monitoreo de controller.
/var/log/Bigdata/dbservice	Registro de DBService.
/var/log/Bigdata/flume	Registro de Flume.
/var/log/Bigdata/hbase	Registro de HBase.
/var/log/Bigdata/hdfs	Registro de HDFS.
/var/log/Bigdata/hive	Registro de Hive.
/var/log/Bigdata/httpd	Registro de HTTPD.
/var/log/Bigdata/hue	Registro de Hue.
/var/log/Bigdata/kerberos	Registro de Kerberos.
/var/log/Bigdata/ldapclient	Registro de cliente de LDAP.
/var/log/Bigdata/ldapserver	Registro del servidor de LDAP.
/var/log/Bigdata/loader	Registro de Loader.
/var/log/Bigdata/logman	Registro de gestión de registro de scripts de Logman.
/var/log/Bigdata/mapreduce	Registro de MapReduce.
/var/log/Bigdata/nodeagent	Registro de NodeAgent.
/var/log/Bigdata/okerberos	Registro de Kerberos de OMS.
/var/log/Bigdata/oldapserver	Registro de LDAP de OMS.

Directorio de archivo	Contenido de registro
/var/log/Bigdata/omm	**oms**: registro de procesamiento de eventos complejos, registro de servicio de alarma, registro de HA, registro de gestión de autenticación y autorización y registro de ejecución de servicio de monitoreo del servidor omm. **oma**: registro de instalación y registro de ejecución del agente omm. **core**: registro de volcado generado cuando el agente omm y el proceso HA están suspendidos.
/var/log/Bigdata/spark	Registro de Spark.
/var/log/Bigdata/sudo	Registro generado cuando el comando **sudo** es ejecutado por el usuario **omm**.
/var/log/Bigdata/timestamp	Registro de gestión de sincronización de tiempo.
/var/log/Bigdata/tomcat	Registro de Tomcat.
/var/log/Bigdata/yarn	Registro de Yarn.
/var/log/Bigdata/zookeeper	Registro de ZooKeeper.
/var/log/Bigdata/kafka	Registro de Kafka.
/var/log/Bigdata/storm	Registro de Storm.
/var/log/Bigdata/patch	Registro de parches.

Registros de ejecución

Tabla 8-19 describe la información de ejecución registrada en los registros de ejecución.

Tabla 8-19 Información de ejecución

Registro de ejecución	Descripción
Registro de preparación de la instalación	Registra información sobre los preparativos para la instalación, como la información de operación de detección, configuración y retroalimentación.
Registro de inicio de proceso	Registra información sobre los comandos ejecutados durante el inicio del proceso.
Registro de excepciones de inicio de proceso	Registra información sobre excepciones durante el inicio del proceso, como errores de servicio dependientes y recursos insuficientes.
Registro de ejecución del proceso	Registra información sobre el proceso que ejecuta información de pista e información de depuración, como entradas y salidas de funciones, así como mensajes de interfaz de módulo cruzado.

Registro de ejecución	Descripción
Registro de excepción de ejecución de proceso	Registra los errores que causan errores de ejecución del proceso, por ejemplo, los objetos de entrada vacíos o errores de codificación o decodificación.
Registro de entorno en ejecución del proceso	Registra información sobre el entorno en ejecución del proceso, como el estado de los recursos y las variables de entorno.
Registros de script	Registra información sobre el proceso de ejecución del script.
Registro de recuperación de recursos	Registra información sobre el proceso de recuperación de recursos.
Registros de borrado de desinstalación	Registra información sobre las operaciones realizadas durante la desinstalación del servicio, como la eliminación de directorios y el tiempo de ejecución

Registros de auditoría

La información de auditoría registrada en los registros de auditoría incluye la información de auditoría de FusionInsight Manager y la información de auditoría de componentes.

Tabla 8-20 Información de auditoría de FusionInsight Manager

Registro de auditoría	Tipo de operación	Operación
Registro de auditoría de Manager	Gestión de usuarios.	Creación de un usuario Modificación de un usuario Eliminación de usuarios Creación de un grupo de usuarios Modificación de un grupo de usuarios Eliminación de un grupo de usuarios Adición de un rol Modificación de un rol Eliminación de un rol Cambio de una política de contraseñas Cambio de contraseña Restablecimiento de una contraseña Inicio de sesión del usuario Cierre de sesión del usuario Desbloqueo de la pantalla Descargar la credencial de autenticación Operación no autorizada Desbloqueo de una cuenta de usuario Bloqueo de una cuenta de usuario Bloqueo de la pantalla Exportación de información de usuario Exportación de un grupo de usuarios Exportación de un rol

Registro de auditoría	Tipo de operación	Operación
	Gestión de tenant	Guardar la configuración estática Adición de un tenant Eliminación de un tenant Asociar un servicio con un tenant Eliminar un servicio de un tenant Configuración de recursos Creación de recursos Eliminación de recursos Adición de un grupo de recursos Modificación de un grupo de recursos Eliminación de un grupo de recursos Restauración de datos de tenant

Registro de auditoría	Tipo de operación	Operación
	Gestión de clúster	Iniciar un clúster Detener un clúster Guardar configuraciones Sincronización de configuraciones de clúster Personalización de los indicadores de monitoreo de clústeres Guardar umbrales de monitoreo Descargar un archivo de configuración de cliente Configuración de la API en dirección norte Configuración de la API de SNMP en dirección norte Creación de una plantilla de umbral Eliminación de una plantilla de umbral Aplicación de una plantilla de umbral Guardar datos de configuración de monitoreo de clústeres Exportación de datos de configuración Importación de datos de configuración de clúster Exportación de una plantilla de instalación Modificación de una plantilla de umbral Cancelación de la aplicación de una plantilla de umbral Enmascaramiento de alarmas Enviar una alarma Cambio de la contraseña de la base de datos de OMS Cambio de la contraseña de la base de datos de componentes

Registro de auditoría	Tipo de operación	Operación
		Iniciar la comprobación de estado de un clúster Actualización de la configuración de comprobación de estado Exportación de resultados de comprobación de estado de clúster Importación de un archivo de certificado Eliminación de informes históricos de comprobación de estado Exportación de informes históricos de comprobación de estado Personalización de indicadores de monitoreo de informes Exportación de datos de monitoreo de informes Personalización de indicadores de monitoreo para grupos de recursos estáticos Exportación de datos de monitoreo de grupo de recursos estático

Registro de auditoría	Tipo de operación	Operación
	Gestión de servicio	Iniciar un servicio Detener un servicio Sincronización de configuraciones de servicio Actualización de una cola de servicio Personalización de los indicadores de monitoreo del servicio Reinicio de un servicio Exportación de datos de monitoreo de servicios Importación de datos de configuración de servicio Iniciar la comprobación de estado de un servicio Exportación de resultados de comprobación de estado del servicio Configuración del servicio Cargar un archivo de configuración Descargar un archivo de configuración
	Gestión de instancias	Sincronización de configuraciones de instancia Puesta en marcha de una instancia Desmantelamiento de una instancia Inicio de una instancia Detención de una instancia Personalización de indicadores de monitoreo de instancias Reinicio de una instancia Exportación de datos de monitoreo de instancia Importación de datos de configuración de instancia

Registro de auditoría	Tipo de operación	Operación
	Gestión de hosts	Configuración de un rack de nodos Iniciar todos los roles Detener todos los roles Aislamiento de un host Cancelación del aislamiento del host Personalización de los indicadores de monitoreo de host Exportación de datos de monitoreo de host Iniciar la comprobación de estado de un host Exportación del resultado de la comprobación de estado de un host

Registro de auditoría	Tipo de operación	Operación
	Gestión de mantenimiento	Exportación de alarmas Rectificación de alarmas Exportación de eventos Borrar alarmas en lotes Borrar alarma a través de SNMP Adición de un destino de trap a través de SNMP Eliminación de un destino de trap a través de SNMP Comprobación de alarmas a través de SNMP Sincronización de alarmas a través de SNMP Modificación de configuraciones de volcado de auditoría Exportación de registros de auditoría Recopilación de archivos de registro Descarga de archivos de registro Carga de un archivo Eliminación de un archivo cargado Creación de una tarea de copia de respaldo Ejecución de una tarea de copia de respaldo Detención de una tarea de copia de respaldo Eliminación de una tarea de copia de respaldo Modificación de una tarea de copia de respaldo Bloqueo de una tarea de copia de respaldo Desbloqueo de una tarea de copia de respaldo Creación de una tarea de restauración

Registro de auditoría	Tipo de operación	Operación
		Ejecución de una tarea de restauración de copia de respaldo Detención de una tarea de restauración Reintentar una tarea de restauración Eliminación de una tarea de restauración

Tabla 8-21 Información de auditoría de componentes

Registro de auditoría	Tipo de operación	Operación
Registro de auditoría de DBService	Gestión de mantenimiento	Realización de operaciones de restauración de copia de respaldo
Registro de auditoría de HBase	Sentencia de lenguaje de definición de datos (DDL)	Creación de una tabla Eliminación de una tabla Modificación de una tabla Adición de una familia de columna Modificación de una familia de columna Supresión de una familia de columna Habilitación de una tabla Desactivación de una tabla Modificación de la información del usuario Cambio de contraseña Inicio de sesión del usuario

Registro de auditoría	Tipo de operación	Operación
	Sentencia de lenguaje de manipulación de datos (DML)	Poner datos (en las tablas **hbase:meta**, **_ctmeta_** y **hbase:acl**) Eliminar datos (de las tablas **hbase:meta**, **_ctmeta_** y **hbase:acl**) Comprobar y poner datos (en las tablas **hbase:meta**, **_ctmeta_** y **hbase:acl**) Comprobar y eliminar datos (de las tablas **hbase:meta**, **_ctmeta_** y **hbase:acl**)
	Control de permisos	Asignar permisos a un usuario Cancelar la asignación de permisos
Registros de auditoría de Hive	Operación de metadatos	Definir metadatos, como la creación de bases de datos y tablas Eliminar metadatos, como eliminar bases de datos y tablas Modificar metadatos, como agregar columnas y cambiar el nombre de tablas Importación y exportación de metadatos
	Mantenimiento de datos	Carga de datos en una tabla Insertar datos en una tabla
	Gestión de permisos	Creación o eliminación de roles Otorgar/Recuperar roles Concesión/Reclamación de permisos
Registro de auditoría de HDFS	Gestión de permisos	Gestión de permisos en archivos o carpetas Gestión de permisos en archivos o carpetas de información de propietario

Registro de auditoría	Tipo de operación	Operación
	Operación de archivos	Creación de una carpeta Creación de un archivo Apertura de un archivo Anexo de contenido de archivo Cambio del nombre de un archivo Eliminación de un archivo o una carpeta Configuración de la propiedad de tiempo de un archivo Establecer el número de copias de archivos Combinación de archivos Comprobación del sistema de archivos Enlaces de archivo
Registro de auditoría de MapReduce	Ejecución de aplicación	Inicio de una solicitud de Container Detener una solicitud de Container Una vez completada la solicitud de Container, el estado de la solicitud se muestra como exitosa. Una vez completada la solicitud de Container, el estado de la solicitud se muestra como fallido. Una vez completada la solicitud de Container, el estado de la solicitud se muestra como suspendida. Enviar una tarea Finalizar una tarea

Registro de auditoría	Tipo de operación	Operación
Registro de auditoría de LdapServer	Gestión de mantenimiento	Agregar un usuario del sistema operativo Agregar un grupo de usuarios Agregar un usuario al grupo de usuarios Eliminar un usuario Eliminar un grupo
Registro de auditoría de KrbServer	Gestión de mantenimiento	Cambiar la contraseña de una cuenta de Kerberos Agregar una cuenta de Kerberos Eliminar una cuenta de Kerberos Autenticación de un usuario
Registro de auditoría de Loader	Gestión de la seguridad	Inicio de sesión del usuario
	Gestión de metadatos	Consultar información del connector Consultar un framework Consultar información de step
	Gestión de conexiones de fuente de datos	Consultar una conexión de fuente de datos Adición de una conexión de fuente de datos Actualización de una conexión de fuente de datos Eliminación de una conexión de fuente de datos Activación de una conexión de fuente de datos Deshabilitación de una conexión de fuente de datos

Registro de auditoría	Tipo de operación	Operación
	Gestión de trabajo	Consultar un trabajo Creación de un trabajo Actualización de un trabajo Eliminación de un trabajo Activación de un trabajo Desactivación de un trabajo Consultar todos los registros de ejecución de un trabajo Consultar el último registro de ejecución de un trabajo Enviar un trabajo Detener un trabajo
Registro de auditoría de Hue	Iniciar servicio	Iniciar Hue
	Operación del usuario	Inicio de sesión del usuario Cierre de sesión del usuario
	Operación de tarea	Creación de un trabajo Modificación de un trabajo Eliminación de un trabajo Enviar una tarea Guardar una tarea Actualización del estado de una tarea
Registro de auditoría de ZooKeeper	Gestión de permisos	Configuración del permiso de acceso a Znode
	Operación de Znode	Creación de un Znode Eliminación de un Znode Configuración de datos de Znode
Registro de auditoría de Storm	Nimbus	Envío de una topología Detener una topología Reasignación de una topología Desactivación de una topología Activación de una topología

Registro de auditoría	Tipo de operación	Operación
	UI	Detener una topología Reasignación de una topología Desactivación de una topología Activación de una topología

Los registros de auditoría MRS se almacenan en la base de datos. Puede ver y exportar registros de auditoría en la página **Audit**.

En la siguiente tabla se enumeran los directorios para almacenar los registros de auditoría de componentes. Los archivos de registro de auditoría de algunos componentes se almacenan en **/var/log/Bigdata/audit** como HDFS, HBase, MapReduce, Hive, Hue, Yarn, Storm y ZooKeeper. Los registros de auditoría de componentes se comprimen y se copian automáticamente a **/var/log/Bigdata/audit/bk** a las 03:00 todos los días. Se conserva un máximo de 90 archivos de copia de respaldo comprimidos más recientes y no se puede cambiar el tiempo de copia de respaldo.

Los archivos de registro de auditoría de otros componentes se almacenan en el directorio de registro de componentes.

Tabla 8-22 Directorio para almacenar registros de auditoría de componentes

Componente	Directorio de registro de auditoría
DBService	/var/log/Bigdata/audit/dbservice/dbservice_audit.log
HDFS	/var/log/Bigdata/audit/hdfs/nn/hdfs-audit-namenode.log /var/log/Bigdata/audit/hdfs/dn/hdfs-audit-datanode.log /var/log/Bigdata/audit/hdfs/jn/hdfs-audit-journalnode.log /var/log/Bigdata/audit/hdfs/zkfc/hdfs-audit-zkfc.log /var/log/Bigdata/audit/hdfs/httpfs/hdfs-audit-httpfs.log /var/log/Bigdata/audit/hdfs/router/hdfs-audit-router.log
MapReduce	/var/log/Bigdata/audit/mapreduce/jobhistory/mapred-audit-jobhistory.log
Hive	/var/log/Bigdata/audit/hive/hiveserver/hive-audit.log /var/log/Bigdata/audit/hive/metastore/metastore-audit.log /var/log/Bigdata/audit/hive/webhcat/webhcat-audit.log
Loader	/var/log/Bigdata/loader/audit/default.audit
Hue	/var/log/Bigdata/audit/hue/hue-audits.log
ZooKeeper	/var/log/Bigdata/audit/zookeeper/quorumpeer/zk-audit-quorumpeer.log

Componente	Directorio de registro de auditoría
Spark	/var/log/Bigdata/audit/spark/jdbcserver/jdbcserver-audit.log /var/log/Bigdata/audit/spark/jobhistory/jobhistory-audit.log
Yarn	/var/log/Bigdata/audit/yarn/rm/yarn-audit-resourcemanager.log /var/log/Bigdata/audit/yarn/nm/yarn-audit-nodemanager.log
Storm	/var/log/Bigdata/audit/storm/nimbus/audit.log /var/log/Bigdata/audit/storm/ui/audit.log

8.7.2 Lista de registros de Manager

Descripción del registro

Log path: La ruta de almacenamiento predeterminada de los archivos de registro de Manager es **/var/log/Bigdata/***Manager component*.

- ControllerService: **/var/log/Bigdata/controller/** (instalación y registros de ejecución del sistema de mantenimiento & operación (OMS))
- Httpd: **/var/log/Bigdata/httpd** (registros de instalación y ejecución de httpd)
- Logman: **/var/log/Bigdata/logman** (registros de la herramienta de empaquetado de registros)
- NodeAgent: **/var/log/Bigdata/NodeAgent** (registros de instalación y ejecución de NodeAgent)
- okerberos: **/var/log/Bigdata/okerberos** (registros de instalación y ejecución de okerberos)
- oldapserver: **/var/log/Bigdata/oldapserver** (registros de instalación y ejecución de oldapserver)
- MetricAgent: **/var/log/Bigdata/metric_agent** (registro de ejecución de MetricAgent)
- omm: **/var/log/Bigdata/omm** (registros de instalación y ejecución de omm)
- Timestamp: **/var/log/Bigdata/timestamp** (registros de tiempo de inicio de NodeAgent)
- tomcat: **/var/log/Bigdata/tomcat** (registros de procesos de web)
- Parche: **/var/log/Bigdata/patch** (registro de instalación de parches)
- Sudo: **/var/log/Bigdata/sudo** (registro de ejecución de script de sudo)
- OS: **/var/log/***message file* (registro del sistema operativo)
- Rendimiento del sistema operativo: **/var/log/osperf** (registro de estadísticas de rendimiento del sistema operativo)
- Estadísticas de sistema operativo: **/var/log/osinfo/statistics** (registro de configuración de parámetro de sistema operativo)

Regla de archivado de registro:

La función de compresión y archivado automáticos está habilitada para los registros de Manager. De forma predeterminada, cuando el tamaño de un archivo de registro supera los 10 MB, el archivo de registro se comprime automáticamente. La regla de denominación de un

archivo de registro comprimido es la siguiente: <*Original log name*>-<*yyyy-mm-dd_hh-mm-ss*>.[*ID*].**log.zip** Se reserva un máximo de 20 últimos archivos comprimidos.

Tabla 8-23 Registros de Manager

Tipo	Nombre de archivo de registro	Descripción
Registro de ejecución de Controller	controller.log	Registro que registra la instalación de componentes, la actualización, la instalación de parches, la configuración, el monitoreo, las alarmas y las operaciones de operación rutinaria
	controller_client.log	Registro de ejecución de la API de Transferencia de Estado Representacional (REST)
	acs.log	Archivo de registro de ejecución de ACS
	acs_spnego.log	Registro de usuario de spnego en ACS
	aos.log	Regustro de ejecución de AOS
	plugin.log	Registros de complemento de AOS
	backupplugin.log	Registro que registra las operaciones de copia de respaldo y restauración
	controller_config.log	Registro de ejecución de configuración
	controller_nodesetup.log	Registro de tarea de carga de Controller
	controller_root.log	Registro del sistema del proceso de Controller
	controller_trace.log	Registro que registra la comunicación de llamada a procedimiento remoto (RPC) entre el Controller y NodeAgent
	controller_monitor.log	Registro de monitoreo

Tipo	Nombre de archivo de registro	Descripción
	controller_fsm.log	Registro de máquina de estado
	controller_alarm.log	Registro de alarma de Controller
	controller_backup.log	Registro de copia de respaldo y recuperación de Controller
	install.log, distributeAdapter-Files.log, install_os_optimization.log	Registro de instalación de OMS
	oms_ctl.log	Registro de inicio y detención de OMS
	installntp.log	Registro de instalación de NTP
	modify_manager_param.log	Registro de modificación de parámetros de Manager
	backup.log	Registro de ejecución del script de copia de respaldo de OMS
	supressionAlarm.log	Registro de ejecución del script de alarma
	om.log	Registro de generación de certificados de OM
	backupplugin_ctl.log	Registro de inicio del proceso de complemento de copia de respaldo y restauración
	getLogs.log	Registro de ejecución del script de registro de recolección
	backupAuditLogs.log	Registro de ejecución de script de copia de respaldo de registro de auditoría
	certStatus.log	Registro que registra las comprobaciones de certificados regulares
	distribute.log	Registro de distribución de certificados

Tipo	Nombre de archivo de registro	Descripción
	ficertgenetrate.log	Registros de sustitución de certificados, incluidos los registros de certificados de nivel 2, certificados CAS y certificados httpd
	genPwFile.log	Registro que registra la generación de archivos de contraseña de certificado
	modifyproxyconf.log	Registro que registra la modificación de la configuración del proxy HTTPD
	importTar.log	Registro que registra el proceso de importación de certificados en la biblioteca de confianza
Httpd	install.log	Registro de instalación de Httpd
	access_log, error_log	Registro de ejecución de Httpd
logman	logman.log	Registro de herramientas de empaquetado
NodeAgent	install.log, install_os_optimization.log	Registro de instalación de NodeAgent
	installntp.log	Registro de instalación de NTP
	start_ntp.log	Registro de inicio de NTP
	ntpChecker.log	Registro de comprobación de NTP
	ntpMonitor.log	Registro de monitoreo de NTP
	heartbeat_trace.log	Registro que registra los latidos del corazón entre NodeAgent y Controller
	alarm.log	Registro de alarmas
	monitor.log	Registro de monitoreo
	nodeagent_ctl.log, start-agent.log	Registro de inicio de NodeAgent

Tipo	Nombre de archivo de registro	Descripción
	agent.log	NodeAgent run log
	cert.log	Registro de certificados
	agentplugin.log	Registro de monitoreo de estado de ejecución del complemento de agente
	omaplugin.log	Registro de ejecución del complemento de OMA
	diskhealth.log	Registro de comprobación de estado del disco
	supressionAlarm.log	Registro de ejecución del script de alarma
	updateHostFile.log	Registro de actualización de la lista de hosts
	collectLog.log	Registro de ejecución del script de recolección de registro de nodo
	host_metric_collect.log	Registro de ejecución de la colección de índices de host
	checkfileconfig.log	Archivo de registro de ejecución de comprobación de permiso de archivo
	entropycheck.log	Registro de ejecución de comprobación de entropía
	timer.log	Registro de programación periódica de nodos
	pluginmonitor.log	Registro de complemento de monitoreo de componentes
	agent_alarm_py.log	Registro que registra alarmas en caso de permiso de archivo NodeAgent insuficiente
okerberos	addRealm.log, modifyKerberosRealm.log	Registro de traspaso de dominio
	checkservice_detail.log	Registro de comprobación de salud de Okerberos

Tipo	Nombre de archivo de registro	Descripción
	genKeytab.log	registro de generación de keytab
	KerberosAdmin_genConfigDetail.log	Registro de ejecución que registra la generación de kadmin.conf al iniciar el proceso kadmin
	KerberosServer_genConfigDetail.log	Registro de ejecución que registra la generación de krb5kdc.conf al iniciar el proceso krb5kdc
	oms-kadmind.log	Registro de ejecución del proceso kadmin
	oms_kerberos_install.log, postinstall_detail.log	Registro de instalación de Okerberos
	oms-krb5kdc.log	Registro de ejecución del proceso krbkdc
	start_detail.log	Registro de inicio de Okerberos
	realmDataConfigProcess.log	Registro de reversión en caso de fallo en el traspaso de dominio
	stop_detail.log	Registro de parada de Okerberos
oldapserver	ldapserver_backup.log	Registro de copia de respaldo de Oldapserver
	ldapserver_chk_service.log	Registro de comprobación de estado de Oldapserver
	ldapserver_install.log	Registro de instalación de Oldapserver
	ldapserver_start.log	Registro de inicio de Oldapserver
	ldapserver_status.log	Registro que registra el estado del proceso Oldapserver
	ldapserver_stop.log	Registro de parada de Oldapserver
	ldapserver_wrap.log	Registro de gestión de servicio Oldapserver

Tipo	Nombre de archivo de registro	Descripción
	ldapserver_uninstall.log	Registro de desinstalación de Oldapserver
	restart_service.log	Registro de reinicio de Oldapserver
	ldapserver_unlockUser.log	Registro que registra información sobre el desbloqueo de usuarios LDAP y la gestión de cuentas
omm	omsconfig.log	Registro de configuración de OMS
	check_oms_heartbeat.log	Registro de latidos del corazón de OMS
	monitor.log	Registro de monitoreo de OMS
	ha_monitor.log	Registro de operaciones de HA_Monitor
	ha.log	Registro de operación de HA
	fms.log	Registro de alarmas
	fms_ha.log	Registro de monitoreo de alarmas HA
	fms_script.log	Registro de control de alarma
	config.log	Registro de configuración de alarma
	iam.log	Registro de IAM
	iam_script.log	Registro de control de IAM
	iam_ha.log	Registro de monitoreo de IAM HA
	config.log	Registro de configuración de IAM
	operatelog.log	Registro de operación de IAM
	heartbeatcheck_ha.log	Registro de monitoreo de HA de latidos cardíacos de OMS

Tipo	Nombre de archivo de registro	Descripción
	install_oms.log	Registro de instalación de OMS
	pms_ha.log	Registro de monitoreo de HA
	pms_script.log	Registro de control de monitoreo
	config.log	Registro de configuración de monitoreo
	plugin.log	Registro de ejecución de complemento de monitoreo
	pms.log	Registro de monitoreo
	ha.log	Registro de ejecución de HA
	cep_ha.log	Registro de monitorización CEP HA
	cep_script.log	Registro de control de CEP
	cep.log	Registro de CEP
	config.log	Registro de configuración de CEP
	omm_gaussdba.log	Registro de monitoreo de GaussDB HA
	gaussdb-<SERIAL>.log	Registro de ejecución de GaussDB
	gs_ctl-<DATE>.log	Registro de archivo de registro de control de GaussDB
	gs_ctl-current.log	Registro de control de GaussDB
	gs_guc-current.log	Registro de operación de GaussDB
	encrypt.log	Registro de cifrado de Omm
	omm_agent_ctl.log	Registro de control de OMA
	oma_monitor.log	Registro de monitoreo de OMA

Tipo	Nombre de archivo de registro	Descripción
	install_oma.log	Registro de instalación de OMA
	config_oma.log	Registro de configuración de OMA
	omm_agent.log	Registro de ejecución de OMA
	acs.log	Registro de recursos de ACS
	aos.log	Registro de recursos de AOS
	controller.log	Registro de recursos de Controller
	feed_watchdog.log	registro de recurso de feed_watchdog
	floatip.log	Registro de recursos de dirección IP flotante
	ha_ntp.log	Registro de recursos NTP
	httpd.log	Registro de recursos Httpd
	okerberos.log	Registro de recurso Okerberos
	oldap.log	Registro de recursos OLdap
	tomcat.log	Registro de recursos Tomcat
	send_alarm.log	Registro de ejecución del script de envío de alarma HA del nodo de gestión
timestamp	restart_stamp	Registro de tiempo de inicio de NodeAgent
tomcat	cas.log, localhost_access_cas_log.log	Registro de ejecución de CAS
	catalina.log, catalina.out, host-manager.log, localhost.log, manager.log	Registro de ejecución de Tomcat
	localhost_access_web_log.log	Registro que registra el acceso a las API REST del FusionInsight Manager

Tipo	Nombre de archivo de registro	Descripción
	web.log	Registro de ejecución del proceso web
	northbound_ftp_sftp.log, snmp.log	Registro en dirección norte
watchdog	watchdog.log, feed_watchdog.log	registro de ejecución de watchdog
patch	oms_installPatch.log	Registro de instalación de parches de OMS
	agent_installPatch.log	Registro de instalación de parches de agente
	agent_uninstallPatch.log	Registro de desinstalación de parches de agente
	NODE_AGENT_restoreFile.log	Registro de restauración de parches del agente
	NODE_AGENT_updateFile.log	Registro de actualización de parches del agente
	OMA_restoreFile.log	Registro de archivos de restauración de parches de OMA
	OMA_updateFile.log	Registro de archivo de actualización de parches de OMA
	CONTROLLER_restoreFile.log	Registro de archivos de restauración de parches de CONTROLLER
	CONTROLLER_updateFile.log	Registro de archivo de actualización de parches de CONTROLLER
	OMS_restoreFile.log	Registro de archivos de restauración de parches de OMS
	oms_uninstallPatch.log	Registro de desinstalación de parches de OMS
	OMS_updateFile.log	Registro de archivo de actualización de parches de OMS

Tipo	Nombre de archivo de registro	Descripción
	createStackConf.log, decompress.log, decompress_OMS.log, distrExtractPatchOnOMS.log, slimReduction.log, switch_adapter.log	Registro de instalación de parches
sudo	sudo.log	Registro de ejecución del script Sudo

Niveles de registro

Tabla 8-24 describe los niveles de registro proporcionados por Manager. Las prioridades de los niveles de registro son FATAL, ERROR, WARN, INFO y DEBUG en orden descendente. Se imprimen los registros cuyos niveles sean superiores o iguales al nivel especificado. El número de registros impresos disminuye a medida que aumenta el nivel de registro especificado.

Tabla 8-24 Niveles de registro

Nivel	Descripción
FATAL	Los registros de este nivel registran información de error fatal sobre el procesamiento de eventos actuales que puede provocar un bloqueo del sistema.
ERROR	Los registros de este nivel registran información de error sobre el procesamiento de eventos actual, lo que indica que el funcionamiento del sistema es anormal.
WARN	Información anormal sobre el procesamiento del evento actual. Estas anomalías no darán lugar a fallas del sistema.
INFO	Información de estado de ejecución normal sobre el sistema y los eventos.
DEBUG	Los registros de este nivel registran la información del sistema y la información de depuración del sistema.

Formatos de registro

En la siguiente tabla se muestran los formatos de registro de Manager.

Tabla 8-25 Formatos de registro

Tipo	Componente	Formato	Ejemplo
Controller, Httpd, logman, NodeAgent, okerberos, oldapserver, omm, tomcat, upgrade	Controller, Httpd, logman, NodeAgent, okerberos, oldapserver, omm, tomcat, upgrade	*<yyyy-MM-dd HH:mm:ss,SSS>|<Log level>|<Name of the thread that generates the log>|<Message in the log>|<Location where the log event occurs>*	2015-06-30 00:37:09,067 INFO [pool-1-thread-1] Completed Discovering Node. com..hadoop.om.controller.tasks.nodesetup.DiscoverNodeTask.execute(DiscoverNodeTask.java:299)

8.7.3 Consulta y exportación de registros de auditoría

Escenario

Esta sección describe cómo ver y exportar registros de auditoría en MRS Manager. Los registros de auditoría se pueden utilizar para rastrear eventos de seguridad, localizar causas de fallas y determinar responsabilidades.

El sistema registra la siguiente información de registro:

- Información de actividad del usuario, como inicio de sesión y cierre de sesión del usuario, modificación de la información del usuario del sistema y modificación de la información del grupo de usuarios del sistema
- Información de instrucciones de operación del usuario, como inicio, detención y actualización de software del clúster.

Procedimiento

- Consulta de registros de auditoría
  a. En MRS Manager, haga clic en **Audit** para ver los registros de auditoría predeterminados.

     Si un registro de auditoría contiene más de 256 caracteres, haga clic en el botón de expandir para ver los detalles del registro de auditoría.

     - De forma predeterminada, los registros se ordenan en orden descendente por la columna **Occurred**. Puede hacer clic en **Operation Type**, **Severity**, **Occurred**, **User**, **Host**, **Service**, **Instance** o **Operation Result** para cambiar el modo de ordenación.
     - **Severity** puede filtrar todas las alarmas de la misma gravedad. Los resultados incluyen alarmas despejadas y no claras.

     Los registros de auditoría exportados contienen la siguiente información:

     - **Sno**: indica el número de registros de auditoría generados por MRS Manager. El número se incrementa en 1 cuando se genera un nuevo registro de auditoría.
     - **Operation Type**: indica el tipo de operación de una operación de usuario. Hay nueve escenarios: **Alarm**, **Auditlog**, **Backup And Restoration**, **Cluster**, **Collect Log**, **Host**, **Service**, **Tenant** y **User_Manager**. **User_Manager** sólo

se admite en clústeres con autenticación de Kerberos habilitada. Cada escenario contiene diferentes tipos de operación. Por ejemplo, **Alarm** incluye **Export alarms**; **Cluster** incluye **Start cluster** y **Tenant** incluye **Add tenant**.

- **Severity** indica el nivel de seguridad de cada registro de auditoría, incluidos **Critical**, **Major**, **Minor** y **Informational**.
- **Start Time** indica la hora de inicio de la operación. La hora es de CET o CEST .
- **End Time** indica la hora en que finaliza la operación. La hora es de CET o CEST .
- **User IP Address**: indica la dirección IP utilizada por un usuario para realizar operaciones.
- **User**: indica el nombre del usuario que realiza la operación.
- **Host**: indica el nodo donde se realiza la operación del usuario. La información no se guarda si la operación no implica un nodo.
- **Service**: indica el servicio en el clúster donde se realiza la operación del usuario. La información no se guarda si la operación no implica un servicio.
- **Instance**: indica la instancia de rol en el clúster donde se realiza la operación del usuario. La información no se guarda si la operación no implica una instancia de rol.
- **Operation Result**: indica el resultado de la operación, incluidos **Successful**, **Failed** y **Unknown**.
- **Content**: indica la información de ejecución de la operación del usuario.

b. Haga clic en **Advanced Search**. En el área de búsqueda, establezca criterios de búsqueda y haga clic en **Search** para ver los registros de auditoría del tipo especificado. Haga clic en **Reset** para borrar los criterios de búsqueda.

NOTA

Start Time y **End Time** especifican la hora de inicio y la hora de finalización del intervalo de tiempo. Puede buscar las alarmas generadas dentro del rango de tiempo.

- Exportación de registros de auditoría
  a. En la lista de registros de auditoría, haga clic en **Export All** para exportar todos los registros.
  b. En la lista de registros de auditoría, active la casilla de verificación de un registro y haga clic en **Export** para exportar el registro.

8.7.4 Exportación de registros de servicio

Escenario

Esta sección describe cómo exportar los registros generados por cada rol de servicio desde MRS Manager.

Prerrequisitos

- Ha obtenido el ID de clave de acceso (AK) y la clave de acceso secreta (SK) de la cuenta.
- Se ha creado un sistema de archivos paralelo en OBS.

Procedimiento

Paso 1 En MRS Manager, haga clic en **System**.

Paso 2 Haga clic en **Export Log** en **Maintenance**.

Paso 3 Establezca un servicio para **Service**. Establezca **Host** en la dirección IP del host donde se despliega el servicio. Seleccione la hora correspondiente para **Start Time** y **End Time**.

Paso 4 En **Export To**, seleccione una ruta de acceso para guardar los registros. Este parámetro sólo está disponible para clústeres con autenticación de Kerberos activada.

- **Local PC**: indica que los registros se guardan en el entorno local. Entonces vaya a **Paso 8**.
- **OBS** indica que los registros se guardan en OBS. Esta es la opción predeterminada. Entonces vaya a **Paso 5**.

Paso 5 Establezca **OBS Path** en la ruta para almacenar los registros de servicio en OBS.

El valor debe ser una ruta completa y no puede comenzar con una barra diagonal (/). La ruta puede ser inexistente y será creada automáticamente por el sistema. La ruta completa de OBS puede contener un máximo de 900 bytes.

Paso 6 En **Bucket**, escriba el nombre del sistema de archivos de OBS creado.

Paso 7 Establezca **AK** y **SK** en el ID de clave de acceso y clave de acceso secreta del usuario.

Paso 8 Haga clic en **OK**.

----Fin

8.7.5 Configuración de los parámetros de exportación del registro de auditoría

Escenario

Si los registros de auditoría MRS se almacenan en el sistema durante mucho tiempo, el espacio en disco del directorio de datos puede ser insuficiente. Por lo tanto, puede establecer parámetros de exportación para exportar automáticamente registros de auditoría a un directorio especificado en el servidor OBS a tiempo, lo que facilita la gestión del registro de auditoría.

NOTA

Los registros de auditoría exportados al servidor OBS incluyen registros de auditoría de servicio y registros de auditoría de gestión.

- Los registros de auditoría de servicio se comprimen y almacenan automáticamente en el directorio **/var/log/Bigdata/audit/bk/** en el nodo de gestión activa a las 03:00 todos los días. El formato de nombre de archivo es *<yyyy-MM-dd_HH-mm-ss>***.tar.gz**. De forma predeterminada, se pueden almacenar un máximo de siete archivos de registro. Si se almacenan más de siete archivos de registro, el sistema elimina automáticamente los archivos de registro generados hace siete días.
- El rango de datos de los registros de auditoría de gestión exportados a OBS cada vez es desde la última fecha en que los registros se exportan correctamente a OBS hasta la fecha en que se ejecuta la tarea. Cuando el número de registros de auditoría de gestión alcanza los 100,000, el sistema volca automáticamente los primeros 90,000 registros de auditoría en un archivo local y retiene 10,000 registros de auditoría en la base de datos. Los archivos de registro volcados se guardan en el directorio **${BIGDATA_DATA_HOME}/dbdata_om/dumpData/iam/operatelog** en el nodo de gestión activa. El formato de nombre de archivo es **OperateLog_store**_*YY_MM_DD_HH_MM_SS*_**.csv**. Se puede guardar un máximo de 50 archivos de registro de auditoría históricos.

Prerrequisitos

- Ha obtenido el ID de clave de acceso (AK) y la clave de acceso secreta (SK) de la cuenta.
- Se ha creado un sistema de archivos paralelo en OBS.

Procedimiento

Paso 1 En MRS Manager, haga clic en **System**.

Paso 2 Elija **Export Audit Log** en **Maintenance**.

Tabla 8-26 Parámetros para exportar registros de auditoría

Parámetro	Valor	Descripción
Export Audit Log	● On ● Off	(Obligatorio) Especifica si se debe habilitar la función de exportación del registro de auditoría. ● On: habilita la exportación de registros de auditoría. ● Off: deshabilita la exportación del registro de auditoría.
Start Time	24/07/2017 09:00:00 (ejemplo)	(Obligatorio) Especifica la hora de inicio de la exportación de registros de auditoría.
Period (days)	1 día (valor de ejemplo)	(Obligatorio) Especifica el intervalo de exportación de registros de auditoría. El intervalo varía de 1 a 5 días.
Bucket	mrs-bucket (valor de ejemplo)	(Obligatorio) Especifica el nombre del sistema de archivos OBS al que se exportan los registros de auditoría.

Parámetro	Valor	Descripción
OBS path	**/opt/omm/oms/auditLog** (valor de ejemplo)	(Obligatorio) Especifica la ruta de acceso OBS a la que se exportan los registros de auditoría.
AK	*XXX* (valor de ejemplo)	(Obligatorio) Especifica el ID de clave de acceso del usuario.
SK	*XXX* (valor de ejemplo)	(Obligatorio) Especifica la clave de acceso secreta del usuario.

NOTA

Los registros de auditoría se almacenan en los archivos **service_auditlog** y **manager_auditlog** en OBS, que se utilizan para almacenar los registros de auditoría de servicio y los registros de auditoría de gestión, respectivamente.

----Fin

8.8 Gestión de comprobación de estado

8.8.1 Realización de una comprobación de estado

Escenario

Para asegurarse de que los parámetros, las configuraciones y el monitoreo del clúster son correctos y que el clúster puede ejecutarse de forma estable durante mucho tiempo, puede realizar una comprobación de estado durante el mantenimiento de rutina.

NOTA

Una comprobación de estado del sistema incluye las comprobaciones de estado de MRS Manager, de nivel de servicio y de nivel de host:

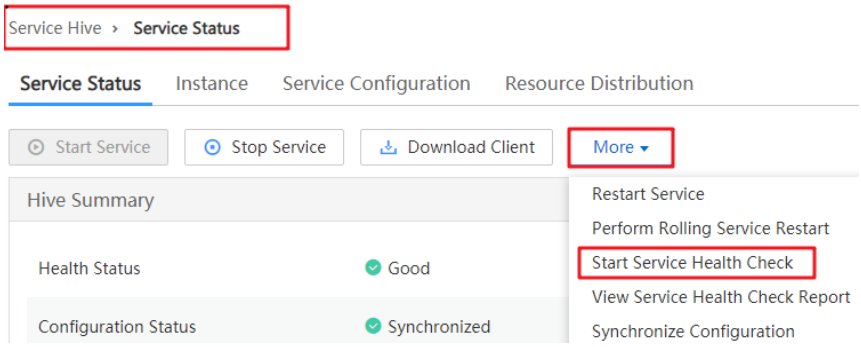
- Las comprobaciones de estado de MRS Manager se centran en si la plataforma de gestión unificada puede proporcionar funciones de gestión.
- Las comprobaciones de estado a nivel de servicio se centran en si los componentes pueden proporcionar servicios correctamente.
- Las comprobaciones de estado a nivel de host se centran en si los indicadores de host son normales.

La comprobación de estado del sistema incluye tres tipos de elementos de comprobación: estado de estado, alarmas relacionadas e indicadores de monitoreo personalizados para cada objeto de comprobación. Los resultados de la comprobación de estado no siempre son los mismos que los del **Health Status** del portal.

Procedimiento

- Realice manualmente la comprobación de estado de todos los servicios.
  a. Haga clic en **Services**.
  b. Elija **More** > **Start Service Health Check** para iniciar la comprobación de estado del servicio.

Figura 8-11 Iniciar la comprobación del estado del servicio



NOTA

- La comprobación del estado del clúster incluye comprobaciones del estado del Manager, del servicio y del host.
- Para realizar comprobaciones de estado del clúster, también puede elegir **System** > **Maintenance** > **Check Health Check** > **Start Cluster Health Check** en MRS Manager.
- Para exportar el resultado de la comprobación de estado, haga clic en **Export Report** en la esquina superior izquierda.

- Realice manualmente la comprobación de estado de un servicio.
  a. Haga clic en **Services**. En la lista de servicios, haga clic en el nombre del servicio deseado.
  b. Elija **More** > **Start Service Health Check** para iniciar la comprobación de estado del servicio.
- Realice manualmente la comprobación de estado de un host.
  a. Haga clic en **Hosts**.
  b. Active la casilla de verificación del host para el que desea comprobar el estado de salud.
  c. Elija **More** > **Start Host Health Check** para iniciar la comprobación de estado del host.
- Realización automática de una comprobación de estado
  a. Haga clic en **System**.
  b. Haga clic en **Check Health Status** en **Maintenance**.
  c. Haga clic en **Configure Health Check** para configurar los elementos de comprobación de estado automática.

     Max. Number of Health Check Reports: número máximo de informes de comprobación de estado. El valor debe ser un número entero comprendido entre 1 y 100.

     Periodic Health Check: especifica si se debe habilitar la comprobación de estado automática. La función **Periodic Health Check** está deshabilitada de forma predeterminada. Puede hacer clic para activar la función y seleccionar **Daily**, **Weekly** o **Monthly** según los requisitos de gestión.
  d. Haga clic en **OK** para guardar la configuración. El **Health check configuration saved successfully** se muestra en la esquina superior derecha.

8.8.2 Consulta y exportación de un informe de comprobación de estado

Escenario

Puede ver el resultado de la comprobación de estado en MRS Manager y exportar los resultados de la comprobación de estado para su análisis posterior.

NOTA

Una comprobación de estado del sistema incluye las comprobaciones de estado de MRS Manager, de nivel de servicio y de nivel de host:

- Las comprobaciones de estado de MRS Manager se centran en si la plataforma de gestión unificada puede proporcionar funciones de gestión.
- Las comprobaciones de estado a nivel de servicio se centran en si los componentes pueden proporcionar servicios correctamente.
- Las comprobaciones de estado a nivel de host se centran en si los indicadores de host son normales.

La comprobación de estado del sistema incluye tres tipos de elementos de comprobación: estado de estado, alarmas relacionadas e indicadores de monitoreo personalizados para cada objeto de comprobación. Los resultados de la comprobación de estado no siempre son los mismos que los del **Health Status** del portal.

Prerrequisitos

Ha realizado una comprobación de salud.

Procedimiento

Paso 1 Haga clic en **Services**.

Paso 2 Elija **More > View Cluster Health Check Report** para ver el informe de comprobación de estado de un clúster.

Paso 3 Haga clic en **Export Report** en el panel de informe de comprobación de estado para exportar el informe y ver información detallada sobre los elementos de comprobación.

NOTA

Para obtener más información sobre cómo corregir los errores de los elementos de comprobación, consulte **Indicadores de comprobación de estado de DBService** a **Indicadores de comprobación de estado de ZooKeeper**.

----Fin

8.8.3 Configuración del número de informes de comprobación de estado que se van a reservar

Escenario

Los informes de comprobación de estado de los clústeres, servicios y hosts de MRS pueden variar con el tiempo y el escenario. Puede modificar el número de informes de comprobación de estado que se reservarán en MRS Manager para una comparación posterior.

Esta configuración es válida para informes de comprobación de estado de clústeres, servicios y hosts. Los archivos de informe se guardan en **$BIGDATA_DATA_HOME/Manager/**

healthcheck en el nodo de gestión activo de forma predeterminada y se sincronizan automáticamente con el nodo de gestión en espera.

Prerrequisitos

Los usuarios han especificado los requisitos de servicio y planificado el tiempo de ahorro y la frecuencia de comprobación de estado, y el espacio en disco de los nodos de gestión activo y en espera es suficiente.

Procedimiento

Paso 1 Elija **System** > **Maintenance** > **Check Health Status** > **Configure Health Check**.

Paso 2 Establezca **Max. Number of Health Check Reports** en el número de informes de comprobación de estado que se van a reservar. El valor varía de 1 a 100. El valor predeterminado es 50.

Paso 3 Haga clic en **OK** para guardar la configuración. El mensaje "Health check configuration saved successfully" aparece en la esquina superior derecha.

----Fin

8.8.4 Gestión de informes de comprobación de estado

Escenario

En MRS Manager, los usuarios pueden gestionar informes históricos de comprobación de estado, por ejemplo, ver, descargar y eliminar informes históricos de comprobación de estado.

Procedimiento

- Descargue un informe de comprobación de estado especificado.
  a. Elija **System** >**Maintenance** >**Check Health Status**.
  b. Busque la fila que contiene el informe de comprobación de estado de destino y haga clic en **Download** para descargar el archivo de informe.
- Descargue los informes de comprobación de estado especificados en lotes.
  a. Elija **System** >**Maintenance** >**Check Health Status**.
  b. Seleccione varios informes de comprobación de estado y haga clic en **Download File** para descargarlos.
- Eliminar un informe de comprobación de estado especificado.
  a. Elija **System** >**Maintenance** >**Check Health Status**.
  b. Busque la fila que contiene el informe de comprobación de estado de destino y haga clic en **Delete** para eliminar el archivo de informe.
- Eliminar los informes de comprobación de estado especificados en lotes.
  a. Elija **System** >**Maintenance** >**Check Health Status**.
  b. Seleccione varios informes de comprobación de estado y haga clic en **Delete File** para eliminarlos.

8.8.5 Indicadores de comprobación de estado de DBService

Comprobación de estado de servicio

Indicador: Estado del servicio

Descripción: Este indicador se utiliza para comprobar si el estado del servicio DBService es normal. Si el estado es anormal, el servicio no está sano.

Método de manejo: Si el indicador es anormal, rectifique el fallo con referencia a ALM-27001.

Comprobación de alarma

Indicador: Información de alarma

Descripción: Este indicador se utiliza para comprobar si existen alarmas en el host. Si existen alarmas, el servicio no está sano.

Guía de recuperación: Si este indicador es anormal, puede corregir la falla consultando la guía de manejo de alarmas.

8.8.6 Indicadores de comprobación de estado de Flume

Estado de salud del servicio

Indicador: Estado del servicio

Descripción: Este indicador se utiliza para comprobar si el estado del servicio de Flume es normal. Si el estado es anormal, el servicio no está sano.

Guía de recuperacion: Si el indicador es anormal, rectifique la falla con referencia a ALM-24000.

Comprobación de alarma

Indicador: Información de alarma

Descripción: Este indicador se utiliza para comprobar si existen alarmas en el host. Si existen alarmas, el servicio no está sano.

Guía de recuperación: Si este indicador es anormal, puede corregir la falla consultando la guía de manejo de alarmas.

8.8.7 Indicadores de comprobación de estado de HBase

Recuento de RegionServer normal

Indicador: Recuento de RegionServer normal

Descripción: Este indicador se utiliza para comprobar el número de RegionServers que se están ejecutando correctamente en un clúster de HBase.

Guía de recuperación: Si el indicador es anormal, compruebe si el estado de RegionServer es normal. Si el estado es anormal, solucione el problema y compruebe que la red es normal.

Estado de salud del servicio

Indicador: Estado del servicio

Descripción: Este indicador se utiliza para comprobar si el estado del servicio HBase es normal. Si el estado es anormal, el servicio no está sano.

Guía de recuperación: Si el indicador es anormal, compruebe si el estado de HMaster y RegionServer es normal. Si el estado es anormal, resuelva el problema. A continuación, compruebe si el estado del servicio ZooKeeper es defectuoso. En el cliente HBase, compruebe si los datos de la tabla HBase se pueden leer correctamente y localice la causa de la falla de lectura de datos. Maneje la alarma siguiendo las instrucciones del documento de procesamiento de alarmas.

Comprobación de alarma

Indicador: Información de alarma

Descripción: Este indicador se utiliza para comprobar si existen alarmas. Si existen alarmas, el servicio no está sano.

Guía de recuperación: Si este indicador es anormal, puede corregir la falla consultando la guía de manejo de alarmas.

8.8.8 Indicadores de comprobación de estado del host

Uso de Swap

Indicador: Uso de Swap

Descripción: Uso de Swap del sistema. El valor se calcula utilizando la siguiente fórmula: Uso de Swap = Tamaño de swap usado/Tamaño total de swap. Supongamos que el umbral actual se establece en 75.0%. Si el uso de los identificadores de archivo en el sistema excede el umbral, el sistema no está sano.

Guía de recuperación:

1. Compruebe el uso de swap del nodo.

   Inicie sesión en el nodo no saludable y ejecute el comando **free -m** para comprobar el espacio de swap total y el espacio de swap usado. Si el uso del espacio de intercambio excede el umbral, vaya a **2**.
2. Si el uso de swap excede el umbral, se recomienda ampliar la capacidad del sistema, por ejemplo, agregar nodos.

Uso del identificador de archivo de host

Indicador: Uso del identificador de archivo de host

Description: Este indicador indica el uso del identificador de archivo en el sistema. Uso del identificador de archivo de host = Número de identificadores usados/Número total de identificadores. Si el uso excede el umbral, el sistema no está sano.

Guía de recuperación:

1. Verifique el uso del identificador de archivo del host.

Inicie sesión en el nodo no saludable y ejecute el comando **cat /proc/sys/fs/file-nr**. En la salida del comando, las columnas primera y tercera indican el número de identificadores usados y el número total de identificadores, respectivamente. Si el uso excede el umbral, vaya a **2**.

2. Si el uso del identificador de archivos del host excede el umbral, se recomienda comprobar el sistema y analizar el uso del identificador de archivos.

Desfase de NTP

Indicador: Desplazamiento de NTP

Descripción: Este indicador indica el desplazamiento de tiempo de NTP. Si la desviación de tiempo excede el umbral, el sistema no está sano.

Guía de recuperación:

1. Compruebe el desplazamiento de tiempo de NTP.

   Inicie sesión en el nodo no saludable y ejecute el comando **/usr/sbin/ntpq -np** para ver la información. En la salida del comando, la columna **Offset** indica el desplazamiento de tiempo. Si el desplazamiento de tiempo es mayor que el umbral, vaya a **2**.

2. Si el indicador es anormal, compruebe si la configuración de la fuente del reloj es correcta. Póngase en contacto con el personal de O&M.

Carga promedio

Indicador: Carga promedia

Descripción: Carga promedia del sistema, que indica el número medio de procesos en la cola en ejecución en un período especificado. La carga media del sistema se calcula utilizando el valor de carga obtenido por el comando de uptime. Método de cálculo: (Carga de 1 minuto + Carga de 5 minutos + Carga de 15 minutos)/(3 x Número de CPUs). Supongamos que el umbral actual se establece en 2. Si la carga media excede 2, el sistema no está sano.

Guía de recuperación:

1. Inicie sesión en el nodo no saludable y ejecute el comando **uptime**. Las últimas tres columnas de la salida del comando indican la carga en 1 minuto, 5 minutos y 15 minutos, respectivamente. Si la carga media del sistema supera el umbral, vaya a **2**.
2. Si la carga media del sistema excede el umbral, se recomienda realizar la ampliación de la capacidad del sistema, como agregar nodos.

Procesos de estado D

Indicador: Proceso del Estado D

Descripción: Este indicador indica el proceso de sueño imparable, es decir, el proceso en el estado D. Un proceso que está en el estado D está esperando E/S, como E/S de disco y E/S de red, y experimenta una excepción de E/S. Si existe algún proceso en el estado D en el sistema, el sistema no está sano.

Guía de recuperación: Si el indicador es anormal, el sistema genera una alarma. Se le aconseja que maneje la alarma por referencia a ALM-12028.

Estado del hardware

Indicador: Estado del hardware

Descripción: Este indicador se utiliza para comprobar el estado del hardware del sistema, incluidos la CPU, la memoria, el disco, la fuente de alimentación y el ventilador. Este indicador obtiene información relacionada con el hardware mediante **ipmitool sdr elist**. Si el estado del hardware es anormal, el hardware no está sano.

Guía de recuperación:

1. Inicie sesión en el nodo donde el resultado de la comprobación no está sano. Ejecute el comando **ipmitool sdr elist** para comprobar el estado del hardware del sistema. La última columna de la salida del comando indica el estado del hardware. Si el estado se incluye en la siguiente tabla de descripción de fallas, el resultado de la comprobación no está sano.

Módulo	Síntomas
Processor	IERR Thermal Trip FRB1/BIST failure FRB2/Hang in POST failure FRB3/Processor startup/init failure Configuration Error SM BIOS Uncorrectable CPU-complex Error Disabled Throttled Uncorrectable machine check exception
Power Supply	Failure detected Predictive failure Power Supply AC lost AC lost or out-of-range AC out-of-range, but present Config Error: Vendor Mismatch Config Error: Revision Mismatch Config Error: Processor Missing Config Error: Power Supply Rating Mismatch Config Error: Voltage Rating Mismatch Config Error

Módulo	Síntomas
Power Unit	240VA power down Interlock power down AC lost Soft-power control failure Failure detected Predictive failure
Memory	Uncorrectable ECC Parity Memory Scrub Failed Memory Device Disabled Correctable ECC logging limit reached Configuration Error Throttled Critical Overtemperature
Drive Slot	Drive Fault Predictive Failure Parity Check In Progress In Critical Array In Failed Array Rebuild In Progress Rebuild Aborted
Battery	Low Failed

2. Si el indicador es anormal, póngase en contacto con el personal de O&M.

Nombre del host

Indicador: Nombre de host

Descripción: Este indicador se utiliza para comprobar si el nombre de host está definido. Si el nombre de host no está definido, el sistema no está sano. Si el indicador es anormal, se recomienda establecer el nombre de host correctamente.

Guía de recuperación:

1. Inicie sesión en el nodo donde el resultado de la comprobación no está sano.
2. Ejecute el comando hostname nombre de host para cambiar el nombre de host para asegurarse de que el nombre de host es coherente con el nombre de host planificado.

   hostname*host name* Por ejemplo, para cambiar el nombre de host a **Bigdata-OM-01**, ejecute el comando **hostname Bigdata-OM-01**.
3. Modifique el archivo de configuración del nombre de host.

Ejecute el comando **vi /etc/HOSTNAME** para editar el archivo. Cambie el contenido del archivo a **Bigdata-OM-01**. Guarde el archivo y salga.

Umask

Indicador: Umask

Descripción: Este indicador se utiliza para comprobar si la configuración de umask de usuario **omm** es correcta. Si Umask no es 0077, el sistema no está sano.

Guía de recuperación:

1. Si el indicador es anormal, se recomienda establecer umask del usuario **omm** a 0077. Inicie sesión en el nodo no saludable y ejecute el comando **su - omm** para cambiar a usuario **omm**.
2. Ejecute el comando **vi ${BIGDATA_HOME}/.om_profile** y cambie el valor de **umask** a **0077**. Guarde y salga.

Estado de HA de OMS

Indicador: Estado de HA de OMS

Descripción: Este indicador se utiliza para comprobar si los recursos del clúster de dos nodos de OMS son normales. Puede ejecutar el comando **${CONTROLLER_HOME}/sbin/status-oms.sh** para ver información detallada sobre el estado de los recursos del clúster de dos nodos de OMS. Si algún módulo es anormal, el OMS no está sano.

Guía de recuperación:

1. Inicie sesión en el nodo de gestión activo y ejecute el comando **su - omm** para cambiar a usuario **omm**. Ejecute el comando **${CONTROLLER_HOME}/sbin/status-oms.sh** para comprobar el estado de OMS.
2. Si floteip, okerberos y oldap son anormales, maneje los problemas con referencia a ALM-12002, ALM-12004 y ALM-12005 respectivamente.
3. Si otros recursos son anormales, se recomienda ver los registros de los módulos defectuosos.

   Si los recursos del controlador son anormales, vea **/var/log/Bigdata/controller/controller.log** del nodo defectuoso.

   Si los recursos de CEP son anormales, vea **/var/log/Bigdata/omm/oms/cep/cep.log** del nodo defectuoso.

   Si los recursos AOS son anormales, vea **/var/log/Bigdata/controller/aos/aos.log** del nodo defectuoso.

   Si los recursos feed_watchdog son anormales, vea el **/var/log/Bigdata/watchdog/watchdog.log** del nodo anormal.

   Si los recursos de HTTPD son anormales, vea **/var/log/Bigdata/httpd/error_log** del nodo anormal.

   Si los recursos de FMS son anormales, vea **/var/log/Bigdata/omm/oms/fms/fms.log** del nodo anormal.

   Si los recursos de PMS son anormales, vea **/var/log/Bigdata/omm/oms/pms/pms.log** del nodo anormal.

   Si los recursos de IAM son anormales, vea **/var/log/Bigdata/omm/oms/iam/iam.log** del nodo anormal.

Si el recurso GaussDB es anormal, compruebe el **/var/log/Bigdata/omm/oms/db/omm_gaussdba.log** del nodo anormal.

Si los recursos NTP son anormales, vea **/var/log/Bigdata/omm/oms/ha/scriptlog/ha_ntp.log** del nodo anormal.

Si los recursos de Tomcat son anormales, vea **/var/log/Bigdata/tomcat/catalina.log** del nodo anormal.

4. Si la falla no se puede corregir en función de los registros, póngase en contacto con el personal de O&M y envíe los registros de fallas recopiladas.

Comprobación del directorio de instalación y del directorio de datos

Indicator: Comprobación de directorios de instalación y directorios de datos

Descripción: Este indicador comprueba el directorio **lost+found** en el directorio raíz de la partición de disco donde se encuentra el directorio de instalación (de forma predeterminada, **/opt/Bigdata**). Si el directorio contiene los archivos de usuario **omm**, hay excepciones. Cuando un nodo es anormal, los archivos relacionados se almacenan en el directorio **lost+found**. Este indicador se utiliza para comprobar si los archivos se pierden en tales escenarios. Compruebe el directorio de instalación (por ejemplo, **/opt/Bigdata**) y el directorio de datos (por ejemplo, **/srv/BigData**). Si existen archivos de usuarios no-omm en los dos directorios, el sistema no está sano.

Guía de recuperación:

1. Inicie sesión en el nodo no saludable y ejecute el comando **su - omm** para cambiar a usuario **omm**. Compruebe si existen archivos o carpetas del usuario omm en el directorio **lost+found**.

   Si el archivo de usuario **omm** existe, se recomienda restaurarlo y comprobar de nuevo. Si el archivo de usuario **omm** no existe, vaya a **2**.

2. Compruebe el directorio de instalación y el directorio de datos. Compruebe si los archivos o carpetas de otros usuarios existen en el directorio de instalación y en el directorio de datos. Si los archivos y carpetas se generan manualmente archivos temporales, se recomienda eliminarlos y comprobar de nuevo.

Uso de CPU

Indicador: Uso de CPU

Descripción: Este indicador se utiliza para comprobar si el uso de la CPU excede el umbral. Si el uso del disco excede el umbral, el sistema no está sano.

Guía de recuperación: Si el indicador es anormal, el sistema genera una alarma. Se le aconseja que maneje la alarma al referirse a ALM-12016.

Uso de memoria

Indicador: Uso de memoria

Descripción: Este indicador se utiliza para comprobar si el uso de memoria excede el umbral. Si el uso del disco excede el umbral, el sistema no está sano.

Guía de recuperación: Si el indicador es anormal, el sistema genera una alarma. Se le aconseja que maneje la alarma al referirse a ALM-12018.

Uso del disco de host

Indicador: Uso del disco de host

Descripción: Este indicador se utiliza para comprobar si el uso del disco host excede el umbral. Si el uso del disco excede el umbral, el sistema no está sano.

Guía de recuperación: Si el indicador es anormal, el sistema genera una alarma. Se le aconseja que maneje la alarma al referirse a ALM-12017.

Tasa de escritura de disco de host

Indicador: Tasa de escritura en disco de host

Descripción: Este indicador se utiliza para comprobar la velocidad de escritura en disco de un host. La velocidad de escritura del disco host puede variar según el escenario de servicio. Por lo tanto, el valor de este indicador refleja solo el valor especificado. Debe determinar si el indicador es normal en escenarios de servicio especificados.

Guía de recuperación: Determine si la velocidad de escritura del disco actual es normal en función del escenario de servicio.

Tasa de lectura del disco del host

Indicador: Tasa de lectura del disco del host

Descripción: Este indicador se utiliza para comprobar la velocidad de lectura del disco de un host. La velocidad de lectura del disco host puede variar según el escenario de servicio. Por lo tanto, el valor de este indicador refleja solo el valor especificado. Debe determinar si el indicador es normal en escenarios de servicio especificados.

Guía de recuperación: Determine si la velocidad de lectura del disco actual es normal en función del escenario de servicio.

Estado de la red del plano de servicio del host

Indicador: Estado de la red del plano de servicio del host

Descripción: Este indicador se utiliza para comprobar la conectividad de la red del plano de servicio del host del clúster. Si los hosts están desconectados, el clúster no está sano.

Guía de recuperación: Si se utiliza la red de un solo plano, compruebe la dirección IP del único plano. Para una red de doble plano, el procedimiento de operación es el siguiente:

1. Compruebe la conectividad de red entre las direcciones IP del plano de servicio de los nodos de gestión activo y en espera.

   Si la red es anormal, vaya a **3**.

   Si la red es normal, vaya a **2**.
2. Compruebe la conectividad de red entre la dirección IP del nodo de gestión activo y la dirección IP del nodo anormal en el clúster.
3. Si la red está desconectada, póngase en contacto con el personal de O&M para corregir la falla de la red y asegurarse de que la red cumple con los requisitos de servicio.

Estado de host

Indicador: Estado del host

Descripción: Este indicador se utiliza para comprobar si el estado del host es normal. Si un nodo está defectuoso, el host no está sano.

Guía de recuperación: Si el indicador es anormal, rectifique la falla con referencia a ALM-12006.

Comprobación de alarma

Indicador: Comprobación de alarma

Descripción: Este indicador se utiliza para comprobar si existen alarmas en el host. Si existen alarmas, el servicio no está sano.

Guía de recuperación: Si este indicador es anormal, puede corregir la falla consultando la guía de manejo de alarmas.

8.8.9 Indicadores de comprobación de estado de HDFS

Tiempo promedio de envío de paquetes

Indicador: Tiempo promedio de envío de paquetes

Descripción: Este indicador se utiliza para recopilar estadísticas sobre el tiempo promedio para que el DataNode en el HDFS ejecute SendPacket cada vez. Si el tiempo promedio es mayor que 2,000,000 ns, el DataNode no es saludable.

Guía de recuperación: Si el indicador es anormal, compruebe si la velocidad de red del clúster es normal y si el uso de memoria o CPU es demasiado alto. Compruebe si la carga HDFS en el clúster es alta.

Estado de salud del servicio

Indicador: Estado del servicio

Descripción: Este indicador se utiliza para comprobar si el estado del servicio HDFS es normal. Si un nodo está defectuoso, el host no está sano.

Guía de recuperación: Si el indicador es anormal, compruebe si el estado de salud de los servicios KrbServer, LdapServer y ZooKeeper es defectuoso. De ser así, rectifique la falla. A continuación, compruebe si el error de escritura de archivos es causado por HDFS SafeMode ON. Utilice el cliente para comprobar si los datos no se pueden escribir en HDFS y localizar la causa del error de escritura de datos de HDFS. Maneje la alarma siguiendo las instrucciones del documento de procesamiento de alarmas.

Comprobación de alarma

Indicador: Información de alarma

Descripción: Este indicador se utiliza para comprobar si existen alarmas. Si existen alarmas, el servicio no está sano.

Guía de recuperación: Si este indicador es anormal, puede corregir la falla consultando la guía de manejo de alarmas.

8.8.10 Indicadores de comprobación de salud de Hive

Número máximo de sesiones permitidas por HiveServer

Indicador: Número máximo de sesiones permitidas por HiveServer

Descripción: Este indicador se utiliza para comprobar el número máximo de sesiones que se pueden conectar a Hive.

Guía de recuperación: Si este indicador es anormal, puede corregir la falla consultando la guía de manejo de alarmas.

Número de sesiones conectadas a HiveServer

Indicador: Número de sesiones conectadas a HiveServer

Descripción: Este indicador se utiliza para comprobar el número de conexiones de Hive.

Guía de recuperación: Si este indicador es anormal, puede corregir la falla consultando la guía de manejo de alarmas.

Estado de salud del servicio

Indicador: Estado del servicio

Descripción Este indicador se utiliza para comprobar si el estado del servicio Hive es normal. Si el estado es anormal, el servicio no está sano.

Guía de recuperación: Si este indicador es anormal, puede corregir la falla consultando la guía de manejo de alarmas.

Comprobación de alarma

Indicador: Información de alarma

Descripción: Este indicador se utiliza para comprobar si existen alarmas en el host. Si existen alarmas, el servicio no está sano.

Guía de recuperación: Si este indicador es anormal, puede corregir la falla consultando la guía de manejo de alarmas.

8.8.11 Indicadores de comprobación de salud de Kafka

Número de nodos de Broker disponibles

Indicador: Número de Brokers

Descripción: Este indicador se utiliza para comprobar el número de nodos de Broker disponibles en un clúster. Si el número de nodos de Broker disponibles en un clúster es menor que 2, el clúster no está sano.

Guía de recuperación: Si el indicador es anormal, vaya a la página de instancia de servicio de Kafka y haga clic en el nombre de host de la instancia de Broker no disponible. Vea el estado del host en el área **Overview**. Si el estado de salud del host es de **Good**, rectifique la falla haciendo referencia a las sugerencias de manejo de alarmas de **Process Fault**. Si el

estado no es **Good**, rectifique la falla consultando el procedimiento de manejo de la alarma **Node Fault**.

Estado de salud del servicio

Indicador: Estado del servicio

Descripción: Este indicador se utiliza para comprobar si el estado del servicio de Kafka es normal. Si el estado es anormal, el servicio no está sano.

Guía de recuperación: Si el indicador es anormal, rectificar la falla haciendo referencia a la alarma "Servicio Kafka no disponible".

Comprobación de alarma

Indicador: Información de alarma

Descripción: Este indicador se utiliza para comprobar si existen alarmas. Si existen alarmas, el servicio no está sano.

Guía de recuperación: Si este indicador es anormal, puede corregir la falla consultando la guía de manejo de alarmas.

8.8.12 Indicadores de comprobación de estado de KrbServer

Disponibilidad del servicio de KerberosAdmin

Indicator: Disponibilidad del servicio KerberosAdmin

Descripción: El sistema comprueba el estado del servicio KerberosAdmin. Si el resultado de la comprobación es anormal, el servicio KerberosAdmin no está disponible.

Guía de recuperación: Si el resultado de la comprobación del indicador es anormal, la causa posible es que el nodo donde se encuentra el servicio KerberosAdmin está defectuoso o el servicio SlapdServer no está disponible. Durante la recuperación del servicio KerberosAdmin, intente las siguientes operaciones:

1. Compruebe si el nodo donde se encuentra el servicio KerberosAdmin es defectuoso.
2. Compruebe si el servicio SlapdServer no está disponible.

Disponibilidad del servicio KerberosServer

Indicador: Disponibilidad del servicio KerberosServer

Descripción: El sistema comprueba el estado del servicio KerberosServer. Si el resultado de la comprobación es anormal, el servicio KerberosServer no está disponible.

Guía de recuperación: Si el resultado de la comprobación del indicador es anormal, la causa posible es que el nodo donde se encuentra el servicio KerberosServer está defectuoso o el servicio SlapdServer no está disponible. Durante la recuperación del servicio KerberosServer, intente las siguientes operaciones:

1. Compruebe si el nodo donde se encuentra el servicio KerberosServer es defectuoso.
2. Compruebe si el servicio SlapdServer no está disponible.

Estado de salud del servicio

Indicador: Estado del servicio

Descripción: El sistema comprueba el estado del servicio KrbServer. Si el resultado de la comprobación es anormal, el servicio KrbServer no está disponible.

Guía de recuperación: Si el resultado de la comprobación del indicador es anormal, la causa posible es que el nodo donde reside el servicio KrbServer está defectuoso o el servicio LdapServer no está disponible. Para obtener más información, consulte el procedimiento de manipulación de ALM-25500.

Comprobación de alarma

Indicador: Información de alarma

Descripción: Este indicador se utiliza para comprobar la información de alarma sobre el servicio KrbServer. Si existen alarmas, el servicio KrbServer puede ser anormal.

Guía de recuperación: Si el resultado de la comprobación del indicador es anormal, consulte el documento de alarma relacionado para manejar las alarmas.

8.8.13 Indicadores de comprobación de estado de LdapServer

Disponibilidad del servicio de SlapdServer

Indicador: Disponibilidad del servicio de SlapdServer

Descripción: El sistema comprueba el estado del servicio de SlapdServer. Si el estado es anormal, el servicio SlapdServer no está disponible.

Guía de recuperación: Si el resultado de la comprobación del indicador es anormal, la causa posible es que el nodo donde se encuentra el servicio SlapdServer está defectuoso o el proceso SlapdServer está defectuoso. Durante la recuperación del servicio SlapdServer, intente las siguientes operaciones:

1. Compruebe si el nodo donde se encuentra el servicio SlapdServer es defectuoso. Para más detalles, véase ALM-12006.
2. Compruebe si el proceso SlapdServer es normal. Para más detalles, véase ALM-12007.

Estado de salud del servicio

Indicador: Estado del servicio

Descripción: Este indicador se utiliza para comprobar la información de alarma sobre el servicio LdapServer. Si el estado es anormal, el servicio LdapServer no está disponible.

Guía de recuperación: Si el resultado de la comprobación del indicador es anormal, la causa posible es que el nodo donde reside el servicio LdapServer activo es defectuoso o el proceso LdapServer activo es defectuoso. Para obtener más información, consulte ALM-25000.

Comprobación de alarma

Indicador: Información de alarma

Descripción: Este indicador se utiliza para comprobar la información de alarma sobre el servicio LdapServer. Si existen alarmas, el servicio LdapServer puede ser anormal.

Guía de recuperación: Si el resultado de la comprobación del indicador es anormal, consulte el documento de alarma relacionado para manejar las alarmas.

8.8.14 Indicadores de comprobación de estado del Loader

Estado de salud de ZooKeeper

Indicator: Estado de salud de ZooKeeper

Description: Este indicador se utiliza para comprobar si el estado de salud del ZooKeeper es normal. Si el estado es anormal, el servicio ZooKeeper no está sano.

Guía de recuperación: Si este indicador es anormal, puede corregir la falla consultando la guía de manejo de alarmas.

Estado de salud de HDFS

Indicator: Estado de salud de HDFS

Description: Este indicador se utiliza para comprobar si el estado de salud de HDFS es normal. Si el estado es anormal, el servicio no está sano.

Guía de recuperación: Si este indicador es anormal, puede corregir la falla consultando la guía de manejo de alarmas.

Estado de salud de DBService

Indicator: Estado de salud de DBService

Description: Este indicador se utiliza para comprobar si el estado de mantenimiento de DBService es normal. Si el estado es anormal, el servicio DBService no está bien.

Guía de recuperación: Si este indicador es anormal, puede corregir la falla consultando la guía de manejo de alarmas.

Estado de salud de Yarn

Indicator: Estado de salud de Yarn

Description: Este indicador se utiliza para comprobar si el estado de salud de Yarn es normal. Si el estado es anormal, el servicio no está sano.

Guía de recuperación: Si este indicador es anormal, puede corregir la falla consultando la guía de manejo de alarmas.

Estado de salud de MapReduce

Indicator: Estado de salud de MapReduce

Descripción: Este indicador se utiliza para comprobar si el estado de salud del MapReduce es normal. Si el estado es anormal, el servicio MapReduce no está sano.

Guía de recuperación: Si este indicador es anormal, puede corregir la falla consultando la guía de manejo de alarmas.

Estado del proceso del Loader

Indicator: Estado del proceso del Loader

Description: Este indicador se utiliza para comprobar si el proceso del Loader es normal. Si el estado es anormal, el servicio no está sano.

Guía de recuperación: Si este indicador es anormal, puede corregir la falla consultando la guía de manejo de alarmas.

Estado de salud del servicio

Indicador: Estado del servicio

Descripción: Este indicador se utiliza para comprobar si el estado del servicio del cargador es normal. Si el estado es anormal, el servicio no está sano.

Guía de recuperación: Si este indicador es anormal, puede corregir la falla consultando la guía de manejo de alarmas.

Comprobación de alarma

Indicador: Información de alarma

Descripción: Este indicador se utiliza para comprobar si existen alarmas para loader. Si existen alarmas, el servicio no está sano.

Guía de recuperación: Si este indicador es anormal, puede corregir la falla consultando la guía de manejo de alarmas.

8.8.15 Indicadores de comprobación de estado de MapReduce

Estado de salud del servicio

Indicador: Estado del servicio

Descripción: Este indicador se utiliza para comprobar si el estado del servicio MapReduce es normal. Si el estado es anormal, el servicio no está sano.

Guía de recuperación: Si este indicador es anormal, puede corregir la falla consultando la guía de manejo de alarmas.

Comprobación de alarma

Indicador: Información de alarma

Descripción: Este indicador se utiliza para comprobar si existen alarmas. Si existen alarmas, el servicio no está sano.

Guía de recuperación: Si este indicador es anormal, puede corregir la falla consultando la guía de manejo de alarmas.

8.8.16 Indicadores de comprobación de estado de OMS

Comprobación de estado de OMS

Indicador: Comprobación del estado de OMS

Descripción: La comprobación de estado de OMS incluye la comprobación de estado de HA y la comprobación de estado de recursos. El estado HA incluye **active**, **standby** y **NULL** que indican el nodo activo, el nodo en espera y el desconocido, respectivamente. El estado del recurso incluye normal, anormal y NULL. Si el estado HA es NULL, el estado HA no está sano. Si el estado del recurso es NULL o anormal, el estado del recurso no es saludable.

Tabla 8-27 Descripción del estado de OMS

Nombre	Descripción
HA state	**active**: indica el nodo activo. **standby**: indica el nodo en espera. **NULL**: desconocido
Resource status	**normal**: Todos los recursos son normales. **abnormal**: indica que existen recursos anormales. **NULL**: desconocido

Guía de recuperación:

1. Inicie sesión en el nodo de gestión activo y ejecute el comando **su - omm** para cambiar a usuario **omm**. Ejecute el comando **${CONTROLLER_HOME}/sbin/status-oms.sh** para comprobar el estado de OMS.
2. Si el estado HA es NULL, el sistema puede estar reiniciando. NULL es un estado intermedio, y el estado HA cambiará automáticamente a un estado normal.
3. Si el estado del recurso es anormal, ciertos recursos de componentes del FusionInsight Manager son anormales. Compruebe si el estado de los componentes tales como acs, aos cep, controlador, feed_watchdog, fms, guassDB, httpd, iam, ntp, okerberos, oldap, pms, y el componente tomcat es normal.
4. Si algún recurso de componente de Manager es anormal, consulte comprobación de estado de componente de Manager para rectificar el error.

Comprobación del estado de los componentes de Manager

Indicador: Comprobación del estado de los componentes de Manager

Descripción: Este indicador se utiliza para comprobar el estado de ejecución y el estado de HA de los componentes de Manager. El estado de ejecución del recurso incluye **Normal** y **Abnormal** y el estado de HA del recurso incluye **Normal** y **Exception**. Los componentes del Manager incluyen Acs, Aos, Cep, Controller, feed_watchdog, Floatip, Fms, GaussDB, HeartBeatCheck, httpd, IAM, NTP, Okerberos, OLDAP, PMS, y Tomcat. Si el estado de ejecución y el estado HA no son Normal, el resultado de la comprobación no es saludable.

Tabla 8-28 Descripción del estado de Manager

Nombre	Descripción
Resource running status:	**Normal**: El sistema se está ejecutando correctamente. **Abnormal**: La ejecución es anormal. **Stopped**: La tarea se detiene. **Unknown**: El estado es desconocido. **Starting**: Se está iniciando el proceso. **Stopping**: La tarea se está deteniendo. **Active_normal**: El nodo activo se está ejecutando correctamente. **Standby_normal**: El nodo en espera se está ejecutando correctamente. **Raising_active**: El nodo está siendo promovido para ser el nodo activo. **Lowing_standby**: El nodo se está configurando para que sea el nodo en espera. **No_action**: la acción no existe. **Repairing**: Se está reparando el disco. **NULL**: desconocido
Resource HA status	**Normal**: el estado es normal. **Exception**: indica una falla. **Non_steady**: indica el estado no estable. **Unknown**: desconocido **NULL**: desconocido

Guía de recuperación:

1. Inicie sesión en el nodo de gestión activo y ejecute el comando **su - omm** para cambiar a usuario **omm**. Ejecute el comando **${CONTROLLER_HOME}/sbin/status-oms.sh** para comprobar el estado de OMS.
2. Si floteip, okerberos y oldap son anormales, maneje los problemas con referencia a ALM-12002, ALM-12004 y ALM-12005 respectivamente.
3. Si otros recursos son anormales, se recomienda ver los registros de los módulos defectuosos.

   Si los recursos del controlador son anormales, vea **/var/log/Bigdata/controller/controller.log** del nodo defectuoso.

   Si los recursos de CEP son anormales, vea **/var/log/Bigdata/controller/controller.log** del nodo defectuoso.

   Si los recursos AOS son anormales, vea **/var/log/Bigdata/controller/aos/aos.log** del nodo defectuoso.

   Si los recursos feed_watchdog son anormales, vea el **/var/log/Bigdata/watchdog/watchdog.log** del nodo anormal.

Si los recursos de HTTPD son anormales, vea **/var/log/Bigdata/httpd/error_log** del nodo anormal.

Si los recursos de FMS son anormales, vea **/var/log/Bigdata/omm/oms/fms/fms.log** del nodo anormal.

Si los recursos de PMS son anormales, vea **/var/log/Bigdata/omm/oms/pms/pms.log** del nodo anormal.

Si los recursos de IAM son anormales, vea **/var/log/Bigdata/omm/oms/iam/iam.log** del nodo anormal.

Si el recurso de GaussDB es anormal, compruebe el **/var/log/Bigdata/omm/oms/db/omm_gaussdba.log** del nodo anormal.

Si los recursos NTP son anormales, vea **/var/log/Bigdata/omm/oms/ha/scriptlog/ha_ntp.log** del nodo anormal.

Si los recursos de Tomcat son anormales, vea **/var/log/Bigdata/tomcat/catalina.log** del nodo anormal.

4. Si la falla no se puede corregir en función de los registros, póngase en contacto con el personal de O&M y envíe los registros de fallas recopiladas.

Estado de ejecución de OMA

Indicador: Estado de ejecución de OMA

Descripción: Este indicador se utiliza para comprobar el estado de funcionamiento del OMA. El estado puede ser **Running** o **Stopped**. Si el OMA es de **Stopped**, el OMA no es saludable.

Guía de recuperación:

1. Inicie sesión en el nodo no saludable y ejecute el comando **su - omm** para cambiar a usuario **omm**.
2. Ejecute **${OMA_PATH}/restart_oma_app** para iniciar manualmente el OMA y vuelva a comprobarlo. Si el resultado de la comprobación sigue siendo poco saludable, vaya a **3**.
3. Si el inicio manual de OMA no puede resolver el problema, se recomienda comprobar los registros de OMA en **/var/log/Bigdata/omm/oma/omm_agent.log**.
4. Si la falla no se puede corregir en función de los registros, póngase en contacto con el personal de O&M y envíe los registros de fallas recopiladas.

Confianza de SSH entre cada nodo y el nodo de gestión activa

Indicador: Confianza SSH entre cada nodo y el nodo de gestión activa

Descripción: Este indicador se utiliza para comprobar si la confianza mutua de SSH es normal. Si puede cambiar a otro nodo a través de SSH desde el nodo de OMS activo como usuario omm sin necesidad de introducir la contraseña, la comunicación SSH es normal. De lo contrario, la comunicación SSH es anormal. Además, si puede cambiar a otro nodo a través de SSH desde el nodo de OMS activo, pero no puede cambiar al nodo de OMS activo desde los otros nodos, la comunicación de SSH es anormal.

Guía de recuperación:

1. Si el resultado de la comprobación del indicador es anormal, las relaciones de confianza de SSH entre los nodos y el nodo de gestión activo son anormales. En este caso, compruebe si el permiso del directorio **/home/omm** es **omm**. Si los usuarios no-omm tienen el permiso de directorio, la relación de confianza SSH puede ser anormal. Se

recomienda ejecutar **chown omm:wheel** para modificar el permiso y volver a comprobarlo. Si el permiso en el directorio **/home/omm** es normal, vaya a **2**.

2. La excepción de relación de confianza SSH puede causar excepciones de latidos entre el Controller y NodeAgent, lo que resulta en alarmas de falla de nodo. En este caso, rectificar la falla haciendo referencia al procedimiento de manipulación de ALM-12006.

Tiempo de ejecución del proceso

Indicador: Tiempo de ejecución de NodeAgent y Tomcat

Descripción: Este indicador se utiliza para comprobar el tiempo de ejecución de los procesos NodeAgent, Controller, y Tomcat. Si el tiempo es inferior a media hora (1,800s), el proceso puede haber sido reiniciado. Se recomienda comprobar el proceso después de media hora. Si los resultados de comprobación múltiple indican que el proceso se ejecuta durante menos de media hora, el proceso es anormal.

Guía de recuperación:

1. Inicie sesión en el nodo no saludable y ejecute el comando **su - omm** para cambiar a usuario **omm**.
2. Ejecute el siguiente comando para comprobar el PID basado en el nombre del proceso:

   ps -ef | grep NodeAgent
3. Ejecute el siguiente comando para comprobar el tiempo de inicio del proceso basado en el PID:

   ps -p pid -o lstart
4. Compruebe si la hora de inicio del proceso es normal. Si el proceso se reinicia repetidamente, vaya a **5**.
5. Vea los registros relacionados y analice las causas de reinicio.

   Si el tiempo de ejecución de NodeAgent es anormal, marque **/var/log/Bigdata/NodeAgent/agentlog/agent.log**.

   Si el tiempo de ejecución del Controller es anormal, compruebe el archivo **/var/log/Bigdata/controller/controller.log**.

   Si el tiempo de ejecución de Tomcat es anormal, compruebe el archivo **/var/log/Bigdata/tomcat/web.log**.
6. Si la falla no se puede corregir en función de los registros, póngase en contacto con el personal de O&M y envíe los registros de fallas recopiladas.

Comprobación de vencimiento de cuenta y contraseña

Indicador: Comprobación de vencimiento de cuenta y contraseña

Descripción: Este indicador comprueba los dos usuarios del sistema operativo **omm** y **ommdba** de MRS. Para los usuarios del sistema operativo, se debe comprobar el tiempo de caducidad de la cuenta y la contraseña. Si el período de validez de la cuenta o contraseña no es superior a 15 días, la cuenta es anormal.

Guía de recuperación: Si el período de validez de la cuenta o contraseña es inferior o igual a 15 días, póngase en contacto con el personal de O&M.

8.8.17 Indicadores de comprobación de estado de Spark

Estado de salud del servicio

Indicador: Estado del servicio

Description: Este indicador se utiliza para comprobar si el estado del servicio de Spark es normal. Si el estado es anormal, el servicio no está sano.

Recovery Guide: Si el indicador es anormal, rectifique la falla con referencia a ALM-28001.

Comprobación de alarma

Indicador: Información de alarma

Descripción: Este indicador se utiliza para comprobar si existen alarmas. Si existen alarmas, el servicio no está sano.

Guía de recuperación: Si este indicador es anormal, puede corregir la falla consultando la guía de manejo de alarmas.

8.8.18 Indicadores de comprobación de estado de Storm

Número de nodos de trabajo

Indicador: Número de Supervisores

Descripción: Este indicador se utiliza para comprobar el número de Supervisores disponibles en un clúster. Si el número de Supervisores disponibles en un clúster es menor que 1, el clúster no está en buen estado.

Guía de recuperación: Si el indicador es anormal, vaya a la página de instancia de servicio de streaming y haga clic en el nombre de host de la instancia de Supervisor no disponible. Vea el estado del host en el área **Overview**. Si el estado de salud del host es de **Good**, rectifique la falla haciendo referencia a ALM-12007 Fallas de proceso. Si el estado no es **Good**, rectifique la falla haciendo referencia al procedimiento de manejo de ALM-12006 Fallas de nodo.

Número de ranuras inactivas

Indicador: Número de ranuras inactivas

Descripción: Este indicador se utiliza para comprobar el número de ranuras inactivas en un clúster. Si el número de ranuras inactivas en un clúster es menor que 1, el clúster no está sano.

Guía de recuperación: Si el indicador es anormal, vaya a la página de instancia de servicio Storm y compruebe el estado de salud de la instancia Supervisor. Si el estado de salud de todas las instancias de Supervisor es **Good**, debe ampliar la capacidad del nodo de Core en el clúster. Si no es así, rectifique la falla haciendo referencia a ALM-12007 Fallas de proceso.

Estado de salud del servicio

Indicador: Estado del servicio

Descripción: Este indicador se utiliza para comprobar si el estado del servicio Storm es normal. Si el estado es anormal, el servicio no está sano.

Guía de recuperación: Si el indicador es anormal, rectifique la falla haciendo referencia a la alarma "ALM-26051 Storm Service No Disponible".

Comprobación de alarma

Indicador: Información de alarma

Descripción: Este indicador se utiliza para comprobar si existen alarmas. Si existen alarmas, el servicio no está sano.

Guía de recuperación: Si este indicador es anormal, puede corregir la falla consultando la guía de manejo de alarmas.

8.8.19 Indicadores de comprobación de la salud de Yarn

Estado de salud del servicio

Indicador: Estado del servicio

Descripción: Este indicador se utiliza para comprobar si el estado del servicio de Yarn es normal. Si no se puede obtener el número de nodos de NodeManager, el sistema no está sano.

Guía de recuperación: Si este indicador es anormal, puede manejar la alarma consultando la guía de manejo de alarmas y asegurarse de que la red es normal.

Comprobación de alarma

Indicador: Información de alarma

Descripción: Este indicador se utiliza para comprobar si existen alarmas. Si existen alarmas, el servicio no está sano.

Guía de recuperación: Si este indicador es anormal, puede corregir la falla consultando la guía de manejo de alarmas.

8.8.20 Indicadores de comprobación de estado de ZooKeeper

Latencia promedio de procesamiento de solicitudes de ZooKeeper

Indicador: Latencia promedio de procesamiento de solicitudes de servicio de ZooKeeper

Descripción: Este indicador se utiliza para comprobar el retraso promedio para que el servicio ZooKeeper procese las solicitudes. Si el retraso promedio es superior a 300 ms, el servicio ZooKeeper no está sano.

Guía de recuperación: Si el indicador es anormal, compruebe si la velocidad de red del clúster es normal y si el uso de memoria o CPU es demasiado alto.

Uso de conexiones de ZooKeeper

Indicador: Uso de conexiones de ZooKeeper

Descripción: Este indicador se utiliza para comprobar si el uso de memoria de ZooKeeper supera el 80%. Si el uso del disco excede el umbral, el sistema no está sano.

Guía de recuperación: Si el indicador es anormal, se recomienda aumentar la memoria disponible para el servicio ZooKeeper. El método para aumentar la memoria es el siguiente:

Aumentar el valor de **-Xmx** en el elemento de configuración **GC_OPTS** del servicio ZooKeeper. Después de la modificación, reinicie el servicio ZooKeeper para que la configuración surta efecto.

Estado de salud del servicio

Indicador: Estado del servicio

Descripción: Este indicador se utiliza para comprobar si el estado del servicio de ZooKeeper es normal. Si el estado es anormal, el servicio no está sano.

Guía de recuperación: Si el indicador es anormal, compruebe si el estado de salud de los servicios KrbServer y LdapServer es defectuoso. De ser así, rectifique la falla. Inicie sesión en el cliente de ZooKeeper, compruebe si la escritura de datos de ZooKeeper falla. En caso afirmativo, busque la causa de la falla basándose en el mensaje de error y maneje la falla de acuerdo con el mensaje de error. Rectifique la falla siguiendo el procedimiento para el manejo de ALM-13000.

Comprobación de alarma

Indicador: Información de alarma

Descripción: Este indicador se utiliza para comprobar si existen alarmas. Si existen alarmas, el servicio no está sano.

Guía de recuperación: Si este indicador es anormal, puede corregir la falla consultando la guía de manejo de alarmas.

8.9 Gestión de grupo de servicio estático

8.9.1 Consulta del estado de un grupo de servicios estático

Escenario

MRS Manager gestiona y aísla los recursos de servicio que no se ejecutan en YARN a través del grupo de recursos de servicio estático. Gestiona dinámicamente el total de recursos de CPU, E/S y memoria que HDFS y YARN pueden utilizar en el nodo de despliegue. El sistema admite el ajuste automático basado en el tiempo de los grupos de recursos de servicio estático. Esto permite que el clúster ajuste automáticamente los valores de los parámetros en diferentes períodos para garantizar una utilización más eficiente de los recursos.

En MRS Manager, puede ver las métricas de monitoreo de los recursos utilizados por cada servicio en el grupo de servicios estático. Las métricas de monitoreo son las siguientes:

- Uso total de CPU del servicio
- Velocidad total de lectura de E/S de disco del servicio
- Velocidad total de escritura de E/S del disco del servicio
- Uso total de memoria del servicio

Procedimiento

Paso 1 En MRS Manager, haga clic en **System**. En el área **Resource**, haga clic en **Configure Static Service Pool**.

Paso 2 Haga clic en **Status**.

Paso 3 Compruebe los valores base del ajuste de recursos del sistema.

- **System Resource Adjustment Base** indica el volumen máximo de recursos que puede utilizar cada nodo del clúster. Si un nodo solo tiene un servicio, el servicio ocupa exclusivamente los recursos disponibles en el nodo. Si un nodo tiene varios servicios, todos los servicios comparten los recursos disponibles en el nodo.
- **CPU(%)** indica el número máximo de CPUs que pueden utilizar los servicios en un nodo.
- **Memory(%)** indica la memoria máxima que pueden utilizar los servicios en un nodo.

Paso 4 Compruebe el uso de recursos del servicio de clúster.

En el área del gráfico, seleccione **All services** en el cuadro de lista desplegable del servicio. Se muestra el estado de uso de recursos de todos los servicios del grupo de servicios.

NOTA

Effective Configuration Group indica el grupo de configuración de control de recursos utilizado por el servicio de clúster. De forma predeterminada, el grupo de configuración **default** se utiliza en todo momento todos los días, lo que indica que el servicio de clúster puede utilizar todas las CPU y 70% de memoria del nodo.

Paso 5 Vea el uso de recursos de un solo servicio.

En el área del gráfico, seleccione un servicio en el cuadro de lista desplegable de servicios. Se muestra el estado de uso de recursos del servicio.

Paso 6 Puede establecer el intervalo para actualizar automáticamente la página.

Se admiten las siguientes opciones de intervalo de actualización:

- **Refresh every 30 seconds**
- **Refresh every 60 seconds**
- **Stop refreshing**

Paso 7 En el área **Period**, seleccione un intervalo de tiempo para ver los recursos de servicio. Las opciones son las siguientes:

- Real time
- Last 3 hours
- Last 6 hours
- Last 24 hours
- Last week
- Last month
- Last 3 months
- Last 6 months
- Personalizar: Si selecciona esta opción, puede personalizar el período de visualización de los datos de monitoreo.

Paso 8 Haga clic en **View** para ver los datos de recursos de servicio en el intervalo de tiempo correspondiente.

Paso 9 Personalice un informe de recursos de servicio.

1. Haga clic en **Customize** y seleccione los indicadores de origen de servicio que se mostrarán.
   - Velocidad total de lectura de E/S de disco del servicio
   - Uso total de memoria del servicio
   - Velocidad total de escritura de E/S del disco del servicio
   - Uso total de CPU del servicio
2. Haga clic en **OK** para guardar las métricas de monitoreo seleccionadas para mostrarlas.

   NOTA

   Haga clic en **Clear** para cancelar todas las métricas de monitoreo seleccionadas en un lote.

Paso 10 Exportar un informe de monitoreo.

Haga clic en **Export**. MRS Manager generará un informe sobre los recursos de servicio seleccionados en un período de tiempo especificado. Guarde el informe.

NOTA

Para ver los gráficos de curvas de las métricas de monitoreo en un período especificado, haga clic en **View**.

----Fin

8.9.2 Configuración de un grupo de servicio estático

Escenario

Si necesita controlar los recursos de nodo que puede utilizar el servicio de clúster o el uso de CPU del nodo que utiliza el clúster en diferentes períodos de tiempo, puede ajustar la base de recursos en MRS Manager y personalizar los grupos de configuración de recursos.

Prerrequisitos

- Después de configurar el grupo de servicios estático, los servicios HDFS y YARN deben reiniciarse. Durante el reinicio, los servicios no están disponibles.
- Después de configurar un grupo de servicios estático, el número máximo de recursos utilizados por cada instancia de servicio e rol no puede exceder el límite superior.

Procedimiento

Paso 1 Modifique la base de ajuste de recursos del sistema.

1. En MRS Manager, haga clic en **System**. En el área **Resource**, haga clic en **Configure Static Service Pool**.
2. Haga clic en **Configuration**. Se muestra la página de gestión del grupo de configuración del grupo de servicios.
3. En el área **System Resource Adjustment Base**, cambie los valores de **CPU(%)** y **Memory(%)**.

La modificación de **System Resource Adjustment Base** limita el porcentaje máximo de recursos físicos de CPU y memoria de los nodos que pueden utilizar los servicios Flume, HBase, HDFS, Impala y YARN. Si se despliegan varios servicios en el mismo nodo, el uso máximo de recursos físicos de todos los servicios no puede exceder el uso ajustado de CPU o memoria.

4. Haga clic en **Next**.

   Si necesita modificar los parámetros de nuevo, haga clic en **Previous** en la parte inferior de la página.

Paso 2 Modifique el grupo de configuración **default** del grupo de servicios.

1. En la tabla **Service Pool Configuration**, establezca **CPU LIMIT(%)**, **CPU SHARE(%)**, **I/O(%)** y **Memory(%)** para los servicios Flume, HBase, HDFS, Impala y YARN.

   NOTA

   - La suma de **CPU LIMIT(%)** utilizados por todos los servicios puede superar el 100%.
   - La suma de **CPU SHARE(%)** y **I/O(%)** utilizados por todos los servicios debe ser del 100%. Por ejemplo, si se asignan recursos de CPU a los servicios HDFS y Yarn, el total de recursos de CPU asignados a los dos servicios es del 100%.
   - La suma de **Memory(%)** utilizados por todos los servicios puede ser mayor, menor o igual al 100%.
   - **Memory(%)** no puede tener efecto dinámicamente y solo se puede modificar en el grupo de configuración predeterminado.

2. Haga clic en el área en blanco de la página para completar la edición. MRS Manager genera los valores correctos de los parámetros del grupo de servicios en el área **Detailed Configuration** basándose en los recursos de hardware del clúster y la información de asignación.

3. Puede hacer clic en a la derecha de **Detailed Configuration** para modificar los valores de parámetros del grupo de servicios en función de los requisitos de servicio.

   En el área **Service Pool Configuration**, haga clic en el nombre del servicio especificado. El área **Detailed Configuration** muestra solo los parámetros del servicio. El cambio manual de los valores de los parámetros no actualiza el uso de los recursos de servicio. En los grupos de configuración agregados, se mostrarán los números de grupo de configuración de los parámetros que tienen efecto dinámicamente. Por ejemplo, **HBase: RegionServer: dynamic-config1.RES_CPUSET_PERCENTAGE**. Las funciones de parámetro no cambian.

Tabla 8-29 Parámetros del grupo de servicios estático

Parámetro	Descripción
– RES_CPUSET_PERCENTAGE – dynamic-configX.RES_CPUSET_PERCENTAGE	Configura el porcentaje de CPU del servicio.
– RES_CPU_SHARE – dynamic-configX.RES_CPU_SHARE	Configura el recurso compartido de CPU del servicio.

Parámetro	Descripción
– RES_BLKIO_WEIGHT – dynamic-configX.RES_BLKIO_WEIGHT	Configura el uso de E/S del servicio.
HBASE_HEAPSIZE	Configura la memoria JVM máxima para RegionServer.
HADOOP_HEAPSIZE	Configura la memoria JVM máxima de un DataNode.
yarn.nodemanager.resource.memory-mb	Configura la memoria que puede utilizar NodeManager en el nodo actual.
dfs.datanode.max.locked.memory	Configura la memoria máxima que puede utilizar un DataNode como caché de HDFS.
FLUME_HEAPSIZE	Configura la memoria JVM máxima que puede utilizar cada instancia de Flume.
IMPALAD_MEM_LIMIT	Configura la memoria máxima que puede utilizar una instancia de Impalad.

Paso 3 Agregar un grupo de configuración de recursos personalizado.

1. Determine si se debe ajustar automáticamente las configuraciones de recursos en función del tiempo.

   En caso afirmativo, vaya a **Paso 3.2**.

   Si no, vaya a **Paso 4**.

2. Haga clic en para agregar un grupo de configuración de recursos. En el área **Scheduling Time**, haga clic en . Se muestra la página de configuración de la política de tiempo.

   Modifique los siguientes parámetros en función de los requisitos de servicio y haga clic en **OK**.

   – **Repeat**: Si se selecciona, el grupo de configuración de recursos se ejecuta repetidamente en función del período de programación. Si no está seleccionado, establezca la fecha y la hora en que se puede aplicar la configuración del grupo de recursos.

   – **Repeat Policy**: se puede establecer en **Daily**, **Weekly** y **Monthly**. Este parámetro sólo es válido cuando se selecciona **Repeat**.

   – **Between**: indica el período de tiempo entre la hora de inicio y la hora de finalización cuando se aplica la configuración de recursos. Establezca un rango de tiempo único. Si el intervalo de tiempo se superpone con el de un grupo existente de configuración de recursos, el intervalo de tiempo no se puede guardar. Este parámetro sólo es válido cuando se selecciona **Repeat**.

NOTA

- El grupo **default** de configuración de recursos tiene efecto en todos los segmentos de tiempo indefinidos.
- El grupo de recursos recién agregado es un conjunto de parámetros que tiene efecto dinámicamente en un intervalo de tiempo especificado.
- El grupo de recursos recién agregado se puede eliminar. Se puede agregar un máximo de cuatro grupos de configuración de recursos que tengan efecto dinámicamente.
- Seleccione una política de repetición. Si la hora de finalización es anterior a la hora de inicio, el día siguiente se etiqueta de forma predeterminada. Por ejemplo, si un período de validez oscila entre las 22:00 y las 06:00, la configuración de recursos personalizada tiene efecto entre las 22:00 del día actual y las 06:00 del día siguiente.
- Si los tipos de políticas de repetición de varios grupos de configuración son diferentes, los intervalos de tiempo pueden superponerse. Los tipos de política se enumeran de la siguiente manera por prioridad de menor a mayor: diario, semanal y mensual. Lo siguiente es un ejemplo. Hay dos grupos de configuración de recursos que utilizan las políticas mensuales y diarias, respectivamente. Sus intervalos de tiempo de aplicación en un día se superponen de la siguiente manera: [04:00 a 07:00] y [06:00 a 08:00]. En este caso, prevalece la configuración del grupo que utiliza la política mensual.
- Si los tipos de políticas de repetición de varios grupos de configuración de recursos son los mismos, los intervalos de tiempo de diferentes fechas pueden superponerse. Por ejemplo, si hay dos grupos de programación semanales, puede establecer el mismo intervalo de tiempo en un día diferente para ellos, como de 04:00 a 07:00, el lunes y el miércoles, respectivamente.

3. En la página **Service Pool Configuration**, modifique la configuración de recursos de cada servicio. Haga clic en el área en blanco de la página para completar la edición y vaya a **Paso 4**.

   Puede hacer clic en a la derecha de **Service Pool Configuration** para modificar los parámetros. Haga clic en en el área **Detailed Configuration** para actualizar manualmente los valores de parámetros generados por el sistema en función de los requisitos de servicio.

Paso 4 Guarda la configuración.

Haga clic en **Save**. En el cuadro de diálogo **Save Configuration**, seleccione **Restart the affected services or instances**. Haga clic en **OK** para guardar la configuración y reiniciar los servicios relacionados.

Se muestra **Operation succeeded**. Haga clic en **Finish**. El servicio se inicia correctamente.

----Fin

8.10 Gestión de tenants

8.10.1 Descripción

Definición

Un clúster de MRS proporciona varios recursos y servicios para que compartan varias organizaciones, departamentos o aplicaciones. El clúster proporciona tenants como entidad lógica para usar estos recursos y servicios. Un modo que involucra diferentes tenants se llama modo multitenant. Actualmente, solo el clúster de análisis admite la gestión de tenant.

Principios

El clúster de MRS proporciona la función multitenant. Soporta un modelo de tenant por capas y permite agregar o eliminar tenants dinámicos para aislar recursos. Gestiona y configura dinámicamente los recursos informáticos y de almacenamiento de tenants.

Los recursos informáticos indican los recursos de cola de tareas de Yarn de tenants. La cuota de cola de tareas se puede modificar y se pueden ver el estado de uso y las estadísticas de la cola de tareas.

Los recursos de almacenamiento se pueden almacenar en HDFS. Puede agregar y eliminar los directorios de almacenamiento HDFS de tenants y establecer las cuotas de cantidad de archivos y el espacio de almacenamiento de los directorios.

Como plataforma unificada de gestión de tenant de clústeres MRS, MRS Manager proporciona a las empresas modelos de gestión de múltiples tenants probados en el tiempo, lo que permite la gestión centralizada de tenant y servicio. Los tenants pueden crear y gestionar tenants en un clúster según los requisitos de servicio.

- Los roles, los recursos informáticos y los recursos de almacenamiento se crean automáticamente cuando se crean los tenants. De forma predeterminada, todos los permisos de los nuevos recursos informáticos y de almacenamiento se asignan a los roles de un tenant.
- Los permisos para ver los recursos del tenant actual, agregar un subtenant y gestionar los recursos del subtenant se otorgan a los roles del tenant de forma predeterminada.
- Después de modificar los recursos informáticos o de almacenamiento de tenant, los permisos de las funciones de tenant se actualizan automáticamente.

MRS Manager admite un máximo de 512 tenants. Los tenants que se crean de forma predeterminada en el sistema contienen **default**. Los tenants que están en la capa superior con el tenant por defecto se denominan tenants de nivel 1.

Grupos de recursos

Las colas de tareas de Yarn sólo admiten la política de programación basada en etiquetas. Esta política permite que las colas de tareas de Yarn asocien NodeManagers que tienen etiquetas de nodo específicas. De esta manera, las tareas de Yarn se ejecutan en nodos especificados para que las tareas se planifiquen y se utilicen ciertos recursos de hardware. Por ejemplo, las tareas de Yarn que requieren una gran capacidad de memoria pueden ejecutarse en nodos con una gran capacidad de memoria por medio de la asociación de etiquetas, evitando un rendimiento de servicio deficiente.

En un clúster MRS, el tenant divide lógicamente los nodos del clúster de Yarn para combinar múltiples NodeManagers en un grupo de recursos. Las colas de tareas de Yarn se pueden asociar a grupos de recursos especificados mediante la configuración de políticas de capacidad de cola, lo que garantiza una utilización eficiente e independiente de los recursos en los grupos de recursos.

MRS Manager admite un máximo de 50 grupos de recursos. El sistema tiene un grupo de recursos **Default**.

8.10.2 Creación de un tenant

Escenario

Puede crear un tenant en MRS Manager para especificar el uso de recursos.

Prerrequisitos

- Se ha planeado un nombre de tenant. El nombre no debe ser el mismo que el de un rol o una cola de Yarn que exista en el clúster actual.
- Si un tenant requiere recursos de almacenamiento, se planificó un directorio de almacenamiento en función de los requisitos de servicio y el directorio planificado no existe en el directorio HDFS.
- Los recursos que se pueden asignar al tenant actual han sido planificados y la suma de los porcentajes de recursos de subtenants directos bajo el tenant principal en cada nivel no supera el 100%.

Procedimiento

Paso 1 En MRS Manager, haga clic en **Tenant**.

Paso 2 Haga clic en **Create Tenant**. En la página que se muestra, configure las propiedades de tenant.

Tabla 8-30 Parámetros del tenant

Parámetro	Descripción
Name	Especifica el nombre del tenant actual. El valor consta de 1 a 20 caracteres y puede contener letras, números y guiones bajos (_).
Tenant Type	Las opciones incluyen **Leaf** y **Non-leaf**. Si se selecciona **Leaf**, el tenant actual es un tenant hoja y no se puede agregar ningún subtenant. Si se selecciona **Non-leaf**, se pueden agregar subtenants al tenant actual.
Dynamic Resources	Especifica los recursos de cálculo dinámicos para el tenant actual. El sistema crea automáticamente una cola de tareas con el nombre del tenant en Yarn. Cuando los recursos dinámicos no son **Yarn**, el sistema no crea automáticamente una cola de tareas.
Default Resource Pool Capacity (%)	Especifica el porcentaje de los recursos informáticos utilizados por el tenant actual en el grupo de recursos **default**.
Default Resource Pool Max. Capacity (%)	Especifica el porcentaje máximo de los recursos informáticos utilizados por el tenant actual en el grupo de recursos **default**.

Parámetro	Descripción
Storage Resource	Especifica los recursos de almacenamiento para el tenant actual. El sistema crea automáticamente una carpeta de archivos con el nombre de tenant en el directorio **/tenant**. Cuando se crea un tenant por primera vez, el sistema crea automáticamente el directorio **/tenant** en el directorio raíz HDFS. Si los recursos de almacenamiento no son **HDFS**, el sistema no crea un directorio de almacenamiento bajo el directorio raíz de HDFS.
Space Quota (MB)	Especifica la cuota de espacio de almacenamiento de HDFS utilizada por el tenant actual. El valor oscila entre **1** y **8796093022208**. La unidad es MB. Este parámetro indica el espacio de almacenamiento de HDFS máximo que puede utilizar un tenant, pero no indica el espacio real utilizado. Si el valor es mayor que el tamaño del disco físico HDFS, el espacio máximo disponible es el espacio completo del disco físico oHDFS. **NOTA** Para garantizar la confiabilidad de los datos, se genera automáticamente una copia de un archivo cuando el archivo se almacena en HDFS. Es decir, se almacenan dos copias del mismo archivo de forma predeterminada. El espacio de almacenamiento de HDFS indica el espacio total en disco ocupado por todas estas copias. Por ejemplo, si el valor de **Storage Space Quota** se establece en **500**, el espacio real para almacenar archivos es de aproximadamente 250 MB (500/2 = 250).
Storage Path	Especifica el directorio de almacenamiento de HDFS del tenant. El sistema crea automáticamente una carpeta de archivos con el nombre del tenant en el directorio **/tenant** de forma predeterminada. Por ejemplo, el directorio de almacenamiento HDFS predeterminado para el **ta1** del tenant es **tenant/ta1**. Cuando se crea un tenant por primera vez, el sistema crea automáticamente el directorio **/tenant** en el directorio raíz HDFS. La ruta de almacenamiento es personalizable.
Service	Especifica otros recursos de servicio asociados con el tenant actual. HBase es compatible. Para configurar este parámetro, haga clic en **Associate Services**. En el cuadro de diálogo que se muestra, establezca **Service** en **HBase**. Si **Association Mode** se establece en **Exclusive**, los recursos de servicio se ocupan exclusivamente. Si se selecciona **share**, se comparten los recursos de servicio.
Description	Especifica la descripción del tenant actual.

Paso 3 Haga clic en **OK** para guardar la configuración.

Se tarda unos minutos en guardar la configuración. Si el **Tenant created successfully** se muestra en la esquina superior derecha, el tenant se agrega correctamente.

NOTA

- Los roles, los recursos informáticos y los recursos de almacenamiento se crean automáticamente cuando se crean los tenants.
- El nuevo rol tiene permisos sobre los recursos informáticos y de almacenamiento. El rol y sus permisos son controlados por el sistema automáticamente y no pueden ser controlados manualmente en **Manage Role**.
- Si desea utilizar el tenant, cree un usuario del sistema y asigne al usuario el rol Manager_tenant y el rol correspondiente al tenant. Para obtener más información, consulte **Creación de un usuario**.

----Fin

Tareas relacionadas

Ver un tenant agregado

Paso 1 En MRS Manager, haga clic en **Tenant**.

Paso 2 En la lista de tenant de la izquierda, haga clic en el nombre del tenant agregado.

La pestaña **Summary** se muestra a la derecha de forma predeterminada.

Paso 3 Vea **Basic Information**, **Resource Quota** y **Statistics** del tenant.

Si HDFS está en el estado **Stopped**, **Available** y **Used** de **Space** en **Resource Quota** son **unknown.**

----Fin

8.10.3 Creación de un subtenant

Escenario

Puede crear un subtenant en MRS Manager si los recursos del tenant actual necesitan ser asignados más.

Prerrequisitos

- Se ha agregado un tenant principal.
- Se ha planeado un nombre de tenant. El nombre no debe ser el mismo que el de un rol o una cola de Yarn que exista en el clúster actual.
- Si un subtenant requiere recursos de almacenamiento, se ha planificado un directorio de almacenamiento en función de los requisitos de servicio y el directorio planificado no existe en el directorio de almacenamiento del tenant principal.
- Los recursos que se pueden asignar al tenant actual han sido planificados y la suma de los porcentajes de recursos de subtenants directos bajo el tenant principal en cada nivel no supera el 100%.

Procedimiento

Paso 1 En MRS Manager, haga clic en **Tenant**.

Paso 2 En la lista de tenant de la izquierda, mueva el cursor al nodo de tenant al que se va a agregar un subtenant. Haga clic en **Create sub-tenant**. En la página mostrada, configure los atributos de subtenant de acuerdo con la siguiente tabla:

Tabla 8-31 Parámetros de subtenant

Parámetro	Descripción
Parent tenant	Especifica el nombre del tenant principal.
Name	Especifica el nombre del tenant actual. El valor consta de 1 a 20 caracteres y puede contener letras, números y guiones bajos (_).
Tenant Type	Las opciones incluyen **Leaf** y **Non-leaf**. Si se selecciona **Leaf**, el tenant actual es un tenant hoja y no se puede agregar ningún subtenant. Si se selecciona **Non-leaf**, se pueden agregar subtenants al tenant actual.
Dynamic Resources	Especifica los recursos de cálculo dinámicos para el tenant actual. El sistema crea automáticamente una cola de tareas con el nombre del subtenant en la cola principal de Yarn. Cuando los recursos dinámicos no son **Yarn**, el sistema no crea automáticamente una cola de tareas. Si el tenant principal no tiene recursos dinámicos, el subtenant no puede usar recursos dinámicos.
Default Resource Pool Capacity (%)	Especifica el porcentaje de recursos utilizados por el tenant actual. El valor base es el total de recursos del tenant principal.
Default Resource Pool Max. Capacity (%)	Especifica el porcentaje máximo de los recursos informáticos utilizados por el tenant actual. El valor base es el total de recursos del tenant principal.
Storage Resource	Especifica los recursos de almacenamiento para el tenant actual. El sistema crea automáticamente un archivo en el directorio de tenant principal de HDFS. El nombre del archivo es el mismo que el nombre del subtenant. Si los recursos de almacenamiento no son **HDFS**, el sistema no crea un directorio de almacenamiento bajo el directorio raíz de HDFS. Si el tenant principal no tiene recursos de almacenamiento, el subtenant no puede usar recursos de almacenamiento.

Parámetro	Descripción
Space Quota (MB)	Especifica la cuota de espacio de almacenamiento de HDFS utilizada por el tenant actual. El valor mínimo es 1, y el valor máximo es la cuota de almacenamiento total del tenant principal. La unidad es MB. Este parámetro indica el espacio de almacenamiento de HDFS máximo que puede utilizar un tenant, pero no indica el espacio real utilizado. Si el valor es mayor que el tamaño del disco físico HDFS, el espacio máximo disponible es el espacio completo del disco físico oHDFS. Si la cuota es mayor que la cuota del tenant principal, la capacidad de almacenamiento real está sujeta a la cuota del tenant principal. **NOTA** Para garantizar la confiabilidad de los datos, se genera automáticamente una copia de un archivo cuando el archivo se almacena en HDFS. Es decir, se almacenan dos copias del mismo archivo de forma predeterminada. El espacio de almacenamiento de HDFS indica el espacio total en disco ocupado por todas estas copias. Por ejemplo, si el valor se establece en **500**, el espacio real para almacenar archivos es de aproximadamente 250 MB (500/2 = 250).
Storage Path	Especifica el directorio de almacenamiento de HDFS del tenant. El sistema crea automáticamente una carpeta de archivos con el nombre del subtenant en el directorio del tenant principal de forma predeterminada. Por ejemplo, si el subtenant es **ta1s** y el directorio principal es **tenant/ta1**, el sistema establece este parámetro para el subtenant en **tenant/ta1/ta1s**. La ruta de almacenamiento se puede personalizar en el directorio principal. El directorio principal de la ruta de almacenamiento debe ser el directorio de almacenamiento del tenant principal.
Service	Especifica otros recursos de servicio asociados con el tenant actual. HBase es compatible. Para configurar este parámetro, haga clic en **Associate Services**. En el cuadro de diálogo que se muestra, establezca **Service** en **HBase**. Si **Association Mode** se establece en **Exclusive**, los recursos de servicio se ocupan exclusivamente. Si se selecciona **share**, se comparten los recursos de servicio.
Description	Especifica la descripción del tenant actual.

Paso 3 Haga clic en **OK** para guardar la configuración.

Se tarda unos minutos en guardar la configuración. Si el **Tenant created successfully** se muestra en la esquina superior derecha, el tenant se agrega correctamente. El tenant se crea con éxito.

NOTA

- Los roles, los recursos informáticos y los recursos de almacenamiento se crean automáticamente cuando se crean los tenants.
- El nuevo rol tiene permisos sobre los recursos informáticos y de almacenamiento. El rol y sus permisos son controlados por el sistema automáticamente y no pueden ser controlados manualmente en **Manage Role**.
- Cuando utilice este tenant, cree un usuario del sistema y asigne al usuario un rol de tenant relacionado. Para obtener más información, consulte **Creación de un usuario**.

----Fin

8.10.4 Eliminación de un tenant

Escenario

Puede eliminar un inquilino que no sea necesario en MRS Manager.

Prerrequisitos

- Se ha agregado un tenant.
- Ha comprobado si el tenant que se va a eliminar tiene subtenants. Si el tenant tiene subtenants, elimínelos; de lo contrario, no podrá eliminar el tenant.
- El rol del tenant que se va a eliminar no se puede asociar a ningún usuario o grupo de usuarios. Para obtener más información sobre cómo cancelar el enlace entre un rol y un usuario, consulte **Modificación de la información de usuario**.

Procedimiento

Paso 1 En MRS Manager, haga clic en **Tenant**.

Paso 2 En la lista de inquilinos de la izquierda, mueva el cursor hasta el nodo de tenant que se va a eliminar y haga clic en **Delete**.

Aparece el cuadro de diálogo **Delete Tenant**. Si desea guardar los datos del tenant, seleccione **Reserve the data of this tenant**. De lo contrario, se eliminará el espacio de almacenamiento del tenant.

Paso 3 Haga clic en OK para guardar la configuración.

Se tarda unos minutos en guardar la configuración. Una vez que el tenant se elimina correctamente, el rol y el espacio de almacenamiento del tenant también se eliminan.

NOTA

- Después de eliminar el tenant, la cola de tareas del tenant todavía existe en Yarn.
- Si decide no reservar datos al eliminar el tenant principal, también se eliminarán los datos de los subtenants si los subtenants utilizan recursos de almacenamiento.

----Fin

8.10.5 Gestión de directorio de tenant

Escenario

Puede gestionar el directorio de almacenamiento HDFS utilizado por un tenant específico en MRS Manager. Las operaciones de gestión incluyen agregar un directorio de tenant, modificar la cuota de archivo de directorio, modificar el espacio de almacenamiento y eliminar un directorio.

Prerrequisitos

Se ha agregado un tenant asociado con los recursos de almacenamiento de HDFS.

Procedimiento

- Ver un directorio de tenant
  a. En MRS Manager, haga clic en **Tenant**.
  b. En la lista de tenant de la izquierda, haga clic en el tenant de destino.
  c. Haga clic en la pestaña **Resource**.
  d. Vea la tabla **HDFS Storage**.
     - La columna Quota indica las cuotas de cantidad de archivos y directorios.
     - La columna **Storage Space Quota** indica el tamaño del espacio de almacenamiento del directorio del tenant.
- Adición de un directorio de tenant
  a. En MRS Manager, haga clic en **Tenant**.
  b. En la lista de tenant de la izquierda, haga clic en el tenant cuyo directorio de almacenamiento de HDFS debe agregarse.
  c. Haga clic en la pestaña **Resource**.
  d. En la tabla **HDFS Storage**, haga clic en **Create Directory**.
     - En **Parent Directory**, seleccione un directorio de almacenamiento de un tenant principal.

       Este parámetro sólo se aplica a los subtenants. Si el tenant principal tiene varios directorios, seleccione cualquiera de ellos.
     - Establezca **Path** en una ruta de directorio del tenant.

       NOTA

       - Si el tenant actual no es un subtenant, la nueva ruta se crea en el directorio raíz de HDFS.
       - Si el tenant actual es un subtenant, la nueva ruta se crea en el directorio especificado.

       Un directorio de almacenamiento de HDFS completo puede contener un máximo de 1,023 caracteres. Un nombre de directorio de HDFS contiene dígitos, letras, espacios y guiones bajos (_). El nombre no puede comenzar ni terminar con un espacio.
     - Establezca **Quota** en las cuotas de cantidad de archivos y directorios.

       Maximum Number of Files/Directories es opcional. Su valor oscila entre **1** y **9223372036854775806**.

- Establezca **Storage Space Quota** en el tamaño del espacio de almacenamiento del directorio del tenant.

  El valor de **Storage Space Quota** oscila entre **1** y **8796093022208**.

  NOTA

  Para garantizar la confiabilidad de los datos, se genera automáticamente una copia de un archivo cuando el archivo se almacena en HDFS. Es decir, se almacenan dos copias del mismo archivo de forma predeterminada. El espacio de almacenamiento HDFS indica el espacio total en disco ocupado por todas estas copias. Por ejemplo, si el valor de **Storage Space Quota** se establece en **500**, el espacio real para almacenar archivos es de aproximadamente 250 MB (500/2 = 250).

e. Haga clic en **OK**. El sistema crea directorios de tenant en el directorio raíz de HDFS.

- Modificar un directorio de tenant.

  a. En MRS Manager, haga clic en **Tenant**.

  b. En la lista de tenant de la izquierda, haga clic en el tenant cuyo directorio de almacenamiento de HDFS necesita modificarse.

  c. Haga clic en la pestaña **Resource**.

  d. En la tabla **HDFS Storage**, haga clic en **Modify** en la columna **Operation** del directorio de tenant especificado.

  - Establezca **Quota** en las cuotas de cantidad de archivos y directorios.

    Maximum Number of Files/Directories es opcional. Su valor oscila entre **1** y **9223372036854775806**.

  - Establezca **Storage Space Quota** en el tamaño del espacio de almacenamiento del directorio del tenant.

    El valor de **Storage Space Quota** oscila entre **1** y **8796093022208**.

    NOTA

    Para garantizar la confiabilidad de los datos, se genera automáticamente una copia de un archivo cuando el archivo se almacena en HDFS. Es decir, se almacenan dos copias del mismo archivo de forma predeterminada. El espacio de almacenamiento HDFS indica el espacio total en disco ocupado por todas estas copias. Por ejemplo, si el valor de **Storage Space Quota** se establece en **500**, el espacio real para almacenar archivos es de aproximadamente 250 MB (500/2 = 250).

  e. Haga clic en **OK**.

- Eliminar un directorio de tenant.

  a. En MRS Manager, haga clic en **Tenant**.

  b. En la lista de tenant de la izquierda, haga clic en el tenant cuyo directorio de almacenamiento HDFS debe eliminarse.

  c. Haga clic en la pestaña **Resource**.

  d. En la tabla **HDFS Storage**, haga clic en **Delete** en la columna **Operation** del directorio de tenant especificado.

  No se puede eliminar el directorio de almacenamiento HDFS predeterminado establecido durante la creación del tenant. Solo se puede eliminar el directorio de almacenamiento HDFS recién agregado.

  e. Haga clic en **OK**.

8.10.6 Restauración de datos de tenant

Escenario

Los datos del tenant se almacenan en Manager y en los componentes del clúster de forma predeterminada. Cuando los componentes se restauran de fallas o se reinstalan, algunos datos de configuración del tenant pueden ser anormales. En este caso, puede restaurar manualmente los datos del tenant.

Procedimiento

Paso 1 En MRS Manager, haga clic en **Tenant**.

Paso 2 En la lista de tenant de la izquierda, haga clic en un nodo de tenant.

Paso 3 Compruebe el estado de los datos del tenant.

1. En **Summary**, comprueba el color del círculo a la izquierda de **Basic Information**. El verde indica que el tenant está disponible y el gris indica que el tenant no está disponible.
2. Haga clic en **Resources** y marque el círculo a la izquierda de **Yarn** o **HDFS Storage**. El verde indica que el recurso está disponible y el gris indica que el recurso no está disponible.
3. Haga clic en **Service Association** y compruebe la columna **Status** de la tabla de servicios asociada. **Good** indica que el componente puede proporcionar servicios para el tenant asociado. **Bad** indica que el componente no puede proporcionar servicios al tenant.
4. Si cualquier resultado de la comprobación es anormal, vaya a **Paso 4** para restaurar los datos del tenant.

Paso 4 Haga clic en **Restore Tenant Data**.

Paso 5 En la ventana **Restore Tenant Data**, seleccione uno o más componentes cuyos datos deben restaurarse. Haga clic en **OK**. El sistema restaura automáticamente los datos del tenant.

----Fin

8.10.7 Creación de un grupo de recursos

Escenario

En un clúster MRS, los usuarios pueden dividir lógicamente los nodos del clúster de Yarn para combinar múltiples NodeManagers en un grupo de recursos de Yarn. Cada NodeManager pertenece únicamente a un grupo de recursos. El sistema contiene un grupo de recursos **Default** de forma predeterminada. Todas las NodeManagers que no se agregan a grupos de recursos personalizados pertenecen a este grupo de recursos.

Puede crear un grupo de recursos personalizado en MRS Manager y agregar hosts que no se hayan agregado a otros grupos de recursos personalizados.

Procedimiento

Paso 1 En MRS Manager, haga clic en **Tenant**.

Paso 2 Haga clic en la pestaña **Resource Pools**.

Paso 3 Haga clic en **Add Resource Pool**.

Paso 4 En **Create Resource Pool**, defina las propiedades del grupo de recursos.

- **Name**: Introduzca un nombre para el grupo de recursos. El nombre del grupo de recursos recién creado no puede ser **Default**.

  El nombre consta de 1 a 20 caracteres y puede contener dígitos, letras y guiones bajos (_) pero no puede comenzar con un guion bajo (_).

- **Hosts**: En la lista de hosts de la izquierda, seleccione el nombre de un host especificado y haga clic en 

para agregar el host seleccionado al grupo de recursos. Solo se pueden seleccionar los hosts del clúster. La lista de hosts de un grupo de recursos se puede dejar en blanco.

Paso 5 Haga clic en **OK**.

Paso 6 Después de crear un grupo de recursos, los usuarios pueden ver **Name**, **Members**, **Type**, **vCore** y **Memory** en la lista del grupo de recursos. Los hosts que se agregan al grupo de recursos personalizado ya no son miembros del grupo de recursos **Default**.

----Fin

8.10.8 Modificación de un grupo de recursos

Escenario

Puede modificar miembros de un grupo de recursos existente en MRS Manager.

Procedimiento

Paso 1 En MRS Manager, haga clic en **Tenant**.

Paso 2 Haga clic en la pestaña **Resource Pools**.

Paso 3 Busque la fila que contiene el grupo de recursos especificado y haga clic en **Modify** en la columna **Operation**.

Paso 4 En **Modify Resource Pool**, modifique **Added Hosts**.

- Agregar un host: seleccione el nombre de un host especificado en la lista de hosts de la izquierda y haga clic en 

para agregar el host seleccionado al grupo de recursos.
- Eliminar un host: en la lista de hosts de la derecha, seleccione el nombre del host especificado y haga clic en 

para agregar el host seleccionado al grupo de recursos. La lista de hosts de un grupo de recursos se puede dejar en blanco.

Paso 5 Haga clic en **OK**.

----Fin

8.10.9 Eliminación de un grupo de recursos

Escenario

Puede eliminar un grupo de recursos existente en MRS Manager.

Prerrequisitos

- Cualquier cola de un clúster no puede utilizar el grupo de recursos que se va a eliminar como grupo de recursos predeterminado. Antes de eliminar el grupo de recursos, cancele el grupo de recursos predeterminado. Para obtener más información, consulte **Configuración de una cola**.
- Las políticas de distribución de recursos de todas las colas se han borrado del grupo de recursos que se está eliminando. Para obtener más información, consulte **Borrar la configuración de una cola**.

Procedimiento

Paso 1 En MRS Manager, haga clic en **Tenant**.

Paso 2 Haga clic en la pestaña **Resource Pools**.

Paso 3 Busque la fila que contiene el grupo de recursos especificado y haga clic en **Delete** en la columna **Operation**.

En el cuadro de diálogo que se muestra, haga clic en **OK**.

----Fin

8.10.10 Configuración de una cola

Escenario

Esta sección describe cómo modificar la configuración de cola para un tenant especificado en MRS Manager.

Prerrequisitos

Se ha agregado un tenant asociado con Yarn y recursos dinámicos asignados.

Procedimiento

Paso 1 En MRS Manager, haga clic en **Tenant**.

Paso 2 Haga clic en la pestaña **Dynamic Resource Plan**.

Paso 3 Haga clic en la pestaña **Queue Configuration**.

Paso 4 En la tabla de colas de tenant, haga clic en **Modify** en la columna **Operation** de la cola de tenant especificada.

NOTA

En la lista de tenant a la izquierda de la pestaña **Tenant Management**, haga clic en el tenant de destino.

En la ventana que se muestra, elija **Resource**. En la página que se muestra, haga clic en para abrir la página de modificación de cola.

Tabla 8-32 Parámetros de configuración de cola

Parámetro	Descripción
Maximum Application	Especifica el número máximo de aplicaciones. El valor oscila entre 1 y 2147483647.
Maximum AM Resource Percent	Especifica el porcentaje máximo de recursos que se pueden utilizar para ejecutar el ApplicationMaster en un clúster. El valor varía de 0 a 1.
Minimum User Limit Percent (%)	Especifica el porcentaje mínimo de recursos consumidos por un usuario. El valor varía de 0 a 100.
User Limit Factor	Especifica el factor límite del uso máximo de recursos de usuario. El porcentaje máximo de uso de recursos de usuario se puede obtener multiplicando el factor límite por el porcentaje del uso real de recursos del tenant en el clúster. El valor mínimo es **0**.
Status	Especifica el estado actual de un plan de recursos. Los valores son **Running** y **Stopped**.
Default Resource Pool	Especifica el grupo de recursos utilizado por una cola. El valor predeterminado es **Default**. Si desea cambiar el grupo de recursos, configure primero la capacidad de la cola. Para obtener más información, consulte **Configuración de la política de capacidad de cola de un grupo de recursos**.

----Fin

8.10.11 Configuración de la política de capacidad de cola de un grupo de recursos

Escenario

Después de agregar un grupo de recursos, las políticas de capacidad de los recursos disponibles deben configurarse para las colas de tareas de Yarn. Esto garantiza que las tareas del grupo de recursos se estén ejecutando correctamente. Cada cola se puede configurar con la política de capacidad de cola de un solo grupo de recursos. Los usuarios pueden ver las colas en cualquier grupo de recursos y configurar políticas de capacidad de cola. Una vez configuradas las políticas de cola, se asocian las colas de tareas de Yarn y los grupos de recursos.

Puede configurar políticas de cola en MRS Manager.

Prerrequisitos

- Se ha agregado un grupo de recursos.
- Las colas de tareas no están asociadas con otros grupos de recursos. De forma predeterminada, todas las colas están asociadas al grupo de recursos **Default**.

Procedimiento

Paso 1 En MRS Manager, haga clic en **Tenant**.

Paso 2 Haga clic en la pestaña **Dynamic Resource Plan**.

Paso 3 En el campo **Resource Pools**, seleccione un grupo de recursos especificado.

Available Resource Quota: indica que todos los recursos de cada grupo de recursos están disponibles para colas de forma predeterminada.

Paso 4 Busque la cola especificada en la tabla **Resource Allocation** y haga clic en **Modify** en la columna **Operation**.

Paso 5 En **Modify Resource Allocation**, configure la política de capacidad de recursos de la cola de tareas en el grupo de recursos.

- **Capacity (%)**: especifica el porcentaje del uso de recursos informáticos del tenant actual.
- **Maximum Capacity (%)**: especifica el porcentaje del uso máximo de recursos informáticos del tenant actual.

Paso 6 Haga clic en **OK** para guardar la configuración.

----Fin

8.10.12 Borrar la configuración de una cola

Escenario

Los usuarios pueden borrar la configuración de una cola en MRS Manager cuando la cola no necesita recursos de un grupo de recursos o si un grupo de recursos necesita estar desasociado de la cola. Borrar configuraciones de cola significa que se cancela la política de capacidad de recursos de la cola.

Prerrequisitos

Si una cola va a ser independiente de un grupo de recursos, este grupo de recursos no puede servir como el grupo de recursos predeterminado de la cola. Por lo tanto, primero debe cambiar el grupo de recursos predeterminado de la cola a otro. Para obtener más información, consulte **Configuración de una cola**.

Procedimiento

Paso 1 En MRS Manager, haga clic en **Tenant**.

Paso 2 Haga clic en la pestaña **Dynamic Resource Plan**.

Paso 3 En el campo **Resource Pools**, seleccione un grupo de recursos especificado.

Paso 4 Busque la cola especificada en la tabla **Resource Allocation** y haga clic en **Clear** en la columna **Operation**.

En el cuadro de diálogo **Clear Queue Configuration**, haga clic en **OK** para borrar la configuración de cola en el grupo de recursos actual.

NOTA

Si no se configura ninguna política de capacidad de recursos para una cola, la función de borrado no está disponible para la cola de forma predeterminada.

----Fin

8.11 Copia de respaldo y restauración

8.11.1 Introducción

Propósito

MRS Manager proporciona copias de respaldo y restauración de datos de usuario y datos del sistema. La función de copia de respaldo se proporciona en función de los componentes para hacer copias de respaldo de los datos del Manager (incluidos los datos de OMS y LdapServer), los datos del usuario de Hive, los metadatos de los componentes guardados en DBService y los metadatos de HDFS.

Las tareas de copia de respaldo y restauración se realizan en los siguientes escenarios:

- La copia de respaldo de rutina se realiza para garantizar la seguridad de los datos del sistema y los componentes.
- Si el sistema está defectuoso, la copia de respaldo de datos se puede utilizar para recuperar el sistema.
- Si el clúster activo es completamente defectuoso, es necesario crear un clúster duplicado idéntico al clúster activo. Puede utilizar los datos de copia de respaldo para restaurar el clúster activo.

Tabla 8-33 Copia de respaldo de metadatos

Tipo de copia de respaldo	Contenido de copia de respaldo
OMS	Datos de base de datos (excluidos los datos de alarma) y datos de configuración en el sistema de gestión de clústeres que se van a respaldar de forma predeterminada
LdapServer	Información del usuario, incluidos el nombre de usuario, la contraseña, la clave, la política de contraseñas y la información del grupo
DBService	Metadatos de los componentes (Hive) gestionados por DBService
NameNode	Metadatos de HDFS.

Principios

Tarea

Antes de realizar una copia de respaldo o restauración, debe crear una tarea de copia de respaldo o restauración y establecer parámetros de tarea, como el nombre de la tarea, el origen de datos de copia de respaldo y el tipo de ruta de guardado del archivo de copia de respaldo. La copia de respaldo y restauración de datos se pueden realizar ejecutando tareas de copia de respaldo y restauración. Cuando el Manager se utiliza para recuperar los datos de HDFS, HBase, Hive y NameNode, no se puede acceder a ningún clúster.

Cada tarea de copia de respaldo puede realizar copias de respaldo de datos de diferentes orígenes de datos y generar un archivo de copia de respaldo independiente para cada origen de datos. Todos los archivos de copia de respaldo generados en cada tarea de copia de respaldo forman un conjunto de archivos de copia de respaldo, que se pueden utilizar en tareas de restauración. Los datos de copia de respaldo se pueden almacenar en discos locales de Linux, HDFS de clúster local y HDFS de clúster en espera. La tarea de copia de respaldo proporciona la copia de respaldo completa o las políticas de copia de respaldo incremental. Las tareas de copia de respaldo HDFS y Hive admiten la política de copia de respaldo incremental, mientras que las tareas de copia de respaldo OMS, LdapServer, DBService y NameNode solo admiten la política de copia de respaldo completa.

NOTA

Reglas de ejecución de tareas:

- Si se está ejecutando una tarea, la tarea no se puede ejecutar repetidamente y otras tareas no se pueden iniciar al mismo tiempo.
- El intervalo en el que se ejecuta automáticamente una tarea periódica debe ser superior a 120 segundos; de lo contrario, la tarea se pospone y se ejecutará en el siguiente período. Las tareas manuales se pueden ejecutar en cualquier intervalo.
- Cuando se va a ejecutar automáticamente una tarea periódica, la hora actual no puede ser 120 segundos más tarde que la hora de inicio de la tarea; de lo contrario, la tarea se pospone y ejecuta en el siguiente período.
- Cuando se bloquea una tarea periódica, no se puede ejecutar automáticamente y es necesario desbloquearla manualmente.
- Antes de que se inicie una tarea de copia de respaldo de OMS, LdapServer, DBService o NameNode, asegúrese de que la partición LocalBackup del nodo de gestión activo tenga más de 20 GB de espacio disponible. De lo contrario, no se puede iniciar la tarea de copia de respaldo.
- Cuando planifique tareas de copia de respaldo y restauración, seleccione los datos que se van a realizar o restaurar estrictamente en función de la lógica del servicio, la estructura del almacén de datos y la asociación de bases de datos o tablas. El sistema crea una tarea de copia de respaldo periódica predeterminada **default** cuyo intervalo de ejecución es de 24 horas para realizar una copia de respaldo completa de los datos de OMS, de LdapServer y de DBService, y NameNode en el disco local de Linux.

Especificaciones

Tabla 8-34 Especificaciones de funciones de copia de respaldo y restauración

Concepto	Especificaciones
Número máximo de tareas de copia de respaldo o restauración	100
Número de tareas en ejecución simultánea	1

Concepto	Especificaciones
Número máximo de tareas en espera	199
Tamaño máximo de los archivos de copia de respaldo en un disco local de Linux (GB)	600

Tabla 8-35 Especificaciones de la tarea **default**

Concepto	OMS	LdapServer	DBService	NameNode
Período de copia de respaldo	1 hora			
Número máximo de copias	2			
Tamaño máximo de un archivo de copia de respaldo	10 MB	20 MB	100 MB	1.5 GB
Tamaño máximo del espacio en disco utilizado	20 MB	40 MB	200 MB	3 GB
Ruta de guardado de datos de copia de respaldo	*Data save path*/**LocalBackup/** de los nodos de gestión activo y en espera			

NOTA

Los datos de copia de respaldo de la tarea **default** deben transferirse y guardarse periódicamente fuera del clúster según los requisitos de operación de la empresa.

8.11.2 Copia de respaldo de metadatos

Escenario

Para garantizar la seguridad de los metadatos de forma rutinaria o antes y después de realizar operaciones críticas de metadatos (como expansión horizontal, reducción horizontal, instalación de parches, actualizaciones y migración), se debe realizar una copia de respaldo de los metadatos. Los datos de copia de respaldo se pueden utilizar para recuperar el sistema si se produce una excepción o si la operación no ha logrado el resultado esperado. Esto minimiza el impacto adverso en los servicios. Los metadatos incluyen datos de OMS, LdapServer

DBService, y NameNode. Los datos de MRS Manager que se van a respaldar incluyen datos de OMS y datos de LdapServer.

De forma predeterminada, la tarea **default** admite la copia de respaldo de metadatos. Esta sección describe cómo crear una tarea de copia de respaldo y hacer una copia de respaldo de metadatos en MRS Manager. Tanto las tareas de copia de respaldo automáticas como las tareas de copia de respaldo manuales son compatibles.

Prerrequisitos

- Se ha creado un clúster en espera para realizar copias de respaldo de los datos y la red está conectada. Las reglas entrantes de los dos grupos de seguridad del clúster del mismo nivel se han agregado a los dos grupos de seguridad de cada clúster para permitir todas las solicitudes de acceso de todos los protocolos y puertos de todos los ECS de los grupos de seguridad.
- El tipo de copia de respaldo, el período, la política y otras especificaciones se han planificado en función de los requisitos de servicio y se ha comprobado si *Data storage path*/**LocalBackup/** tiene suficiente espacio en los nodos de gestión activo y en espera.

Procedimiento

Paso 1 Crear una tarea de copia de respaldo.

1. En MRS Manager, elija **System** > **Back Up Data**.
2. Haga clic en **Create Backup Task**.

Paso 2 Configurar una política de copia de respaldo.

1. Establezca **Task Name** en el nombre de la tarea de copia de respaldo.
2. Establezca **Backup Mode** en el tipo de tarea de copia de respaldo. **Periodic** indica que la tarea de copia de respaldo se ejecuta periódicamente. **Manual** indica que la tarea de copia de respaldo se ejecuta manualmente.

   Para crear una tarea de copia de respaldo periódica, establezca los siguientes parámetros:

   – **Started**: indica la hora en la que se inicia la tarea por primera vez.
   – **Period**: indica el intervalo de ejecución de la tarea. Las opciones incluyen **By hour** y **By day**.
   – **Backup Policy**: indica el volumen de datos que se van a hacer copias de respaldo en cada ejecución de tarea. Las opciones incluyen **Full backup at the first time and incremental backup later**, **Full backup every time** y **Full backup once every n times**. Si selecciona **Full backup once every n times**, debe especificar el valor de **n**.

Paso 3 Seleccione las fuentes de copia de respaldo.

En el área **Configuration**, seleccione **OMS** y **LdapServer** en **Metadata**.

Paso 4 Establezca los parámetros de copia de respaldo.

1. Establecer **Path Type** de **OMS** y **LdapServer** en un tipo de directorio de copia de respaldo.

   Se admiten los siguientes tipos de directorio de copia de respaldo:

   – **LocalDir** indica que los archivos de copia de respaldo se almacenan en el disco local del nodo de gestión activo y el nodo de gestión en espera sincroniza automáticamente los archivos de copia de respaldo. De forma predeterminada, los

archivos de copia de respaldo se almacenan en "*Data storage path*/**LocalBackup/**". Si selecciona **LocalDir**, debe establecer el número máximo de copias para especificar el número de archivos de copia de respaldo que se pueden conservar en el directorio de copia de respaldo.

- **LocalHDFS**: indica que los archivos de copia de respaldo se almacenan en el directorio de HDFS del clúster actual. Si selecciona **SFTP**, establezca los siguientes parámetros:
  - **Target Path**: indica el directorio de HDFS para almacenar los archivos de copia de respaldo. La ruta de acceso de guardado no puede ser un directorio oculto HDFS, como un directorio de instantáneas o papelera de reciclaje, o un directorio de sistema predeterminado.
  - **Max Number of Backup Copies**: indica el número de archivos de copia de respaldo que se pueden retener en el directorio de copia de respaldo.
  - **Target Instance Name**: indica el nombre NameService del directorio de copia de respaldo. El valor predeterminado es **hacluster**.

2. Haga clic en **OK**.

Paso 5 Ejecute la tarea de copia de respaldo.

En la columna **Operation** de la tarea creada en la lista de tareas de copia de respaldo, haga clic en **Back Up Now** si **Backup Mode** está establecido en **Periodic** o haga clic en **Start** si **Backup Mode** está establecido en **Manual** para ejecutar la tarea de copia de respaldo.

Después de ejecutar la tarea de copia de respaldo, el sistema crea automáticamente un subdirectorio para cada tarea de copia de respaldo en el directorio de copia de respaldo. El formato del nombre del subdirectorio es de *Backup task name*_*Task creation time* y el subdirectorio se utiliza para guardar los archivos de copia de respaldo de origen de datos. El formato del nombre del archivo de copia de respaldo es *Version*_*Data source*_*Task execution time*.**tar.gz**.

----Fin

8.11.3 Restauración de metadatos

Escenario

Debe restaurar metadatos en los siguientes escenarios: Un usuario modifica o elimina los datos de forma inesperada, los datos deben recuperarse, los datos del sistema se vuelven anormales o no logran el resultado esperado, todos los módulos son defectuosos y los datos se migran a un nuevo clúster.

Esta sección describe cómo restaurar metadatos en MRS Manager. Solo se admiten las tareas de restauración manuales.

AVISO

- La restauración de datos solo se puede realizar cuando la versión del sistema es coherente con la de la copia de respaldo de datos.
- Para restaurar los datos cuando los servicios son normales, realice primero una copia de seguridad manual de los datos de gestión más recientes y, a continuación, restaure los datos. De lo contrario, los datos que se generan después de la copia de respaldo de datos y antes de la restauración de datos se perderán.
- Utilice los datos de OMS y los datos de LdapServer respaldados al mismo tiempo para restaurar los datos. De lo contrario, el servicio y la operación pueden fallar.
- De forma predeterminada, los clústeres MRS usan DBService para almacenar metadatos de Hive.

Impacto en el sistema

- Después de restaurar los datos, se pierden los datos generados entre el tiempo de copia de respaldo y el tiempo de restauración.
- Después de restaurar los datos, la configuración de los componentes que dependen de DBService puede caducar y estos componentes deben reiniciarse.

Prerrequisitos

- Se ha realizado una copia de respaldo de los datos de los archivos de copia de respaldo de OMS y LdapServer al mismo tiempo.
- El estado de los recursos de OMS y las instancias LdapServer es normal. Si el estado es anormal, no se puede realizar la restauración de datos.
- El estado de los hosts y servicios del clúster es normal. Si el estado es anormal, no se puede realizar la restauración de datos.
- Las topologías del host del clúster durante la restauración de datos y la copia de respaldo de datos son las mismas. Si las topologías son diferentes, no se puede realizar la restauración de datos y es necesario realizar una copia de respaldo de los datos de nuevo.
- Los servicios agregados al clúster durante la restauración de datos y la copia de respaldo de datos son los mismos. Si los servicios son diferentes, no se puede realizar la restauración de datos y es necesario realizar una copia de seguridad de los datos de nuevo.
- El estado de las instancias de DBService activas y en espera es normal. Si el estado es anormal, no se puede realizar la restauración de datos.
- Se han detenido las aplicaciones de capa superior que dependen del clúster de MRS.
- En MRS Manager, ha detenido todas las instancias de rol NameNode cuyos datos se van a recuperar. Otras instancias de rol HDFS se están ejecutando correctamente. Después de recuperar los datos, las instancias de rol NameNode deben reiniciarse y no se puede acceder antes del reinicio.
- Ha comprobado si los archivos de copia de respaldo de NameNode se han almacenado en el directorio *Data save path*/**LocalBackup/** en el nodo de gestión activa.

Procedimiento

Paso 1 Compruebe la ubicación de los datos de copia de respaldo.

1. En MRS Manager, elija **System** > **Back Up Data**.
2. En la fila donde reside la tarea de copia de respaldo especificada, elija **More** > **View History** en la columna **Operation** para mostrar los registros históricos de ejecución de la tarea de copia de respaldo. En la ventana que se muestra, seleccione un registro de éxito y haga clic en **View Backup Path** en la columna correspondiente para ver la información de su ruta de copia de respaldo. Encuentre la siguiente información:
   - **Backup Object**: indica el origen de datos de la copia de respaldo.
   - **Backup Path**: indica la ruta completa donde se almacenan los archivos de copia de respaldo.
3. Seleccione la ruta correcta y copie manualmente la ruta completa de los archivos de copia de respaldo de **Backup Path**.

Paso 2 Crear una tarea de restauración.

1. En MRS Manager, elija System > Recovery Management.
2. En la página que se muestra, haga clic en **Create Restoration Task**.
3. Establezca **Task Name** en el nombre de la tarea de restauración.

Paso 3 Seleccione los orígenes de restauración.

En **Configuration**, seleccione el componente de metadatos cuyos datos se van a restaurar.

Paso 4 Establezca los parámetros de restauración.

1. Establezca **Path Type** en un tipo de directorio de copia de respaldo.
2. La configuración varía según los tipos de directorios de copia de respaldo:
   - **LocalDir**: indica que los archivos de copia de respaldo se almacenan en el disco local del nodo de gestión activa. Si selecciona **LocalDir**, debe configurar **Source Path** para especificar la ruta completa del archivo de copia de respaldo. Por ejemplo, *Data storage path*/**LocalBackup**/*Backup task name_Task creation time*/*Data source_Task execution time*/*Version number_Data source_Task execution time*.**tar.gz**.
   - **LocalHDFS**: indica que los archivos de copia de respaldo se almacenan en el directorio de HDFS del clúster actual. Si selecciona **SFTP**, establezca los siguientes parámetros:
     - **Source Path**: indica la ruta HDFS completa de un archivo de copia de respaldo. por ejemplo, *Backup path/Backup task name_Task creation time/Version_Data source_Task execution time*.**tar.gz**.
     - **Source Instance Name**: indica el nombre de NameService correspondiente al directorio de copia de respaldo cuando se ejecuta una tarea de restauración. El valor predeterminado es **hacluster**.
3. Haga clic en **OK**.

Paso 5 Ejecute la tarea de restauración.

En la lista de tareas de restauración, busque la fila donde reside la tarea creada y haga clic en **Start** en la columna **Operation**.

- Después de que la restauración es exitosa, la barra de progreso está en verde.
- Una vez que la restauración se realiza correctamente, la tarea de restauración no se puede ejecutar de nuevo.
- Si la tarea de restauración falla durante la primera ejecución, corrija el error e intente ejecutar la tarea de nuevo haciendo clic en **Start**.

Paso 6 Determine qué metadatos se han restaurado.

- Si se restauran los metadatos de OMS y LdapServer, vaya a **Paso 7**.
- Si se restauran los datos de DBService, no se requiere ninguna otra acción.
- Restaure datos de NameNode. En MRS Manager, seleccione **Services > HDFS > More > Restart Service**. Se ha completado la tarea.

Paso 7 Reinicio del Manager para que los datos recuperados surtan efecto

1. En MRS Manager, elija **LdapServer** > **More** > **Restart Service** y haga clic en **OK**. Espere hasta que el servicio LdapServer se reinicie correctamente.
2. Inicie sesión en el nodo de gestión activo. Para obtener más información, consulte **Determinación de nodos de gestión activos y en espera**.
3. Ejecute el siguiente comando para reiniciar OMS:

   sh ${BIGDATA_HOME}/om-0.0.1/sbin/restart-oms.sh

   El comando se ha ejecutado correctamente si se muestra la siguiente información:

   ```
   start HA successfully.
   ```
4. En MRS Manager, seleccione **KrbServer > More > Synchronize Configuration**. No seleccione Restart the services and instances cuya configuración ha caducado. Haga clic en **OK** y espere hasta que la configuración del servicio KrbServer se sincronice y se reinicie correctamente.
5. Elija **Services > More > Synchronize Configuration**. No seleccione Restart the services and instances cuya configuración ha caducado. Haga clic en **OK** y espere hasta que el clúster se configure y sincronice correctamente.
6. Elija **Services > More > Stop Cluster**. Una vez que se detenga el clúster, seleccione **Services > More> Start Cluster**.

----Fin

8.11.4 Modificación de una tarea de copia de respaldo

Escenario

Esta sección describe cómo modificar los parámetros de una tarea de copia de respaldo creada en MRS Manager para cumplir con los requisitos de servicio cambiantes. Los parámetros de las tareas de restauración se pueden ver pero no modificar.

Impacto en el sistema

Después de modificar una tarea de copia de respaldo, los nuevos parámetros surten efecto cuando la tarea se ejecute la próxima vez.

Prerrequisitos

- Se ha creado una tarea de copia de respaldo.
- Se ha planificado una nueva política de tareas de copia de respaldo en función de la situación real.

Procedimiento

Paso 1 En MRS Manager, elija **System** > **Back Up Data**.

Paso 2 En la lista de tareas, busque una tarea especificada, haga clic en **Modify** en la columna **Operation** para ir a la página de modificación de configuración.

Paso 3 Modifique los siguientes parámetros en la página mostrada:

- Manual backup:
  - Target Path
  - Max Number of Backup Copies
- Periodic backup:
  - Started
  - Period
  - Target Path
  - Max Number of Backup Copies

  NOTA

  - Cuando **Path Type** está establecido en **LocalHDFS**, **Target Path** es válido para modificar una tarea de copia de respaldo.
  - Después de cambiar el valor de **Target Path** para una tarea de copia de respaldo, la copia de respaldo completa se realiza de forma predeterminada cuando la tarea se ejecuta por primera vez.

Paso 4 Haga clic en **OK**.

----Fin

8.11.5 Consulta de tareas de copia de respaldo y restauración

Escenario

Esta sección describe cómo ver las tareas de copia de respaldo y restauración creadas y comprobar su estado de ejecución en MRS Manager.

Procedimiento

Paso 1 En MRS Manager, haga clic en **System**.

Paso 2 Haga clic en **Back Up Data** o **Restore Data**.

Paso 3 En la lista de tareas, obtenga el resultado de ejecución anterior en la columna **Task Progress**. El verde indica que la tarea se ejecuta correctamente y el rojo indica que la ejecución falla.

Paso 4 En la columna **Operation** de una tarea especificada en la lista de tareas, elija **More** > **View History** para ver el registro histórico de la ejecución de copia de respaldo y restauración.

En la ventana mostrada, haga clic en **View** en la columna **Details**. Se muestran los registros de ejecución de tareas y las rutas de acceso.

----Fin

Tareas relacionadas

- Modificación de una tarea de copia de respaldo

  Para obtener más información, consulte **Modificación de una tarea de copia de respaldo**.

- Consulta de una tarea de restauración

  En la columna **Operation** de la tarea especificada en la lista de tareas, haga clic en **View Details** para ver la tarea de restauración. Solo se pueden ver pero no se pueden modificar los parámetros de una tarea de restauración.

- Ejecución de una tarea de copia de respaldo o restauración

  En la lista de tareas, busque una tarea especificada y haga clic en **Start** en la columna **Operation** para iniciar una tarea de copia de respaldo o restauración que esté lista o no se ejecute. Las tareas de restauración ejecutadas no se pueden ejecutar repetidamente.

- Detener las tareas de copia de respaldo

  En la lista de tareas, busque una tarea especificada y haga clic en **More** > **Stop** en la columna **Operation** para detener una tarea de copia de respaldo que se está ejecutando.

- Eliminar una tarea de copia de respaldo o restauración

  En la columna **Operation** de la tarea especificada en la lista de tareas, elija **More** > **Delete** para eliminar la tarea de copia de respaldo o restauración. Después de eliminar una tarea, los datos de copia de respaldo se conservan de forma predeterminada.

- Suspender una tarea de copia de respaldo

  En la columna **Operation** de la tarea especificada en la lista de tareas, elija **More** > **Suspend** para suspender la tarea de copia de respaldo. Solo se pueden suspender las tareas de copia de respaldo periódicas. Las tareas de copia de respaldo suspendidas ya no se ejecutan automáticamente. Cuando suspende una tarea de copia de respaldo que se está ejecutando, la ejecución de la tarea se detiene. Para cancelar el estado de suspensión de una tarea, haga clic en **More** > **Resume**.

8.12 Gestión de seguridad

8.12.1 Usuarios predeterminados de clústeres con autenticación de Kerberos deshabilitada

Clasificación de usuario

El clúster de MRS proporciona los dos tipos de usuarios siguientes. Se aconseja a los usuarios que cambien periódicamente las contraseñas. No se recomienda utilizar las contraseñas predeterminadas.

Tipo de usuario	Descripción
Usuarios del sistema	Usuario que ejecuta procesos de OMS
Usuarios de la base de datos	● Usuario que gestiona la base de datos de OMS y accede a los datos ● Usuario que ejecuta la base de datos de componentes de servicio (Hive, Loader y DBService)

Usuarios del sistema

NOTA

- Se requiere usuario **Idap** del sistema operativo en el clúster de MRS. No elimine esta cuenta. De lo contrario, es posible que el clúster no funcione correctamente. Las políticas de gestión de contraseñas son mantenidas por los usuarios de la operación.
- Restablecer las contraseñas cuando cambie las contraseñas de usuario **ommdba** y usuario **omm** por primera vez. Cambie las contraseñas periódicamente después de recuperarlas.

Operación	Nombre de usuario	Contraseña inicial	Descripción
Administrador del sistema del clúster de MRS	admin	Especificado por el usuario durante la creación del clúster	MRS Manager Este usuario tiene los siguientes permisos: ● Permisos de usuario comunes de HDFS y ZooKeeper. ● Permisos para enviar y consultar tareas de MapReduce y Yarn, gestionar colas de Yarn y acceder a la Yarn web UI. ● Permisos para enviar, consultar, activar, desactivar, reasignar, eliminar topologías y operar todas las topologías del servicio Storm. ● Permisos para crear, eliminar, autorizar, reasignar, consumir, escribir y consultar temas del servicio Kafka.
Usuario del sistema operativo del nodo del clúster de MRS	omm	Generado aleatoriamente por el sistema	Usuario en ejecución interna del sistema de clúster de MRS. Este usuario es un usuario del sistema operativo generado en todos los nodos y no requiere una contraseña unificada.
Usuario del sistema operativo del nodo del clúster de MRS	root	Establecer por el usuario	Usuario para iniciar sesión en el nodo del clúster de MRS. Este usuario es un usuario de OS generado en todos los nodos.

Información del grupo de usuarios

Grupo de usuarios predeterminado	Descripción
supergroup	Grupo principal de usuario **admin**, que no tiene permisos adicionales en el clúster con la autenticación de Kerberos deshabilitada.
check_sec_ldap	Se utiliza para probar si el LDAP activo funciona correctamente. Este grupo de usuarios se genera aleatoriamente en una prueba y se elimina automáticamente una vez completada la prueba. que es un grupo de usuarios interno del sistema utilizado solo entre componentes.
Manager_tenant	Grupo de usuarios del sistema de tenant, que es un grupo de usuarios del sistema interno que se utiliza solo entre componentes. Solo se utiliza en clústeres con autenticación de Kerberos habilitada.
System_administrator	Grupo de administradores del sistema de clúster de MRS, que es un grupo de usuarios del sistema interno que se utiliza solo entre componentes. Solo se utiliza en clústeres con autenticación de Kerberos habilitada.
Manager_viewer	Grupo de visualizadores del sistema de MRS Manager, que es un grupo de usuarios del sistema interno que se utiliza solo entre componentes. Solo se utiliza en clústeres con autenticación de Kerberos habilitada.
Manager_operator	Grupo de operadores del sistema de MRS Manager, que es un grupo de usuarios del sistema interno que se utiliza solo entre componentes. Solo se utiliza en clústeres con autenticación de Kerberos habilitada.
Manager_auditor	Grupo de auditores del sistema de MRS Manager, que es un grupo interno de usuarios del sistema utilizado solo entre componentes. Solo se utiliza en clústeres con autenticación de Kerberos habilitada.
Manager_administrator	Grupo de administradores del sistema de MRS Manager, que es un grupo de usuarios del sistema interno que se utiliza solo entre componentes. Solo se utiliza en clústeres con autenticación de Kerberos habilitada.
compcommon	Grupo interno del clúster de MRS, utilizado para acceder a los recursos públicos del clúster. Todos los usuarios del sistema y los usuarios en ejecución del sistema se agregan a este grupo de usuarios de forma predeterminada.

Grupo de usuarios predeterminado	Descripción
default_1000	Grupo de usuarios creado para tenants, que es un grupo de usuarios interno del sistema que se utiliza solo entre componentes.
launcher-job	Grupo interno de MRS, que se utiliza para enviar trabajos mediante las API de V2.

Grupo de usuarios de sistema operativo	Descripción
wheel	Grupo primario de usuario **omm** en ejecución interna de MRS.
ficommon	Grupo común del clúster de MRS que corresponde a **compcommon** para acceder a los archivos de recursos públicos almacenados en el sistema operativo del clúster.

Usuarios de la base de datos

Los usuarios de base de datos del sistema de clúster de MRS incluyen usuarios de base de datos de OMS y usuarios de base de datos de DBService.

NOTA

No elimine usuarios de base de datos. De lo contrario, es posible que el clúster o los componentes no funcionen correctamente.

Operación	Usuario predeterminado	Contraseña inicial	Descripción
Base de datos de OMS	ommdba	dbChangeMe@123456	Administrador de base de datos de OMS que realiza operaciones de mantenimiento, como crear, iniciar y detener.
	omm	ChangeMe@123456	Usuario para acceder a los datos de la base de datos de OMS
Base de datos de DBService	omm	dbserverAdmin@123	Administrador de la base de datos de GaussDB en el componente de DBService
	hive	HiveUser@	Usuario para que Hive se conecte a la base de datos de DBService

Operación	Usuario predeterminado	Contraseña inicial	Descripción
	hue	HueUser@123	Usuario para que Hue se conecte a la base de datos de DBService
	sqoop	SqoopUser@	Usuario para que Loader se conecte a la base de datos de DBService.

8.12.2 Usuarios predeterminados de clústeres con autenticación de Kerberos habilitada

Clasificación de usuario

El clúster de MRS proporciona los siguientes tres tipos de usuarios. Se aconseja a los usuarios que cambien periódicamente las contraseñas. No se recomienda utilizar las contraseñas predeterminadas.

Tipo de usuario	Descripción
Usuario del sistema	● Usuario creado en Manager for MRS cluster O&M y escenarios de servicio. Hay dos tipos de usuarios: – Usuario **Human-machine**: utilizado para escenarios de O&M de Manager y escenarios de operación de cliente de componentes. – Usuario **Machine-machine**: utilizado para escenarios de desarrollo de aplicaciones de clúster de MRS. ● Usuario que ejecuta procesos de OMS.
Usuario interno del sistema	Usuario interno que realiza las comunicaciones de proceso, guarda la información del grupo de usuarios y asocia los permisos de usuario.
Usuario de la base de datos	● Usuario que gestiona la base de datos de OMS y accede a los datos. ● Usuario que ejecuta la base de datos de componentes de servicio (Hive, Hue, Loader y DBService)

Usuario del sistema

NOTA

- Se requiere usuario **Idap** del sistema operativo en el clúster de MRS. No elimine esta cuenta. De lo contrario, es posible que el clúster no funcione correctamente. Las políticas de gestión de contraseñas son mantenidas por los usuarios de la operación.
- Restablecer las contraseñas cuando cambie las contraseñas de usuario **ommdba** y usuario **omm** por primera vez. Cambie las contraseñas periódicamente después de recuperarlas.

Tipo	Nombre de usuario	Contraseña inicial	Descripción
Administrador del sistema del clúster de MRS	admin	Especificado por el usuario durante la creación del clúster.	Administrador de Manager con los siguientes permisos: ● Permisos de usuario comunes de HDFS y ZooKeeper. ● Permisos para enviar y consultar tareas de MapReduce y Yarn, gestionar colas de Yarn y acceder a la Yarn web UI. ● Permisos para enviar, consultar, activar, desactivar, reasignar, eliminar topologías y operar todas las topologías del servicio Storm. ● Permisos para crear, eliminar, autorizar, reasignar, consumir, escribir y consultar temas del servicio Kafka.
Usuario del sistema operativo del nodo del clúster de MRS	omm	Generado aleatoriamente por el sistema.	Usuario en ejecución interna del sistema de clúster de MRS. Este usuario es un usuario del sistema operativo generado en todos los nodos y no requiere una contraseña unificada.
Usuario del sistema operativo del nodo del clúster de MRS	root	Establecido por el usuario.	Usuario para iniciar sesión en el nodo del clúster de MRS. Este usuario es un usuario de OS generado en todos los nodos.

Usuarios internos del sistema

NOTA

No elimine los siguientes usuarios internos del sistema. De lo contrario, es posible que el clúster o los componentes no funcionen correctamente.

Tipo	Usuario predeterminado	Contraseña inicial	Descripción
Usuario en ejecución de componentes	hdfs	Hdfs@123	Este usuario es administrador del sistema HDFS y tiene los siguientes permisos: 1. Permisos de operación del sistema de archivos: ● Visualiza, modifica y crea archivos. ● Visualiza y crea directorios. ● Visualiza y modifica los grupos a los que pertenecen los archivos. ● Visualiza y establece cuotas de disco para los usuarios. 2. Permisos de operación de gestión de HDFS: ● Visualiza el estado de la interfaz de usuario web. ● Muestra y establece el estado HDFS activo y en espera. ● Entra y sale del HDFS en modo de seguridad. ● Comprueba el sistema de archivos HDFS.

Tipo	Usuario predeterminado	Contraseña inicial	Descripción
	hbase	Hbase@123	Este usuario es un administrador del sistema HBase y tiene los siguientes permisos: ● Permiso de gestión de clústeres: operaciones de **Enable** y **Disable** en tablas para desencadenar operaciones de MajorCompact y ACL. ● Concede y revoca permisos y cierra el clúster. ● Permiso de gestión de tablas: crea, modifica y elimina tablas. ● Permiso de gestión de datos: lee y escribe datos en tablas, familias de columnas y columnas. ● Accede a la interfaz de usuario web de HBase.
	mapred	Mapred@123	Este usuario es administrador del sistema de MapReduce y tiene los siguientes permisos: ● Envía, detiene y visualiza las tareas de MapReduce. ● Modifica los parámetros de configuración de Yarn. ● Accede a la interfaz de usuario web de Yarn y MapReduce.
	spark	Spark@123	Este usuario es el administrador de sistema Spark y tiene los siguientes permisos: ● Accede a la interfaz de usuario web de Spark. ● Envía tareas de Spark.

Información del grupo de usuarios

Grupo de usuarios predeterminado	Descripción
hadoop	Los usuarios agregados a este grupo de usuarios tienen permiso para enviar tareas a todas las colas de Yarn.

Grupo de usuarios predeterminado	Descripción
hbase	Grupo de usuarios común. Los usuarios agregados a este grupo de usuarios no tendrán ningún permiso adicional.
hive	Los usuarios agregados a este grupo de usuarios pueden usar Hive.
spark	Grupo de usuarios común. Los usuarios agregados a este grupo de usuarios no tendrán ningún permiso adicional.
supergroup	Los usuarios agregados a este grupo de usuarios pueden tener el permiso de administrador de HBase, HDFS y Yarn y pueden usar Hive.
check_sec_ldap	Se utiliza para probar si el LDAP activo funciona correctamente. Este grupo de usuarios se genera aleatoriamente en una prueba y se elimina automáticamente una vez completada la prueba. Este es un grupo de usuarios interno del sistema que se utiliza solo entre componentes.
Manager_tenant	Grupo de usuarios del sistema de tenant, que es un grupo de usuarios del sistema interno que se utiliza solo entre componentes.
System_administrator	Grupo de administradores del sistema de clúster de MRS, que es un grupo de usuarios del sistema interno que se utiliza solo entre componentes.
Manager_viewer	Grupo de visualizadores del sistema de MRS Manager, que es un grupo de usuarios del sistema interno que se utiliza solo entre componentes.
Manager_operator	Grupo de operadores del sistema de MRS Manager, que es un grupo de usuarios del sistema interno que se utiliza solo entre componentes.
Manager_auditor	Grupo de auditores del sistema de MRS Manager, que es un grupo interno de usuarios del sistema utilizado solo entre componentes.
Manager_administrator	Grupo de administradores del sistema de MRS Manager, que es un grupo de usuarios del sistema interno que se utiliza solo entre componentes.
compcommon	Grupo de sistema interno para acceder a recursos públicos en un clúster. Todos los usuarios del sistema y los usuarios en ejecución del sistema se agregan a este grupo de usuarios de forma predeterminada.
default_1000	Grupo de usuarios creado para tenants, que es un grupo de usuarios interno del sistema que se utiliza solo entre componentes.

Grupo de usuarios predeterminado	Descripción
kafka	Grupo de usuarios comunes de Kafka. Los usuarios agregados a este grupo deben tener permiso de lectura y escritura por parte de los usuarios del grupo **kafkaadmin** antes de acceder a los topics deseados.
kafkasuperuser	Los usuarios agregados a este grupo tienen permisos para leer datos y escribir datos en todos los topics.
kafkaadmin	Grupo de administradores de Kafka. Los usuarios agregados a este grupo tienen los permisos para crear, eliminar, autorizar, así como leer y escribir datos para todos los topics.
storm	Grupo de usuarios común de Storm. Los usuarios agregados a este grupo tienen los permisos para enviar topologías y gestionar sus propias topologías.
stormadmin	Grupo de usuarios de administrador de Storm. Los usuarios agregados a este grupo tienen los permisos para enviar topologías y gestionar sus propias topologías.
opentsdb	Grupo de usuarios común. Los usuarios agregados a este grupo de usuarios no tendrán ningún permiso adicional.
presto	Grupo de usuarios común. Los usuarios agregados a este grupo de usuarios no tendrán ningún permiso adicional.
flume	Grupo de usuarios común. Los usuarios agregados a este grupo de usuarios no tendrán ningún permiso adicional.
launcher-job	Grupo interno de MRS, que se utiliza para enviar trabajos mediante las API de V2.

Grupo de usuarios de sistema operativo	Descripción
wheel	Grupo primario de usuario **omm** en ejecución interna de MRS.
ficommon	Grupo común del clúster de MRS que corresponde a **compcommon** para acceder a los archivos de recursos públicos almacenados en el sistema operativo del clúster.

Usuario de la base de datos

Los usuarios de base de datos del sistema de clúster de MRS incluyen usuarios de base de datos de OMS y usuarios de base de datos de DBService.

NOTA

No elimine usuarios de base de datos. De lo contrario, es posible que el clúster o los componentes no funcionen correctamente.

Tipo	Usuario predeterminado	Contraseña inicial	Descripción
Base de datos de OMS	ommdba	dbChangeMe@123456	Administrador de base de datos de OMS que realiza operaciones de mantenimiento, como crear, iniciar y detener aplicaciones.
	omm	ChangeMe@123456	Usuario para acceder a los datos de la base de datos de OMS.
DBService database	omm	dbserverAdmin@123	Administrador de la base de datos de GaussDB en el componente de DBService.
	hive	HiveUser@	Usuario para que Hive se conecte a la base de datos de DBService.
	hue	HueUser@123	Usuario para que Hue se conecte a la base de datos de DBService.
	sqoop	SqoopUser@	Usuario para que Loader se conecte a la base de datos de DBService.
	ranger	RangerUser@	Usuario para que Ranger se conecte a la base de datos de DBService.

8.12.3 Cambio de la contraseña de un usuario de sistema operativo

Escenario

Esta sección describe cómo cambiar periódicamente las contraseñas de inicio de sesión de los usuarios del sistema operativo **omm**, **ommdba** y **root** en los nodos del clúster MRS para mejorar la seguridad de O&M del sistema.

Las contraseñas de los usuarios **omm**, **ommdba** y **root** en cada nodo pueden ser diferentes.

Procedimiento

Paso 1 Inicie sesión en el nodo **Master1** y luego inicie sesión en otros nodos cuyas contraseñas de usuario del sistema operativo deben cambiarse.

Paso 2 Ejecute el siguiente comando para cambiar a usuario **root**:

sudo su - root

Paso 3 Ejecute el siguiente comando para cambiar las contraseñas de los usuarios **omm**, **ommdba** o **root**:

passwd omm

passwd ommdba

passwd root

Por ejemplo, si ejecuta el comando **omm:passwd**, el sistema muestra la siguiente información:

```
Changing password for user omm.
New password:
```

Ingrese una contraseña nueva. Las políticas de cambio de contraseña para un sistema operativo varían según el sistema operativo que se utilice.

```
Retype new password:
passwd: all authentication tokens updated successfully.
```

NOTA

Los requisitos de complejidad de contraseña predeterminados del clúster MRS son los siguientes:

- La contraseña debe tener al menos ocho caracteres.
- La contraseña debe contener al menos tres tipos de los siguientes: letras mayúsculas, minúsculas, dígitos, espacios y caracteres especiales ('~!@#$%^&*()-_=+\|[{}];:'",<.>/?).
- La nueva contraseña no puede ser la misma que las últimas cinco contraseñas históricas.

----Fin

8.12.4 Cambiar la contraseña del usuario admin

Esta sección describe cómo cambiar periódicamente la contraseña del usuario del clúster **admin** para mejorar la seguridad del sistema O&M.

Si se cambia la contraseña, la credencial de usuario descargada no estará disponible. Descargue la credencial de autenticación de nuevo y reemplace la antigua.

Cambio de la contraseña del usuario admin en el nodo de clúster

Paso 1 Actualice el cliente del nodo de gestión activo. Para obtener más información, consulte **Actualización de un cliente (Versiones anteriores a 3.x)**.

Paso 2 Inicie sesión en el nodo de gestión activo.

Paso 3 (Opcional) Para cambiar la contraseña como usuario **omm**, ejecute el siguiente comando para cambiar el usuario:

sudo su - omm

Paso 4 Ejecute el siguiente comando para cambiar al directorio del cliente, por ejemplo **/opt/client**.

cd /opt/client

Paso 5 Ejecute el siguiente comando para configurar las variables de entorno:

source bigdata_env

Paso 6 Ejecute el siguiente comando para cambiar la contraseña del usuario **admin**: Esta operación tiene efecto en todo el clúster.

kpasswd admin

Ingrese la contraseña antigua y luego ingrese una nueva contraseña dos veces.

Para el clúster , los requisitos de complejidad de contraseña predeterminados son los siguientes:

- La contraseña debe tener al menos ocho caracteres.
- La contraseña debe contener al menos tres tipos de los siguientes: letras mayúsculas, minúsculas, dígitos, espacios y caracteres especiales ('~!@#$%^&*()-_=+\| [{}];:'",<.>/?).
- La contraseña no puede ser el nombre de usuario o el nombre de usuario inverso.

----Fin

Cambiar la contraseña del usuario admin en MRS Manager

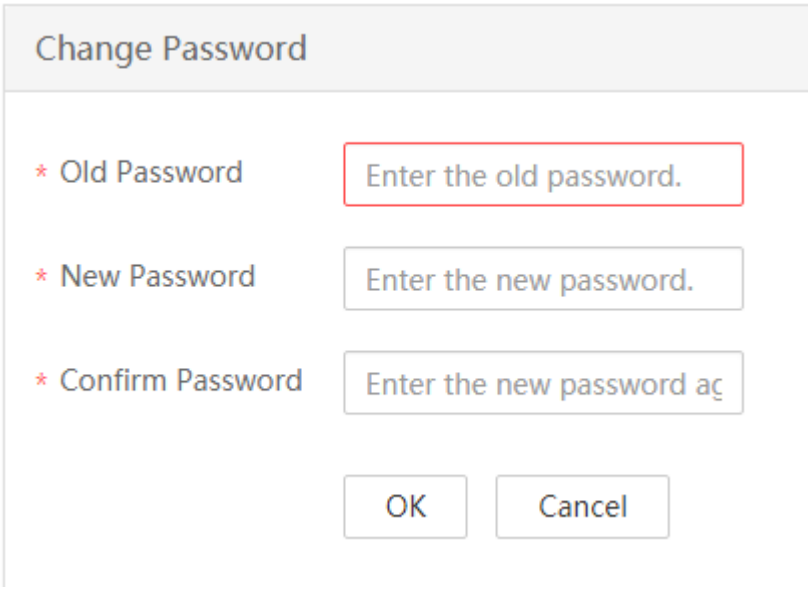
Puede cambiar la contraseña del usuario **admin** en MRS Manager solo para clústeres con autenticación Kerberos activada y clústeres con autenticación Kerberos desactivada pero la función EIP activada.

Paso 1 Inicie sesión en MRS Manager como usuario **admin**.

Paso 2 Haga clic en el nombre de usuario en la esquina superior derecha de la página y elija **Change Password**.

Paso 3 En la página **Change Password**, establezca **Old Password**, **New Password** y **Confirm Password**.

Figura 8-12 Cambiar la contraseña del usuario **admin**



NOTA

Los requisitos de complejidad de contraseña predeterminados son los siguientes:

- La contraseña debe contener entre 8 y 32 caracteres.
- La contraseña debe contener al menos tres tipos de los siguientes: letras mayúsculas, minúsculas, dígitos, espacios y caracteres especiales ('~!@#$%^&*()-_=+\|[{}];:'",<.>/?).
- La contraseña no puede ser el nombre de usuario o el nombre de usuario inverso.

Paso 4 Haga clic en **OK**. Inicie sesión en MRS Manager con la nueva contraseña.

----Fin

Restablecimiento de la contraseña para el usuario admin

Paso 1 Inicie sesión en el nodo **Master1**.

Paso 2 (Opcional) Para cambiar la contraseña como usuario **omm**, ejecute el siguiente comando para cambiar el usuario:

sudo su - omm

Paso 3 Ejecute el siguiente comando para cambiar al directorio del cliente, por ejemplo **/opt/client**:

cd /opt/client

Paso 4 Ejecute el siguiente comando para configurar las variables de entorno:

source bigdata_env

Paso 5 Ejecute el siguiente comando para iniciar sesión en la consola como usuario **kadmin/admin**:

kadmin -p kadmin/admin

NOTA

La contraseña predeterminada del usuario **kadmin/admin** es **KAdmin@123**, que caducará en su primer inicio de sesión. Cambie la contraseña como se le solicite. Mantenga la contraseña segura porque no se puede recuperar una vez que se pierde.

Paso 6 Ejecute el siguiente comando para restablecer la contraseña de un usuario que ejecuta un componente. Esta operación tiene efecto para todos los servidores.

cpw *Component running user name*

Por ejemplo, para restablecer la contraseña del usuario admin, ejecute el comando **cpw admin**.

Para el clúster, los requisitos de complejidad de contraseña predeterminados son los siguientes:

- La contraseña debe contener entre 8 y 32 caracteres.
- La contraseña debe contener al menos tres tipos de los siguientes: letras mayúsculas, minúsculas, dígitos, espacios y caracteres especiales ('~!@#$%^&*()-_=+\|[{}];:'",<.>/?).
- La contraseña no puede ser el nombre de usuario o el nombre de usuario inverso.

----Fin

8.12.5 Cambio de la contraseña del administrador de Kerberos

Escenario

Esta sección describe cómo cambiar periódicamente la contraseña del administrador de Kerberos **kadmin** del clúster MRS para mejorar la seguridad de O&M del sistema.

Si se cambia la contraseña, la credencial de usuario descargada no estará disponible. Descargue la credencial de autenticación de nuevo y reemplace la antigua.

Prerrequisitos

Se ha preparado un cliente en el nodo **Master1**.

Procedimiento

Paso 1 Inicie sesión en el nodo **Master1**.

Paso 2 (Opcional) Para cambiar la contraseña como usuario **omm**, ejecute el siguiente comando para cambiar el usuario:

sudo su - omm

Paso 3 Ejecute el siguiente comando para cambiar al directorio del cliente, por ejemplo **/opt/client**.

cd /opt/client

Paso 4 Ejecute el siguiente comando para configurar las variables de entorno:

source bigdata_env

Paso 5 Ejecute el siguiente comando para cambiar la contraseña de **kadmin/admin**. Esta operación tiene efecto para todos los servidores. Mantenga la contraseña segura porque no se puede recuperar una vez que se pierde.

kpasswd kadmin/admin

Para el clúster, los requisitos de complejidad de contraseña predeterminados son los siguientes:

- La contraseña debe tener al menos ocho caracteres.
- La contraseña debe contener al menos tres tipos de los siguientes: letras mayúsculas, minúsculas, dígitos, espacios y caracteres especiales ('~!@#$%^&*()-_=+\|[{}];:'",<.>/?).
- La contraseña no puede ser el nombre de usuario o el nombre de usuario inverso.

----Fin

8.12.6 Cambio de las contraseñas del administrador LDAP y del usuario LDAP

Escenario

Esta sección describe cómo cambiar periódicamente las contraseñas del administrador LDAP **rootdn:cn=root,dc=hadoop,dc=com** y del usuario LDAP

pg_search_dn:cn=pg_search_dn,ou=Users,dc=hadoop,dc=com para mejorar la seguridad del sistema O&M.

Impacto en el sistema

Es necesario reiniciar todos los servicios para que la nueva contraseña entre en vigor. Los servicios no están disponibles durante el reinicio.

Procedimiento

Paso 1 En MRS Manager, seleccione **Services > LdapServer > More**.

Paso 2 Haga clic en **Change Password**.

Paso 3 En el cuadro de diálogo **Change Password**, seleccione el usuario cuya contraseña debe modificarse en el cuadro desplegable **User Information**.

Paso 4 Introduzca la contraseña antigua en el cuadro de texto **Old Password** e introduzca la nueva contraseña en los cuadros de texto **New Password** y **Confirm Password**.

Los requisitos de complejidad de contraseña predeterminados son los siguientes:

- La contraseña contiene de 16 a 32 caracteres.
- La contraseña debe contener al menos tres tipos de los siguientes: letras mayúsculas, minúsculas, dígitos y caracteres especiales (`~!@#$%^&*()-_=+\|[{}];:",<.>/?).
- La contraseña no puede ser el nombre de usuario o el nombre de usuario inverso.
- La contraseña nueva no puede ser igual a la contraseña actual.

NOTA

La contraseña predeterminada del administrador LDAP **rootdn:cn=root,dc=hadoop,dc=com** es **LdapChangeMe@123** y la del usuario LDAP **pg_search_dn:cn=pg_search_dn,ou=Users,dc=hadoop,dc=com** es **pg_search_dn@123**. Cambie periódicamente las contraseñas y manténgalas seguras.

Paso 5 Seleccione **I have read the information and understand the impact** y haga clic en **OK** para confirmar la modificación y reiniciar el servicio.

----Fin

8.12.7 Cambio de la contraseña de un usuario en ejecución de componentes

Escenario

Esta sección describe cómo cambiar periódicamente la contraseña del usuario en ejecución del componente del clúster MRS para mejorar la seguridad de O&M del sistema.

Si el sistema genera aleatoriamente la contraseña inicial, restablezca la contraseña.

Si se cambia la contraseña, la credencial de usuario descargada no estará disponible. Descargue la credencial de autenticación de nuevo y reemplace la antigua.

Prerrequisitos

Se ha preparado un cliente en el nodo **Master1**.

Procedimiento

Paso 1 Inicie sesión en el nodo **Master1**.

Paso 2 (Opcional) Para cambiar la contraseña como usuario **omm**, ejecute el siguiente comando para cambiar el usuario:

sudo su - omm

Paso 3 Ejecute el siguiente comando para cambiar al directorio del cliente, por ejemplo **/opt/client**:

cd /opt/client

Paso 4 Ejecute el siguiente comando para configurar las variables de entorno:

source bigdata_env

Paso 5 Ejecute el siguiente comando para iniciar sesión en la consola como usuario **kadmin/admin**:

kadmin -p kadmin/admin

NOTA

La contraseña predeterminada del usuario **kadmin/admin** es **KAdmin@123**, que caducará en su primer inicio de sesión. Cambie la contraseña como se le solicite. Mantenga la contraseña segura porque no se puede recuperar una vez que se pierde.

Paso 6 Ejecute el siguiente comando para restablecer la contraseña de un usuario que ejecuta un componente. Esta operación tiene efecto para todos los servidores.

cpw *Component running user name*

Por ejemplo, para restablecer la contraseña del usuario admin, ejecute el comando **cpw admin**.

Para el clúster, los requisitos de complejidad de contraseña predeterminados son los siguientes:

- La contraseña debe contener entre 8 y 32 caracteres.
- La contraseña debe contener al menos tres tipos de los siguientes: letras mayúsculas, minúsculas, dígitos, espacios y caracteres especiales ('~!@#$%^&*()-_=+\|[{}];:'",<.>/?).
- La contraseña no puede ser el nombre de usuario o el nombre de usuario inverso.

----Fin

8.12.8 Cambio de la contraseña del administrador de la base de datos de OMS

Escenario

Esta sección describe cómo cambiar periódicamente la contraseña del administrador de la base de datos de OMS para mejorar la seguridad de O&M del sistema.

Procedimiento

Paso 1 Inicie sesión en el nodo de gestión activo.

NOTA

La contraseña del usuario **ommdba** no se puede cambiar en el nodo de gestión en espera. De lo contrario, es posible que el clúster no funcione correctamente. Cambie la contraseña solo en el nodo de gestión activo.

Paso 2 Ejecute el siguiente comando para cambiar el usuario:

sudo su - omm

Paso 3 Ejecute el siguiente comando para cambiar el directorio:

cd $OMS_RUN_PATH/tools

Paso 4 Ejecute el siguiente comando para cambiar la contraseña del usuario **ommdba**:

mod_db_passwd ommdba

Paso 5 Ingrese la contraseña antigua del usuario **ommdba** e ingrese una nueva contraseña dos veces.

Los requerimientos de complejidad de la contraseña son los siguientes:

- La contraseña contiene de 16 a 32 caracteres.
- La contraseña debe contener al menos tres tipos de los siguientes: letras mayúsculas, minúsculas, dígitos y caracteres especiales ('~!@#$%^&*()-_=+\|[{}];:'",<.>/?).
- La contraseña no puede ser el nombre de usuario o el nombre de usuario inverso.
- La contraseña no puede ser la misma que las últimas 20 contraseñas históricas.

Si se muestra la siguiente información, la contraseña se cambia correctamente.

```
Congratulations, update [ommdba] password successfully.
```

----Fin

8.12.9 Cambio de la contraseña del usuario de acceso a datos de la base de datos de OMS

Escenario

Esta sección describe cómo cambiar periódicamente la contraseña del usuario de acceso a datos de la base de datos de OMS para mejorar la seguridad de O&M del sistema.

Impacto en el sistema

Es necesario reiniciar el servicio OMS para que la nueva contraseña surta efecto. El servicio no está disponible durante el reinicio.

Procedimiento

Paso 1 En MRS Manager, haga clic en **System**.

Paso 2 En el área **Permission**, haga clic en **Change OMS Database Password**.

Paso 3 Busque la fila que contiene el usuario **omm**, y haga clic en **Change password** en la columna **Operation**.

Los requerimientos de complejidad de la contraseña son los siguientes:

- La contraseña debe contener entre 8 y 32 caracteres.
- La contraseña debe contener al menos tres tipos de los siguientes: letras mayúsculas, minúsculas, dígitos y caracteres especiales ('~!@#$%^&*()-_=+\|[{}];:'",<.>/?).
- La contraseña no puede ser el nombre de usuario o el nombre de usuario inverso.
- La contraseña no puede ser la misma que las últimas 20 contraseñas históricas.

Paso 4 Haga clic en **OK**. Cuando se muestre **Operation successful**, haga clic en **Finish**.

Paso 5 Busque la fila que contiene el usuario **omm** y haga clic en **Restart the OMS service** en la columna **Operation** para reiniciar la base de datos de OMS.

NOTA

Si se cambia la contraseña pero no se reinicia la base de datos OMS, el estado del usuario **omm** cambia a **Waiting to restart** y la contraseña no se puede cambiar hasta que se reinicie la base de datos de OMS.

Paso 6 En el cuadro de diálogo que se muestra, seleccione **I have read the information and understand the impact**. Haga clic en **OK** y reinicie el servicio OMS.

----Fin

8.12.10 Cambio de la contraseña de un usuario de base de datos de componentes

Escenario

Esta sección describe cómo cambiar periódicamente la contraseña del usuario de la base de datos de componentes para mejorar la seguridad de O&M del sistema.

Impacto en el sistema

Es necesario reiniciar los servicios para que la nueva contraseña entre en vigor. Los servicios no están disponibles durante el reinicio.

Procedimiento

Paso 1 En MRS Manager, haga clic en **Services** y haga clic en el nombre del servicio de usuario de base de datos que se va a modificar.

Paso 2 Determine el usuario de la base de datos del componente cuya contraseña se va a cambiar.

- Para cambiar la contraseña del usuario de la base de datos DBService, vaya a **Paso 3**.
- Para cambiar la contraseña del usuario de la base de datos de Loader, Hive o Hue, detenga primero el servicio y ejecute **Paso 3**.

Haga clic en **Stop Service**.

Paso 3 Elija **More** > **Change Password**.

Paso 4 Introduzca las contraseñas antiguas y nuevas según se le solicite.

Los requerimientos de complejidad de la contraseña son los siguientes:

- La contraseña del usuario de la base de datos de DBService contiene de 16 a 32 caracteres. La contraseña del usuario de la base de datos de Loader, Hive o Hue contiene entre 8 y 32 caracteres.

- La contraseña debe contener al menos tres tipos de los siguientes: letras mayúsculas, minúsculas, dígitos y caracteres especiales ('~!@#$%^&*()-_=+\|[{}];:'",<.>/?).
- La contraseña no puede ser el nombre de usuario o el nombre de usuario inverso.
- La contraseña no puede ser la misma que las últimas 20 contraseñas históricas.

Paso 5 Haga clic en **OK**. El sistema reinicia automáticamente el servicio correspondiente. Cuando se muestre **Operation successful**, haga clic en **Finish**.

----Fin

8.12.11 Sustitución del certificado de HA

Escenario

Los certificados de HA se utilizan para cifrar la comunicación entre los procesos activos/en espera y los procesos HA para garantizar la seguridad de la comunicación. Esta sección describe cómo reemplazar los certificados HA en los nodos de gestión activos y en espera en MRS Manager para garantizar la seguridad del producto.

El archivo de certificado y el archivo de clave pueden ser generados por el usuario.

Impacto en el sistema

MRS Manager necesita reiniciarse durante el reemplazo y no se puede acceder ni proporcionar servicios en ese momento.

Prerrequisitos

- Ha obtenido el archivo de certificado raíz HA **root-ca.crt** y el archivo de clave **root-ca.pem** que se reemplazarán.
- Ha preparado una contraseña, como **Userpwd@123** para acceder al archivo de clave.

  Para evitar posibles riesgos de seguridad, la contraseña debe cumplir los siguientes requisitos de complejidad:
  - La contraseña debe tener al menos ocho caracteres.
  - La contraseña debe contener al menos cuatro tipos de los siguientes caracteres: letras mayúsculas, minúsculas, dígitos y caracteres especiales (~`!?,.:;-_'(){}[]/<>@#$%^&*+|\=).

Procedimiento

Paso 1 Inicie sesión en el nodo de gestión activo.

Paso 2 Ejecute los siguientes comandos para cambiar el usuario:

sudo su - root

su - omm

Paso 3 Ejecute los siguientes comandos para generar **root-ca.crt** y **root-ca.pem** en el directorio **${OMS_RUN_PATH}/workspace0/ha/local/cert** en el nodo de gestión activo:

sh ${OMS_RUN_PATH}/workspace/ha/module/hacom/script/gen-cert.sh --root-ca --country=*country* **--state=***state* **--city=***city* **--company=***company* **--organize=***organize* **--common-name=***commonname* **--email=***Administrator email address* **--password=***password*

Por ejemplo, ejecute el siguiente comando:**sh ${OMS_RUN_PATH}/workspace/ha/module/hacom/script/gen-cert.sh --root-ca --country=CN --state=gd --city=sz --company=hw --organize=IT --common-name=HADOOP.COM --email=abc@hw.com --password=Userpwd@123**

El comando se ha ejecutado correctamente si se muestra la siguiente información:

```
Generate root-ca pair success.
```

Paso 4 En el nodo de gestión activo, ejecute el siguiente comando como usuario **omm** para copiar **root-ca.crt** y **root-ca.pem** al directorio **${BIGDATA_HOME}/om-0.0.1/security/certHA**:

cp -arp ${OMS_RUN_PATH}/workspace0/ha/local/cert/root-ca.* ${BIGDATA_HOME}/om-0.0.1/security/certHA

Paso 5 Copie las **root-ca.crt** y las **root-ca.pem** generadas en el nodo de gestión activo en el directorio **${BIGDATA_HOME}/om-0.0.1/security/certHA** del nodo de gestión en espera como usuario **omm**.

Paso 6 Ejecute el siguiente comando para generar un certificado HA y realizar el reemplazo automático:

sh ${BIGDATA_HOME}/om-0.0.1/sbin/replacehaSSLCert.sh

Ingrese la contraseña como se le solicite y presione **Enter**.

```
Por favor, introduzca la contraseña de ha ssl cert:
```

El certificado HA se reemplaza correctamente si se muestra la siguiente información:

```
[INFO] Succeed to replace ha ssl cert.
```

Paso 7 Ejecute el siguiente comando para reiniciar OMS:

sh ${BIGDATA_HOME}/om-0.0.1/sbin/restart-oms.sh

Se muestra la siguiente información:

```
start HA successfully.
```

Paso 8 Inicie sesión en el nodo de gestión en espera y cambie a usuario **omm**. Repita el paso **Paso 6** al paso **Paso 7**.

Ejecute el comando **sh ${BIGDATA_HOME}/om-0.0.1/sbin/status-oms.sh** para comprobar si el **HAAllResOK** del nodo de gestión es **Normal**. Acceda a MRS Manager de nuevo. Si se puede acceder a MRS Manager, la operación se realiza correctamente.

----Fin

8.12.12 Actualización de claves de clúster

Escenario

Cuando se instala un clúster, se genera automáticamente una clave de encriptación para almacenar la información de seguridad en el clúster (como todas las contraseñas de usuario de base de datos y contraseñas de acceso a archivos clave) en modo de encriptación. Una vez instalado correctamente el clúster, se recomienda actualizar periódicamente la clave de encriptación según el procedimiento siguiente.

Impacto en el sistema

- Después de actualizar una clave de clúster, se genera una nueva clave aleatoriamente en el clúster. Esta clave se utiliza para cifrar y descifrar los datos recién almacenados. La clave antigua no se elimina, y se utiliza para descifrar datos cifrados utilizando la clave antigua. Después de modificar la información de seguridad, por ejemplo, se cambia una contraseña de usuario de base de datos, la nueva contraseña se cifra usando la nueva clave.
- Cuando se actualiza la clave, se detiene el clúster y no se puede acceder a él.

Prerrequisitos

Las aplicaciones de capa superior que dependen del clúster se detienen.

Procedimiento

Paso 1 Inicie sesión en MRS Manager y elija **Services** > **More** > **Stop Cluster**.

En el cuadro de diálogo mostrado, seleccione **I have read the information and understand the impact.** Haga clic en **OK**. Espere hasta que el sistema muestre un mensaje que indique que la operación se ha realizado correctamente. Haga clic en **Finish**. El clúster se detiene correctamente.

Paso 2 Inicie sesión en el nodo de gestión activo.

Paso 3 Ejecute los siguientes comandos para cambiar el usuario:

sudo su - omm

Paso 4 Ejecute el siguiente comando para deshabilitar el cierre de sesión al finalizar el tiempo de espera:

TMOUT=0

Paso 5 Ejecute el siguiente comando para cambiar el directorio:

cd ${BIGDATA_HOME}/om-0.0.1/tools

Paso 6 Ejecute el siguiente comando para actualizar la clave de clúster:

sh updateRootKey.sh

Escriba **y** como se le solicite.

```
The root key update is a critical operation.
Do you want to continue?(y/n):
```

La clave se actualiza correctamente si se muestra la siguiente información:

```
...
Step 4-1: The key save path is obtained successfully.
...
Step 4-4: The root key is sent successfully.
```

Paso 7 En MRS Manager, seleccione **Services > More > Start Cluster**.

En el cuadro de diálogo que se muestra, haga clic en **OK**. Una vez que se muestre **Operation successful**, haga clic en **Finish**. Se inicia el clúster.

----Fin

8.13 Gestión de permisos

8.13.1 Creación de un rol

Escenario

Esta sección describe cómo crear un rol en MRS Manager y autorizar y gestionar Manager y los componentes.

Se pueden crear roles de hasta 1,000 en MRS Manager.

Prerrequisitos

Ha aprendido los requisitos de servicio.

Procedimiento

Paso 1 En MRS Manager, seleccione **System** > **Manage Role**.

Paso 2 Haga clic en **Create Role** y complete **Role Name** y **Description**.

Role Name es obligatorio y contiene de 3 a 30 dígitos, letras y guiones bajos (_). **Description** es opcional.

Paso 3 En **Permission**, establezca los permisos de rol.

1. Haga clic en **Service Name** y seleccione un nombre en **View Name**.
2. Seleccione uno o más permisos.

NOTA

- El parámetro **Permission** es opcional.
- Si selecciona **View Name** para establecer permisos de componente, puede escribir un nombre de recurso en el cuadro **Search** en la esquina superior derecha y hacer clic en . Se muestra el resultado de la búsqueda.
- El ámbito de búsqueda solo cubre directorios con permisos actuales. No puede buscar subdirectorios. La búsqueda por palabras clave admite la coincidencia difusa y no distingue entre mayúsculas y minúsculas. Los resultados de la siguiente página pueden ser buscados.

Tabla 8-36 Descripción del permiso del Manager

Gestión de permisos de soporte de recursos	Configuraciones de permiso
Alarm	Autoriza la función de alarma del Manager. Puede seleccionar **View** para ver las alarmas y **Management** para gestionar las alarmas.
Audit	Autoriza la función de registro de auditoría del Manager. Puede seleccionar **View** para ver los registros de auditoría y **Management** para gestionar los registros de auditoría.

Gestión de permisos de soporte de recursos	Configuraciones de permiso
Dashboard	Autoriza la función de descripción general del Manager. Puede seleccionar **View** para ver la descripción general del clúster.
Hosts	Autoriza la función de gestión de nodos. Puede seleccionar **View** para ver información de nodo y **Management** para gestionar nodos.
Services	Autoriza la función de gestión del servicio. Puede seleccionar **View** para ver la información del servicio y **Management** para gestionar los servicios.
System_cluster_management	Autoriza la función de gestión de clústeres de MRS. Puede seleccionar **Management** para utilizar la función de gestión de parches de MRS.
System_configuration	Autoriza la función de configuración del clúster de MRS. Puede seleccionar **Management** para configurar clústeres MRS en Manager.
System_task	Autoriza la función de tarea de clúster de MRS. Puede seleccionar **Management** para gestionar tareas periódicas de clústeres MRS en Manager.
Tenant	Autoriza la función de gestión de múltiples tenants del Manager. Puede seleccionar **Management** para gestionar varios tenants.

Tabla 8-37 Descripción del permiso de HBase

Gestión de permisos de soporte de recursos	Configuraciones de permiso
SUPER_USER_GROUP	Le otorga derechos de administrador de HBase.
Global	Tipo de recurso HBase, que indica toda la HBase.
Namespace	Tipo de recurso HBase, que indica espacio de nombres, que se utiliza para almacenar tablas de HBase. Tiene los siguientes permisos: ● **Admin**: permiso para gestionar el espacio de nombres ● **Create**: permiso para crear tablas HBase en el espacio de nombres ● **Read**: permiso para acceder al espacio de nombres ● **Write**: permiso para escribir datos en el espacio de nombres ● **Execute**: permiso para ejecutar el coprocesador (Endpoint)

Gestión de permisos de soporte de recursos	Configuraciones de permiso
Table	Tipo de recurso de HBase, que indica una tabla de datos, que se utiliza para almacenar datos. Tiene los siguientes permisos: ● **Admin**: permiso para gestionar una tabla de datos ● **Create**: permiso para crear familias de columnas y columnas en una tabla de datos ● **Read**: permiso para leer una tabla de datos ● **Write**: permiso para escribir datos en una tabla de datos ● **Execute**: permiso para ejecutar el coprocesador (Endpoint)
ColumnFamily	Tipo de recurso HBase, que indica una familia de columnas, que se utiliza para almacenar datos. Tiene los siguientes permisos: ● **Create**: permiso para crear columnas en una familia de columnas ● **Read**: permiso para leer una familia de columnas ● **Write**: permiso para escribir datos en una familia de columnas
Qualifier	Tipo de recurso de HBase, que indica una columna, que se utiliza para almacenar datos. Tiene los siguientes permisos: ● **Read**: permiso para leer una columna ● **Write**: permiso para escribir datos en una columna

De forma predeterminada, los permisos de un tipo de recurso de HBase de cada nivel son compartidos por tipos de recursos de subniveles. Sin embargo, la opción **Recursive** no está seleccionada de forma predeterminada. Por ejemplo, si los permisos **Read** y **Write** se agregan al espacio de nombres **default**, se agregan automáticamente a las tablas, familias de columnas y columnas del espacio de nombres. Si se establece un recurso secundario después del recurso primario, el permiso del recurso secundario es la unión de los permisos del recurso primario y el recurso secundario actual.

Tabla 8-38 Descripción del permiso de HDFS

Gestión de permisos de soporte de recursos	Configuraciones de permiso
Folder	Tipo de recurso de HDFS, que indica un directorio de HDFS, que se utiliza para almacenar archivos o subdirectorios. Tiene los siguientes permisos: ● **Read**: permiso para acceder al directorio de HDFS ● **Write**: permiso para escribir datos en el directorio de HDFS ● **Execute**: permiso para realizar una operación. Debe seleccionarse al agregar permisos de acceso o escritura.
Files	Tipo de recurso de HDFS, que indica un archivo en HDFS. Tiene los siguientes permisos: ● **Read**: permiso para acceder al archivo ● **Write**: permiso para escribir datos en el archivo ● **Execute**: permiso para realizar una operación. Debe seleccionarse al agregar permisos de acceso o escritura.

Los permisos de un directorio de HDFS de cada nivel no son compartidos por los tipos de directorio de subniveles de forma predeterminada. Por ejemplo, si se agregan permisos **Read** y **Execute** al directorio **tmp**, debe seleccionar **Recursive** al mismo tiempo para agregar permisos a los subdirectorios.

Tabla 8-39 Descripción del permiso de Hive

Gestión de permisos de soporte de recursos	Configuraciones de permiso
Hive Admin Privilege	Le otorga derechos de administrador de Hive.
Database	Tipo de recurso Hive, que indica una base de datos Hive, que se utiliza para almacenar tablas de Hive. Tiene los siguientes permisos: ● **Select**: permiso para consultar la base de datos de Hive ● **Delete**: permiso para realizar la operación de eliminación en la base de datos de Hive ● **Insert**: permiso para realizar la operación de inserción en la base de datos de Hive ● **Create**: permiso para realizar la operación de creación en la base de datos de Hive

Gestión de permisos de soporte de recursos	Configuraciones de permiso
Table	Tipo de recurso de Hive, que indica una tabla de Hive, que se utiliza para almacenar datos. Tiene los siguientes permisos: ● **Select**: permiso para consultar la tabla Hive ● **Delete**: permiso para realizar la operación de eliminación en la tabla Hive ● **Update**: otorga a los usuarios el permiso **Update** de la tabla Hive ● **Insert**: permiso para realizar la operación de inserción en la tabla Hive ● **Grant of Select**: permiso para conceder el permiso **Select** a otros usuarios que usen sentencias de Hive ● **Grant of Delete**: permiso para conceder el permiso **Delete** a otros usuarios que usen sentencias de Hive ● **Grant of Update**: permiso para conceder el permiso **Update** a otros usuarios que usen sentencias de Hive ● **Grant of Insert**: permiso para conceder el permiso **Insert** a otros usuarios que usen sentencias de Hive

De forma predeterminada, los permisos de un tipo de recurso de Hive de cada nivel son compartidos por los tipos de recursos de los subniveles. Sin embargo, la opción **Recursive** no está seleccionada de forma predeterminada. Por ejemplo, si se agregan permisos **Select** y **Insert** a la base de datos **default**, se agregan automáticamente a las tablas y columnas de la base de datos. Si se establece un recurso secundario después del recurso primario, el permiso del recurso secundario es la unión de los permisos del recurso primario y el recurso secundario actual.

Tabla 8-40 Descripción del permiso de Yarn

Gestión de permisos de soporte de recursos	Configuraciones de permiso
Cluster Admin Operations	Le otorga derechos de administrador de Yarn.
root	Cola de raíz de Yarn. Tiene los siguientes permisos: ● **Submit**: permiso para enviar trabajos en la cola ● **Admin**: permiso para gestionar los permisos de la cola actual

Gestión de permisos de soporte de recursos	Configuraciones de permiso
Parent Queue	Tipo de recurso de Yarn, que indica una cola principal que contiene subcolas. Una cola raíz es un tipo de cola principal. Tiene los siguientes permisos: ● **Submit**: permiso para enviar trabajos en la cola ● **Admin**: permiso para gestionar los permisos de la cola actual
Leaf Queue	Tipo de recurso de Yarn, que indica una cola de hoja. Tiene los siguientes permisos: ● **Submit**: permiso para enviar trabajos en la cola ● **Admin**: permiso para gestionar los permisos de la cola actual

De forma predeterminada, los permisos de un tipo de recurso de Yarn de cada nivel son compartidos por los tipos de recursos de los subniveles. Sin embargo, la opción **Recursive** no está seleccionada de forma predeterminada. Por ejemplo, si el permiso **Submit** se agrega a la cola **root**, se agrega automáticamente a la subcola. Los permisos heredados por las subcolas no se mostrarán como seleccionados en la tabla **Permission**. Si se establece un recurso secundario después del recurso primario, el permiso del recurso secundario es la unión de los permisos del recurso primario y el recurso secundario actual.

Tabla 8-41 Descripción del permiso de Hue

Gestión de permisos de soporte de recursos	Configuraciones de permiso
Storage Policy Admin	Le otorga permisos de administrador de política de almacenamiento.

Paso 4 Haga clic en **OK**. Vuelva a **Manage Role**.

----Fin

Tareas relacionadas

Modificación de un rol

Paso 1 En MRS Manager, haga clic en **System**.

Paso 2 En el área **Permission**, haga clic en **Manage Role**.

Paso 3 En la fila del rol que se va a modificar, haga clic en **Modify** para modificar la información del rol.

NOTA

Si cambia los permisos asignados por el rol, se tarda 3 minutos en hacer que las nuevas configuraciones surtan efecto.

Paso 4 Haga clic en **OK**. La modificación está completa.

----Fin

Eliminación de un rol

Paso 1 En MRS Manager, haga clic en **System**.

Paso 2 En el área **Permission**, haga clic en **Manage Role**.

Paso 3 En la fila del rol que se va a eliminar, haga clic en **Delete**.

Paso 4 Haga clic en **OK**. El rol se elimina.

----Fin

8.13.2 Creación de un grupo de usuarios

Escenario

Esta sección describe cómo crear grupos de usuarios y especificar sus permisos de operación en MRS Manager. La gestión de usuarios únicos o múltiples se puede unificar en los grupos de usuarios. Después de agregarse a un grupo de usuarios, los usuarios pueden obtener permisos de operación propiedad del grupo de usuarios.

Se pueden crear hasta 100 grupos de usuarios en MRS Manager.

Prerrequisitos

Los administradores han aprendido los requisitos de servicio y creado los roles requeridos por los escenarios de servicio.

Procedimiento

Paso 1 En MRS Manager, haga clic en **System**.

Paso 2 En el área **Permission**, haga clic en **Manage User Group**.

Paso 3 Encima de la lista de grupos de usuarios, haga clic en **Create User Group**.

Paso 4 Ingrese **Group Name** y **Description**.

Group Name es obligatorio y contiene de 3 a 20 dígitos, letras y guiones bajos (_). **Description** es opcional.

Paso 5 En **Role**, haga clic en **Select and Add Role** para seleccionar y agregar roles especificados.

Si no agrega los roles, el grupo de usuarios que está creando ahora no tiene permiso para usar clústeres MRS.

Paso 6 Haga clic en **OK**. Se crea el grupo de usuarios.

----Fin

Tareas relacionadas

Modificación de un grupo de usuarios

Paso 1 En MRS Manager, haga clic en **System**.

Paso 2 En el área **Permission**, haga clic en **Manage User Group**.

Paso 3 En la fila del grupo de usuarios que se va a modificar, haga clic en **Modify**.

NOTA

Si cambia los permisos de rol asignados al grupo de usuarios, se tardan 3 minutos en hacer que las nuevas configuraciones surtan efecto.

Paso 4 Haga clic en **OK**. La modificación está completa.

----Fin

Eliminación de un grupo de usuario

Paso 1 En MRS Manager, haga clic en **System**.

Paso 2 En el área **Permission**, haga clic en **Manage User Group**.

Paso 3 En la fila del grupo de usuarios que se va a eliminar, haga clic en **Delete**.

Paso 4 Haga clic en **OK**. Se elimina el grupo de usuarios.

----Fin

8.13.3 Creación de un usuario

Escenario

En esta sección se describe cómo crear usuarios en MRS Manager según los requisitos del sitio y especificar sus permisos de operación para cumplir con los requisitos de servicio.

Se pueden crear hasta 1,000 usuarios en MRS Manager.

Si es necesario utilizar una nueva política de contraseñas para la contraseña de un usuario nuevo, siga las instrucciones de **Modificación de una política de contraseñas** para modificar la política de contraseñas y, a continuación, realice las siguientes operaciones para crear un usuario.

Prerrequisitos

Los administradores han aprendido los requisitos de servicio y han creado roles y grupos de roles requeridos por los escenarios de servicio.

Procedimiento

Paso 1 En MRS Manager, haga clic en **System**.

Paso 2 En el área **Permission**, haga clic en **Manage User**.

Paso 3 Encima de la lista de usuarios, haga clic en **Create User**.

Paso 4 Configure los parámetros según se le solicite e introduzca un nombre de usuario en **User Name**.

NOTA

- Si existe un nombre de usuario, no puede crear otro nombre de usuario que solo difiera del nombre de usuario existente en el caso. Por ejemplo, si **User1** se ha creado, no puede crear **user1**.
- Cuando utilice el usuario que creó, introduzca el nombre de usuario correcto, que distingue entre mayúsculas y minúsculas.
- **User Name** es obligatorio y contiene de 3 a 20 dígitos, letras y guiones bajos (_).
- **root**, **omm** y **ommdba** son usuarios reservados del sistema. Seleccione otro nombre de usuario.

Paso 5 Establezca **User Type** en **Human-machine** o **Machine-machine**.

- Usuarios de **Human-Machine**: utilizado para O&M en MRS Manager y operaciones en clientes de componentes. Si selecciona este tipo de usuario, debe introducir una contraseña y confirmar la contraseña de **Password** y **Confirm Password** en consecuencia.
- Usuarios de **Machine-Machine**: utilizados para el desarrollo de aplicaciones de MRS. Si selecciona este tipo de usuario, no es necesario introducir una contraseña, ya que la contraseña se genera aleatoriamente.

Paso 6 En **User Group**, haga clic en **Select and Join User Group** para seleccionar grupos de usuarios y agregar usuarios a ellos.

NOTA

- Si se han agregado roles a grupos de usuarios, se puede conceder a los usuarios permisos de los roles.
- Si desea conceder a nuevos usuarios permisos de Hive, agregue los usuarios al grupo de Hive.
- Si un usuario necesita gestionar recursos de tenant, se debe asignar al grupo de usuarios el rol **Manager_tenant** y el rol correspondiente al tenant.

Paso 7 En **Primary Group**, seleccione un grupo como grupo principal para que los usuarios creen directorios y archivos. La lista desplegable contiene todos los grupos seleccionados en **User Group**.

Paso 8 En **Assign Rights by Role**, haga clic en **Select and Add Role** para agregar roles para los usuarios según los requisitos de servicio.

NOTA

- Cuando crea un usuario, si los permisos de un grupo de usuarios que se concede al usuario no pueden cumplir los requisitos de servicio, puede asignar otros roles creados al usuario. Se tarda 3 minutos en hacer que los permisos de rol otorgados al nuevo usuario tengan efecto.
- Al agregar un rol al crear un usuario se pueden especificar los derechos de usuario.
- Un nuevo usuario puede acceder a WebUIs de HDFS, HBase, Yarn, Spark y Hue incluso cuando los roles no están asignados al usuario.

Paso 9 En **Description**, proporcione una descripción basada en los requisitos de servicio en el sitio.

Description es opcional.

Paso 10 Haga clic en **OK**. Se crea el usuario.

Si se utiliza un usuario nuevo en el clúster MRS por primera vez, por ejemplo, para iniciar sesión en MRS Manager o para usar el cliente del clúster, se debe cambiar la contraseña. Para obtener más información, consulte la sección **Cambio de la contraseña de un usuario de operación**.

----Fin

8.13.4 Modificación de la información de usuario

Escenario

En esta sección se describe cómo modificar la información del usuario en MRS Manager, incluida la información sobre el grupo de usuarios, el grupo principal, el rol y la descripción.

Procedimiento

Paso 1 En MRS Manager, haga clic en **System**.

Paso 2 En el área **Permission**, haga clic en **Manage User**.

Paso 3 En la fila del usuario que se va a modificar, haga clic en **Modify**.

NOTA

Si cambia grupos de usuarios o asigna permisos de rol al usuario, tardas 3 minutos en hacer que las nuevas configuraciones surtan efecto.

Paso 4 Haga clic en **OK**. La modificación está completa.

----Fin

8.13.5 Bloqueo de un usuario

Esta sección describe cómo bloquear usuarios en clústeres de MRS. Un usuario bloqueado no puede iniciar sesión en MRS Manager ni realizar autenticación de seguridad en el clúster.

Un usuario bloqueado puede ser desbloqueado por un administrador manualmente o hasta que expire la duración del bloqueo. Puede bloquear a un usuario mediante cualquiera de los métodos siguientes:

- Bloqueo automático: Ajuste **Number of Password Retries** en **Configure Password Policy**. Si los intentos de inicio de sesión del usuario exceden el valor del parámetro, el usuario se bloquea automáticamente. Para obtener más información, consulte **Modificación de una política de contraseñas**.
- Bloqueo manual: El administrador bloquea manualmente a un usuario.

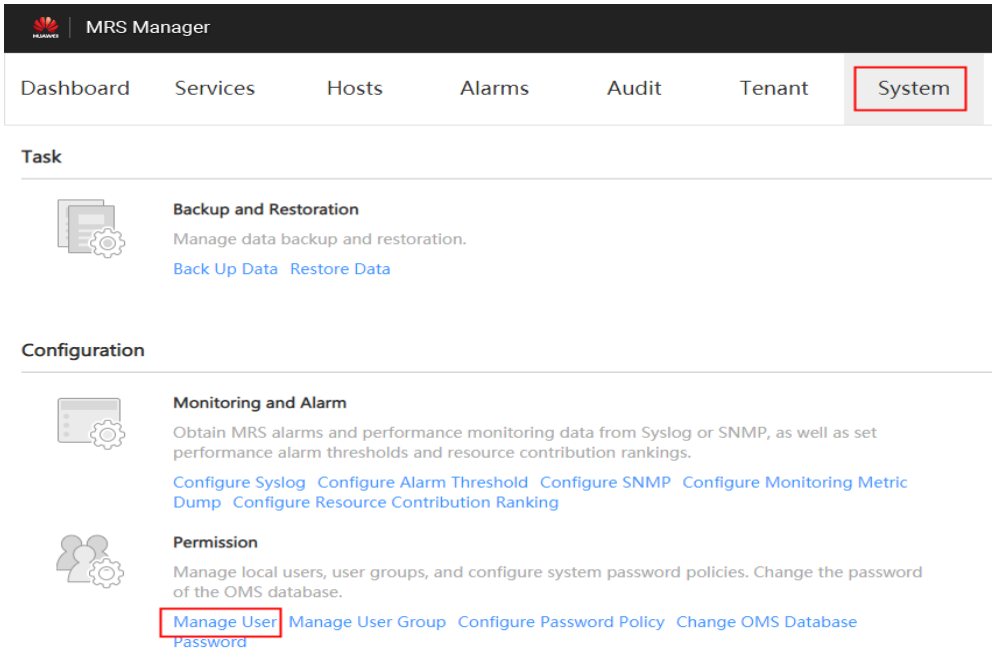
A continuación se describe cómo bloquear manualmente un usuario. Los usuarios de **Machine-Machine** no se pueden bloquear.

Procedimiento

Paso 1 En MRS Manager, haga clic en **System**.

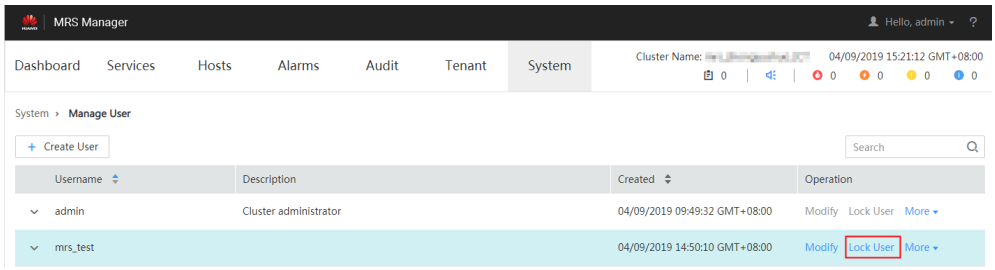
Paso 2 En el área **Permission**, haga clic en **Manage User**.

Figura 8-13 Gestión de usuarios.



Paso 3 En la fila del usuario que se va a bloquear, haga clic en **Lock User**.

Figura 8-14 Bloqueo de un usuario



Paso 4 En la ventana que se muestra, haga clic en **Yes** para bloquear al usuario.

----Fin

8.13.6 Desbloquear un usuario

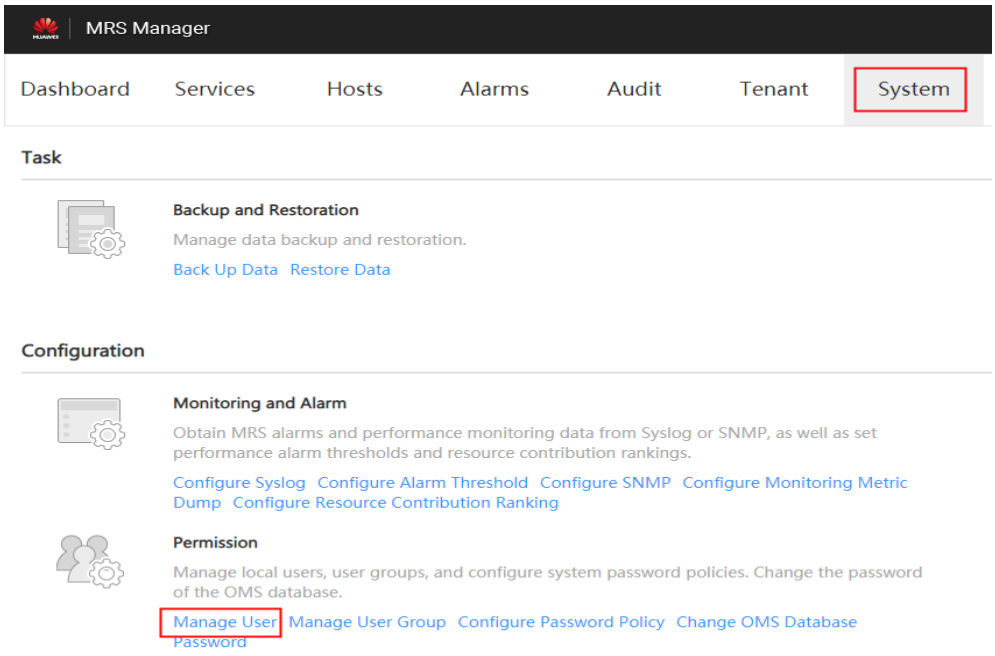
Si un usuario está bloqueado porque el número de intentos de inicio de sesión excede el valor de **Number of Password Retries** o el usuario está bloqueado manualmente por el administrador, el administrador puede desbloquear al usuario en MRS Manager.

Procedimiento

Paso 1 En MRS Manager, haga clic en **System**.

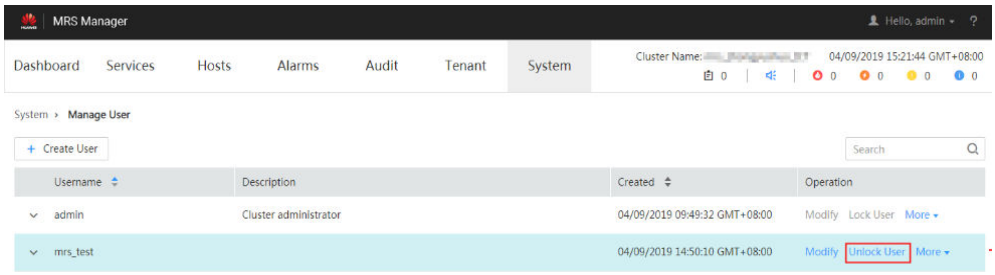
Paso 2 En el área **Permission**, haga clic en **Manage User**.

Figura 8-15 Gestión de usuarios.



Paso 3 En la fila del usuario que se va a desbloquear, haga clic en **Unlock User**.

Figura 8-16 Desbloquear un usuario



Paso 4 En la ventana que se muestra, haga clic en **Yes** para desbloquear al usuario.

----Fin

8.13.7 Eliminación de un usuario

El administrador puede eliminar un usuario del clúster de MRS que no sea necesario en MRS Manager.

NOTA

Si desea crear un nuevo usuario con el mismo nombre que el usuario A después de eliminar el usuario A que ha enviado un trabajo en el cliente o en la consola de MRS, debe eliminar las carpetas residuales del usuario A al eliminar el usuario A. De lo contrario, el usuario A recién creado puede fallar al enviar un trabajo.

Para eliminar carpetas residuales, inicie sesión en cada nodo de Core del clúster MRS y ejecute los siguientes comandos. En los siguientes comandos **$user** indica la carpeta con el nombre de usuario.

cd /srv/BigData/hadoop/data1/nm/localdir/usercache/

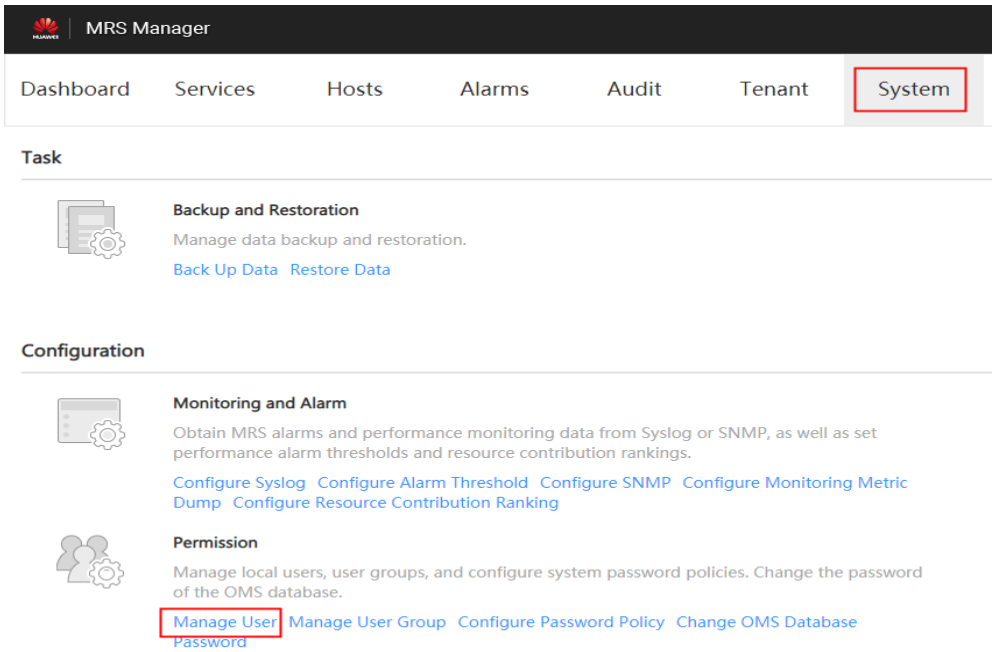
rm -rf $user

Procedimiento

Paso 1 En MRS Manager, haga clic en **System**.

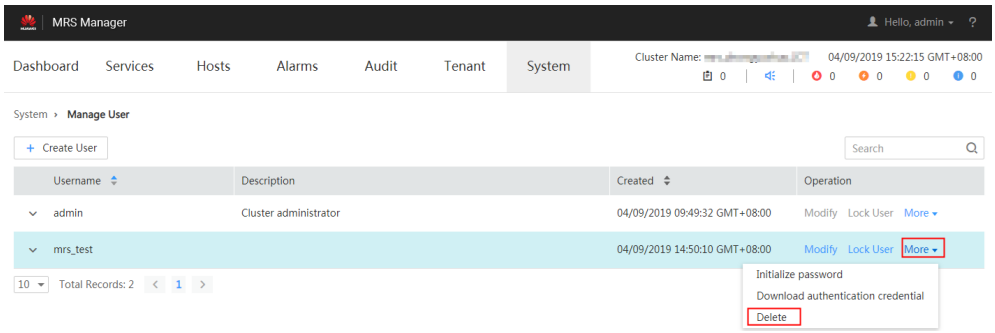
Paso 2 En el área **Permission**, haga clic en **Manage User**.

Figura 8-17 Gestión de usuarios.



Paso 3 En la fila que contiene el usuario que se va a eliminar, elija **More** > **Delete**.

Figura 8-18 Eliminación de un usuario



Paso 4 Haga clic en **OK**.

----Fin

8.13.8 Cambio de la contraseña de un usuario de operación

Escenario

Las contraseñas de los usuarios del sistema **Human-Machine** deben cambiarse regularmente para garantizar la seguridad del clúster MRS. Esta sección describe cómo cambiar sus contraseñas en MRS Manager.

Si es necesario utilizar una nueva política de contraseñas para la contraseña modificada por el usuario, siga las instrucciones de **Modificación de una política de contraseñas** para modificar la política de contraseñas y, a continuación, realice las siguientes operaciones para modificar la contraseña.

Impacto en el sistema

Si ha descargado un archivo de autenticación de usuario, descárguelo de nuevo y obtenga el archivo keytab después de cambiar la contraseña del usuario del clúster MRS.

Prerrequisitos

- Ha obtenido la política de contraseñas actual.
- Usted ha obtenido la URL para acceder a MRS Manager.

Procedimiento

Paso 1 En MRS Manager, mueva el cursor del ratón a  en la esquina superior derecha.

En el menú que se muestra, seleccione **Change Password**.

Paso 2 Rellene el **Old Password**, **New Password** y el **Confirm Password**. Haga clic en **OK**.

Para el clúster, los requisitos de complejidad de contraseña predeterminados son los siguientes:

- La contraseña debe contener entre 8 y 32 caracteres.
- La contraseña debe contener al menos tres tipos de los siguientes: letras mayúsculas, minúsculas, dígitos, espacios y caracteres especiales ('~!@#$%^&*()-_=+\| [{}];:'",<.>/?).
- La contraseña no puede ser el nombre de usuario o el nombre de usuario inverso.

----Fin

8.13.9 Inicialización de la contraseña de un usuario del sistema

Escenario

Esta sección describe cómo inicializar una contraseña en MRS Manager si un usuario olvida la contraseña o la contraseña de una cuenta pública necesita cambiarse regularmente. Después de la inicialización de la contraseña, el usuario debe cambiar la contraseña en el primer inicio de sesión.

Impacto en el sistema

Si ha descargado un archivo de autenticación de usuario, descárguelo de nuevo y obtenga el archivo keytab después de inicializar la contraseña del usuario del clúster de MRS.

Inicialización de la contraseña de un usuario humano-máquina

Paso 1 En MRS Manager, haga clic en **System**.

Paso 2 En el área **Permission**, haga clic en **Manage User**.

Paso 3 Busque la fila que contiene el usuario cuya contraseña se va a inicializar, elija **More** > **Initialize password** y cambie la contraseña según se le solicite.

En la ventana que se muestra, introduzca la contraseña de la cuenta de administrador actual y haga clic en **OK**. A continuación, en **Initialize password**, haga clic en **OK**.

Para el clúster, los requisitos de complejidad de contraseña predeterminados son los siguientes:

- La contraseña debe contener entre 8 y 32 caracteres.
- La contraseña debe contener al menos tres tipos de los siguientes: letras mayúsculas, minúsculas, dígitos, espacios y caracteres especiales ('~!@#$%^&*()-_=+\|[{}];:'",<.>/?).
- La contraseña no puede ser el nombre de usuario o el nombre de usuario inverso.

----Fin

Inicialización de la contraseña de un usuario máquina-máquina

Paso 1 Prepare un cliente basado en las condiciones del servicio e inicie sesión en el nodo donde está instalado el cliente.

Paso 2 Ejecute el siguiente comando para cambiar el usuario:

sudo su - omm

Paso 3 Ejecute el siguiente comando para cambiar al directorio del cliente, por ejemplo **/opt/client**:

cd /opt/client

Paso 4 Ejecute el siguiente comando para configurar las variables de entorno:

source bigdata_env

Paso 5 Ejecute el siguiente comando para iniciar sesión en la consola como usuario **kadmin/admin**:

kadmin -p kadmin/admin

NOTA

La contraseña predeterminada del usuario **kadmin/admin** es **KAdmin@123**, que caducará en su primer inicio de sesión. Cambie la contraseña según se le indique y mantenga segura la nueva contraseña.

Paso 6 Ejecute el siguiente comando para restablecer la contraseña de un usuario que ejecuta un componente. Esta operación tiene efecto para todos los servidores.

cpw *Component running user name*

Por ejemplo, **cpw oms/manager**.

Para el clúster, los requisitos de complejidad de contraseña predeterminados son los siguientes:

- La contraseña debe contener entre 8 y 32 caracteres.
- La contraseña debe contener al menos tres tipos de los siguientes: letras mayúsculas, minúsculas, dígitos, espacios y caracteres especiales ('~!@#$%^&*()-_=+\|[{}];:'",<.>/?).
- La contraseña no puede ser el nombre de usuario o el nombre de usuario inverso.

----Fin

8.13.10 Descargar un archivo de autenticación de usuario

Escenario

Cuando un usuario desarrolla aplicaciones de big data y las ejecuta en un clúster MRS que admite la autenticación de Kerberos, el usuario debe preparar un archivo de autenticación de usuario para acceder al clúster de MRS. El archivo keytab en el archivo de autenticación se puede utilizar para la autenticación del usuario.

Esta sección describe cómo descargar un archivo de autenticación de usuario y exportar el archivo keytab en MRS Manager.

NOTA

- Antes de descargar un archivo de autenticación de usuario de **Human-machine**, cambie la contraseña del usuario en MRS Manager para que la contraseña inicial establecida por el administrador no sea válida. De lo contrario, no se puede utilizar el archivo keytab exportado. Para obtener más información, consulte **Cambio de la contraseña de un usuario de operación**.
- Después de cambiar una contraseña de usuario, el archivo keytab exportado no es válido y debe exportar un archivo keytab de nuevo.

Procedimiento

Paso 1 En MRS Manager, haga clic en **System**.

Paso 2 En el área **Permission**, haga clic en **Manage User**.

Paso 3 En la fila del usuario para el que desea exportar el archivo keytab, elija **More** > **Download authentication credential** para descargar el archivo de autenticación. Después de que el archivo se genere automáticamente, guárdelo en una ruta especificada y guárdelo correctamente.

Paso 4 Abra el archivo de autenticación con un programa de descompresión.

- **user.keytab** indica un archivo keytab del usuario utilizado para la autenticación del usuario.
- **krb5.conf** indica el archivo de configuración del servidor de autenticación. La aplicación se conecta al servidor de autenticación de acuerdo con la información del archivo de configuración al autenticar usuarios.

----Fin

8.13.11 Modificación de una política de contraseñas

Escenario

Esta sección describe cómo establecer reglas de seguridad de contraseña y inicio de sesión de usuario, así como reglas de bloqueo de usuario. Las políticas de contraseñas establecidas en MRS Manager solo tienen efecto para los usuarios de **Human-machine** porque las contraseñas de los usuarios de **Machine-machine** se generan aleatoriamente.

Si se necesita utilizar una nueva política de contraseñas para la contraseña de un nuevo usuario o la contraseña modificada por el usuario, realice las siguientes operaciones para modificar la política de contraseñas primero y, a continuación, cree un usuario o cambie la contraseña siguiendo las instrucciones de **Creación de un usuario** o **Cambio de la contraseña de un usuario de operación**.

AVISO

Modifique las políticas de contraseñas en función de los requisitos de seguridad del servicio, ya que implican la seguridad de gestión de usuarios. De lo contrario, pueden producirse riesgos de seguridad.

Procedimiento

Paso 1 En MRS Manager, haga clic en **System**.

Paso 2 Haga clic en **Configure Password Policy**.

Paso 3 Modifique las políticas de contraseñas según se le solicite. Para obtener más información sobre los parámetros, consulte la tabla siguiente:

Tabla 8-42 Descripción del parámetro de política de contraseñas

Parámetro	Descripción
Minimum Password Length	Indica el número mínimo de caracteres que contiene una contraseña. El valor varía de 8 a 32. El valor predeterminado es **8**.
Number of Character Types	Indica el número mínimo de tipos de caracteres que contiene una contraseña. Los tipos de caracteres son letras mayúsculas, minúsculas, dígitos, espacios y caracteres especiales (~`!?,.:;-_'(){}[]/<>@#$%^&*+|\=). El valor puede ser **3** o **4**. El valor predeterminado **3** indica que la contraseña debe contener al menos tres tipos de los siguientes caracteres: letras mayúsculas, minúsculas, dígitos, caracteres especiales y espacios.
Password Validity Period (days)	Indica el período de validez (días) de una contraseña. El valor varía de 0 a 90. 0 significa que la contraseña es válida permanentemente. El valor predeterminado es **90**.

Parámetro	Descripción
Password Expiration Notification Days	Indica el número de días de antelación que se notifica a los usuarios que sus contraseñas están a punto de caducar. Después de establecer el valor, si la diferencia entre el tiempo de clúster y el tiempo de caducidad de la contraseña es menor que este valor, el usuario recibe notificaciones de caducidad de la contraseña. Cuando un usuario inicia sesión en MRS Manager, se muestra un mensaje que indica que la contraseña está a punto de caducar y le pregunta al usuario si desea cambiar la contraseña. El valor varía de **0** a *X* (*X* debe establecerse en la mitad del período de validez de la contraseña y redondearse hacia abajo). El valor **0** indica que no se envía ninguna notificación. El valor predeterminado es **5**.
Interval of Resetting Authentication Failure Count (min)	Indica el intervalo de retención de intentos de contraseña incorrectos, en minutos. El valor varía de 0 a 1440. 0 indica que los intentos de contraseña incorrectos se conservan permanentemente y 1440 indica que los intentos de contraseña incorrectos se conservan durante un día. El valor predeterminado es **5**.
Number of Password Retries	Indica el número de contraseñas incorrectas consecutivas permitidas antes de que el sistema bloquee al usuario. El valor varía de 3 a 30. El valor predeterminado es **5**.
Account Lock Duration (min)	Indica el período de tiempo durante el que un usuario está bloqueado cuando se cumplen las condiciones de bloqueo del usuario. El valor varía de 5 a 120. El valor predeterminado es **5**.

----Fin

8.14 Gestión de permisos multiusuario de MRS

8.14.1 Usuarios y permisos de clústeres de MRS

Descripción

- **Usuarios de clúster de MRS**

  Indicar las cuentas de seguridad de Manager, incluidos nombres de usuario y contraseñas. Estas cuentas se utilizan para acceder a recursos en clústeres de MRS. Cada clúster de MRS en el que se habilita la autenticación de Kerberos puede tener varios usuarios.

- **Roles de clúster de MRS**

  Antes de utilizar recursos en un clúster de MRS, los usuarios deben obtener el permiso de acceso definido por los objetos del clúster de MRS. Un rol de clúster es un conjunto de uno o más permisos. Por ejemplo, el permiso para acceder a un directorio en HDFS debe configurarse en el directorio especificado y guardarse en un rol.

Manager proporciona la función de gestión de permisos de usuario para clústeres de MRS, facilitando la gestión de permisos y usuarios.

- Gestión de permisos: adopta el modo de control de acceso basado en roles (RBAC). En este modo, los permisos se otorgan por rol para formar un conjunto de permisos. Después de asignar uno o más roles a un usuario, el usuario puede obtener los permisos de los roles.
- Gestión de usuarios: utiliza MRS Manager para gestionar de manera uniforme a los usuarios, adopta el protocolo de Kerberos para la verificación de identidad de usuario y emplea el protocolo ligero de acceso a directorios (LDAP) para almacenar información de usuario.

Gestión de permisos

Los permisos proporcionados por los clústeres de MRS incluyen los permisos de O&M de Manager y componentes (como HDFS, HBase, Hive y Yarn). En la aplicación real, los permisos deben asignarse a cada usuario en función de los escenarios de servicio. Para facilitar la gestión de permisos, Manager introduce la función de rol que permite a los administradores seleccionar y asignar permisos especificados. Los permisos se visualizan y gestionan de forma centralizada en conjuntos de permisos, lo que mejora la experiencia del usuario.

Un rol es una entidad lógica que contiene uno o más permisos. Los permisos se asignan a los roles, y los usuarios pueden obtener los permisos obteniendo los roles.

Un rol puede tener varios permisos y un usuario puede estar enlazado a varios roles.

- Función 1: se asignan permisos de operación A y B. Después de asignar el rol 1 a los usuarios a y b, los usuarios a y b pueden obtener permisos de operación A y B.
- Función 2: se le asigna el permiso de operación C. Después de asignar el rol 2 a los usuarios c y d, los usuarios c y d pueden obtener el permiso de operación C.
- Función 3: se asignan permisos de operación D y F. Después de asignar el rol 3 al usuario a, el usuario a puede obtener los permisos de operación D y F.

Por ejemplo, si un usuario MRS está enlazado al rol de administrador, el usuario se convierte en administrador del clúster de MRS.

Tabla 8-43 muestra los roles que se crean de forma predeterminada en Manager.

Tabla 8-43 Roles y descripción predeterminados

Rol predeterminado	Descripción
default	Rol del tenant
Manager_administrator	Administrador de Manager: Este rol tiene el permiso para gestionar MRS Manager.

Rol predeterminado	Descripción
Manager_auditor	Auditor de Manager: Este rol tiene permiso para ver y gestionar la información de auditoría.
Manager_operator	Operador de Manager: Este rol tiene todos los permisos, excepto los permisos de tenant, configuración y gestión de clústeres.
Manager_viewer	Visor de Manager: Este rol tiene permiso para ver la información sobre sistemas, servicios, hosts, alarmas y registros de auditoría.
System_administrator	Administrador del sistema: Este rol tiene los permisos de los administradores de Manager y de todos los administradores de servicios.
Manager_tenant	Visor del tenant de Manager: Este rol tiene permiso para ver información en la página **Tenant** en MRS Manager.

Al crear un rol en Manager, puede realizar la gestión de derechos para Manager y componentes, como se muestra en **Tabla 8-44**.

Tabla 8-44 Gestión de permisos de Manager y componentes

Permiso	Descripción
Manager	Permiso de acceso e inicio de sesión de Manager.
HBase	Permiso de administrador de HBase y permiso para acceder a las tablas y familias de columnas de HBase.
HDFS	Permiso de directorio y archivo de HDFS.
Hive	● Hive Admin Privilege Permiso de administrador de Hive. ● Hive Read Write Privileges Permiso de gestión de tablas de datos de Hive para establecer y gestionar los datos de las tablas creadas.
Hue	Permisos de administrador de política de almacenamiento.
Yarn	● Cluster Admin Operations Permiso de administrador de Yarn. ● Scheduler Queue Permiso de gestión de recursos de cola.

Gestión de usuarios.

Los clústeres de MRS que admiten la autenticación de Kerberos utilizan el protocolo de Kerberos y LDAP para la gestión de usuarios.

- Kerberos verifica la identidad del usuario cuando un usuario inicia sesión en Manager o utiliza un cliente de componente. La verificación de identidad no es necesaria para los clústeres con la autenticación Kerberos deshabilitada.
- LDAP se utiliza para almacenar información de usuario, incluidos registros de usuario, información de grupo de usuarios e información de permisos.

Los clústeres de MRS pueden actualizar automáticamente los datos de usuario de Kerberos y LDAP cuando se crean o modifican usuarios en Manager. También pueden realizar automáticamente la verificación y autenticación de la identidad del usuario y obtener información del usuario cuando un usuario inicia sesión en Manager o utiliza un cliente de componente. Esto garantiza la seguridad de la gestión de usuarios y simplifica las tareas de gestión de usuarios. Manager también proporciona la función de grupo de usuarios para gestionar uno o varios usuarios por tipo:

- Un grupo de usuarios es un conjunto de usuarios que se pueden utilizar para gestionar usuarios por tipo. Los usuarios del sistema pueden existir de forma independiente o en un grupo de usuarios.
- Después de agregar un usuario a un grupo de usuarios al que se asignan roles, el permiso de rol del grupo de usuarios se asigna al usuario.

Tabla 8-45 muestra los grupos de usuarios que se crean de forma predeterminada en MRS Manager en MRS 3.x o anterior.

Para obtener más información sobre los grupos de usuarios predeterminados en FusionInsight Manager de MRS 3.*x* o posterior, consulte **Grupo de usuario**.

Tabla 8-45 Grupos de usuarios y descripción predeterminados

Grupo de usuario	Descripción
hadoop	Los usuarios agregados a este grupo de usuarios tienen permiso para enviar tareas a todas las colas de Yarn.
hbase	Grupo de usuarios común. Los usuarios agregados a este grupo de usuarios no tendrán ningún permiso adicional.
hive	Los usuarios agregados a este grupo de usuarios pueden usar Hive.
spark	Grupo de usuarios común. Los usuarios agregados a este grupo de usuarios no tendrán ningún permiso adicional.
supergroup	Los usuarios agregados a este grupo de usuarios pueden tener el permiso de administrador de HBase, HDFS y Yarn y pueden usar Hive.
flume	Grupo de usuarios común. Los usuarios agregados a este grupo de usuarios no tendrán ningún permiso adicional.
kafka	Grupo de usuarios comunes de Kafka. Los usuarios agregados a este grupo deben tener permiso de lectura y escritura por parte de los usuarios del grupo **kafkaadmin** antes de acceder a los topics deseados.
kafkasuperuser	Los usuarios agregados a este grupo tienen permisos para leer datos y escribir datos en todos los topics.

Grupo de usuario	Descripción
kafkaadmin	Grupo de administradores de Kafka. Los usuarios agregados a este grupo tienen los permisos para crear, eliminar, autorizar, así como leer y escribir datos para todos los topics.
storm	Grupo de usuarios común de Storm. Los usuarios agregados a este grupo tienen los permisos para enviar topologías y gestionar sus propias topologías.
stormadmin	Grupo de usuarios de administrador de Storm. Los usuarios agregados a este grupo tienen los permisos para enviar topologías y gestionar sus propias topologías.

Usuario **admin** se crea de forma predeterminada para los clústeres de MRS con autenticación de Kerberos activada y se utiliza para que los administradores mantengan los clústeres.

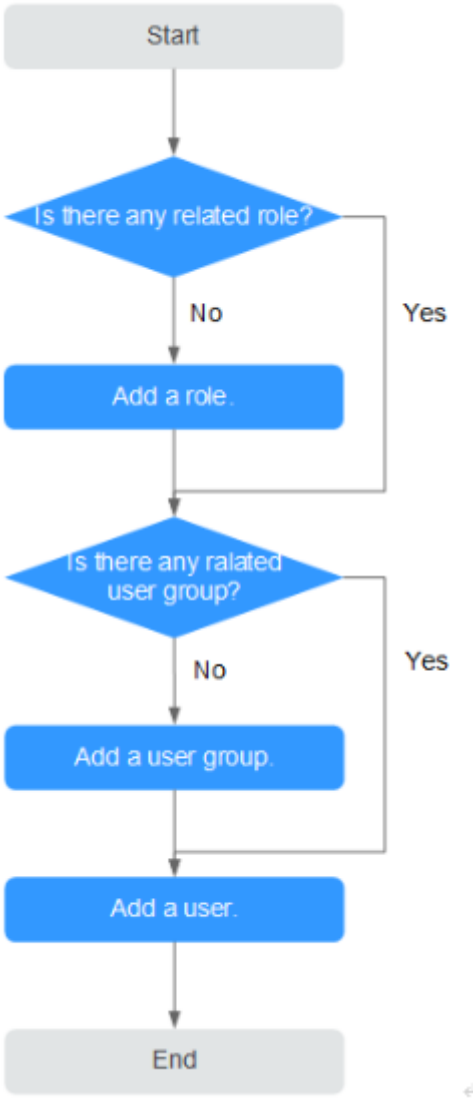
Descripción del proceso

En la práctica, los usuarios del clúster de MRS deben comprender los escenarios de servicio de big data y planificar los permisos de usuario. A continuación, cree roles y asigne permisos a los roles en MRS Manager para cumplir con los requisitos de servicio. Manager proporciona la función de grupo de usuarios para que los administradores creen grupos de usuarios para gestionar usuarios de uno o varios escenarios de servicio del mismo tipo.

NOTA

Si un rol tiene el permiso de HDFS, HBase, Hive o Yarn respectivamente, el rol solo puede utilizar las funciones correspondientes del componente. Para usar Manager, se debe agregar el permiso Manager correspondiente al rol.

Figura 8-19 Proceso de creación de un usuario



8.14.2 Usuarios predeterminados de clústeres con autenticación de Kerberos habilitada

Clasificación de usuario

El clúster de MRS proporciona los siguientes tres tipos de usuarios. Se aconseja a los usuarios que cambien periódicamente las contraseñas. No se recomienda utilizar las contraseñas predeterminadas.

Tipo de usuario	Descripción
Usuario del sistema	● Usuario creado en Manager for MRS cluster O&M y escenarios de servicio. Hay dos tipos de usuarios: – Usuario **Human-machine**: utilizado para escenarios de O&M de Manager y escenarios de operación de cliente de componentes. – Usuario **Machine-machine**: utilizado para escenarios de desarrollo de aplicaciones de clúster de MRS. ● Usuario que ejecuta procesos de OMS.
Usuario interno del sistema	Usuario interno que realiza las comunicaciones de proceso, guarda la información del grupo de usuarios y asocia los permisos de usuario.
Usuario de la base de datos	● Usuario que gestiona la base de datos de OMS y accede a los datos. ● Usuario que ejecuta la base de datos de componentes de servicio (Hive, Hue, Loader y DBService)

Usuario del sistema

NOTA

- Se requiere usuario **Idap** del sistema operativo en el clúster de MRS. No elimine esta cuenta. De lo contrario, es posible que el clúster no funcione correctamente. Las políticas de gestión de contraseñas son mantenidas por los usuarios de la operación.
- Restablecer las contraseñas cuando cambie las contraseñas de usuario **ommdba** y usuario **omm** por primera vez. Cambie las contraseñas periódicamente después de recuperarlas.

Tipo	Nombre de usuario	Contraseña inicial	Descripción
Administrador del sistema del clúster de MRS	admin	Especificado por el usuario durante la creación del clúster.	Administrador de Manager con los siguientes permisos: ● Permisos de usuario comunes de HDFS y ZooKeeper. ● Permisos para enviar y consultar tareas de MapReduce y Yarn, gestionar colas de Yarn y acceder a la Yarn web UI. ● Permisos para enviar, consultar, activar, desactivar, reasignar, eliminar topologías y operar todas las topologías del servicio Storm. ● Permisos para crear, eliminar, autorizar, reasignar, consumir, escribir y consultar temas del servicio Kafka.
Usuario del sistema operativo del nodo del clúster de MRS	omm	Generado aleatoriamente por el sistema.	Usuario en ejecución interna del sistema de clúster de MRS. Este usuario es un usuario del sistema operativo generado en todos los nodos y no requiere una contraseña unificada.
Usuario del sistema operativo del nodo del clúster de MRS	root	Establecido por el usuario.	Usuario para iniciar sesión en el nodo del clúster de MRS. Este usuario es un usuario de OS generado en todos los nodos.

Usuarios internos del sistema

NOTA

No elimine los siguientes usuarios internos del sistema. De lo contrario, es posible que el clúster o los componentes no funcionen correctamente.

Tipo	Usuario predeterminado	Contraseña inicial	Descripción
Usuario en ejecución de componentes	hdfs	Hdfs@123	Este usuario es administrador del sistema HDFS y tiene los siguientes permisos: 1. Permisos de operación del sistema de archivos: ● Visualiza, modifica y crea archivos. ● Visualiza y crea directorios. ● Visualiza y modifica los grupos a los que pertenecen los archivos. ● Visualiza y establece cuotas de disco para los usuarios. 2. Permisos de operación de gestión de HDFS: ● Visualiza el estado de la interfaz de usuario web. ● Muestra y establece el estado HDFS activo y en espera. ● Entra y sale del HDFS en modo de seguridad. ● Comprueba el sistema de archivos HDFS.

Tipo	Usuario predeterminado	Contraseña inicial	Descripción
	hbase	Hbase@123	Este usuario es un administrador del sistema HBase y tiene los siguientes permisos: ● Permiso de gestión de clústeres: operaciones de **Enable** y **Disable** en tablas para desencadenar operaciones de MajorCompact y ACL. ● Concede y revoca permisos y cierra el clúster. ● Permiso de gestión de tablas: crea, modifica y elimina tablas. ● Permiso de gestión de datos: lee y escribe datos en tablas, familias de columnas y columnas. ● Accede a la interfaz de usuario web de HBase.
	mapred	Mapred@123	Este usuario es administrador del sistema de MapReduce y tiene los siguientes permisos: ● Envía, detiene y visualiza las tareas de MapReduce. ● Modifica los parámetros de configuración de Yarn. ● Accede a la interfaz de usuario web de Yarn y MapReduce.
	spark	Spark@123	Este usuario es el administrador de sistema Spark y tiene los siguientes permisos: ● Accede a la interfaz de usuario web de Spark. ● Envía tareas de Spark.

Información del grupo de usuarios

Grupo de usuarios predeterminado	Descripción
hadoop	Los usuarios agregados a este grupo de usuarios tienen permiso para enviar tareas a todas las colas de Yarn.

Grupo de usuarios predeterminado	Descripción
hbase	Grupo de usuarios común. Los usuarios agregados a este grupo de usuarios no tendrán ningún permiso adicional.
hive	Los usuarios agregados a este grupo de usuarios pueden usar Hive.
spark	Grupo de usuarios común. Los usuarios agregados a este grupo de usuarios no tendrán ningún permiso adicional.
supergroup	Los usuarios agregados a este grupo de usuarios pueden tener el permiso de administrador de HBase, HDFS y Yarn y pueden usar Hive.
check_sec_ldap	Se utiliza para probar si el LDAP activo funciona correctamente. Este grupo de usuarios se genera aleatoriamente en una prueba y se elimina automáticamente una vez completada la prueba. Este es un grupo de usuarios interno del sistema que se utiliza solo entre componentes.
Manager_tenant	Grupo de usuarios del sistema de tenant, que es un grupo de usuarios del sistema interno que se utiliza solo entre componentes.
System_administrator	Grupo de administradores del sistema de clúster de MRS, que es un grupo de usuarios del sistema interno que se utiliza solo entre componentes.
Manager_viewer	Grupo de visualizadores del sistema de MRS Manager, que es un grupo de usuarios del sistema interno que se utiliza solo entre componentes.
Manager_operator	Grupo de operadores del sistema de MRS Manager, que es un grupo de usuarios del sistema interno que se utiliza solo entre componentes.
Manager_auditor	Grupo de auditores del sistema de MRS Manager, que es un grupo interno de usuarios del sistema utilizado solo entre componentes.
Manager_administrator	Grupo de administradores del sistema de MRS Manager, que es un grupo de usuarios del sistema interno que se utiliza solo entre componentes.
compcommon	Grupo de sistema interno para acceder a recursos públicos en un clúster. Todos los usuarios del sistema y los usuarios en ejecución del sistema se agregan a este grupo de usuarios de forma predeterminada.
default_1000	Grupo de usuarios creado para tenants, que es un grupo de usuarios interno del sistema que se utiliza solo entre componentes.

Grupo de usuarios predeterminado	Descripción
kafka	Grupo de usuarios comunes de Kafka. Los usuarios agregados a este grupo deben tener permiso de lectura y escritura por parte de los usuarios del grupo **kafkaadmin** antes de acceder a los topics deseados.
kafkasuperuser	Los usuarios agregados a este grupo tienen permisos para leer datos y escribir datos en todos los topics.
kafkaadmin	Grupo de administradores de Kafka. Los usuarios agregados a este grupo tienen los permisos para crear, eliminar, autorizar, así como leer y escribir datos para todos los topics.
storm	Grupo de usuarios común de Storm. Los usuarios agregados a este grupo tienen los permisos para enviar topologías y gestionar sus propias topologías.
stormadmin	Grupo de usuarios de administrador de Storm. Los usuarios agregados a este grupo tienen los permisos para enviar topologías y gestionar sus propias topologías.
opentsdb	Grupo de usuarios común. Los usuarios agregados a este grupo de usuarios no tendrán ningún permiso adicional.
presto	Grupo de usuarios común. Los usuarios agregados a este grupo de usuarios no tendrán ningún permiso adicional.
flume	Grupo de usuarios común. Los usuarios agregados a este grupo de usuarios no tendrán ningún permiso adicional.
launcher-job	Grupo interno de MRS, que se utiliza para enviar trabajos mediante las API de V2.

Grupo de usuarios de sistema operativo	Descripción
wheel	Grupo primario de usuario **omm** en ejecución interna de MRS.
ficommon	Grupo común del clúster de MRS que corresponde a **compcommon** para acceder a los archivos de recursos públicos almacenados en el sistema operativo del clúster.

Usuario de la base de datos

Los usuarios de base de datos del sistema de clúster de MRS incluyen usuarios de base de datos de OMS y usuarios de base de datos de DBService.

NOTA

No elimine usuarios de base de datos. De lo contrario, es posible que el clúster o los componentes no funcionen correctamente.

Tipo	Usuario predeterminado	Contraseña inicial	Descripción
Base de datos de OMS	ommdba	dbChangeMe@123456	Administrador de base de datos de OMS que realiza operaciones de mantenimiento, como crear, iniciar y detener aplicaciones.
	omm	ChangeMe@123456	Usuario para acceder a los datos de la base de datos de OMS.
DBService database	omm	dbserverAdmin@123	Administrador de la base de datos de GaussDB en el componente de DBService.
	hive	HiveUser@	Usuario para que Hive se conecte a la base de datos de DBService.
	hue	HueUser@123	Usuario para que Hue se conecte a la base de datos de DBService.
	sqoop	SqoopUser@	Usuario para que Loader se conecte a la base de datos de DBService.
	ranger	RangerUser@	Usuario para que Ranger se conecte a la base de datos de DBService.

8.14.3 Creación de un rol

Escenario

En esta sección se describe cómo crear un rol en Manager y autorizar y gestionar Manager y componentes.

Se pueden crear hasta 1000 roles en Manager.

NOTA

Las operaciones descritas en esta sección solo se aplican a clústeres de versiones anteriores a MRS 3.x.

Para los clústeres de **MRS 3.*x*** o versiones posteriores, véase **Gestión de roles**.

Prerrequisitos

- Ha aprendido los requisitos de servicio.
- Ha obtenido un clúster con autenticación de Kerberos activada o un clúster común con la función EIP activada.

Procedimiento

Paso 1 Acceda a MRS Manager. Para obtener más información, consulte **Acceso a MRS Manager (MRS 2.x o anterior)**.

Paso 2 En MRS Manager, seleccione **System** > **Manage Role**.

Paso 3 Haga clic en **Create Role** y complete **Role Name** y **Description**.

Role Name es obligatorio y contiene de 3 a 30 caracteres. Solo se permiten dígitos, letras y guiones bajos (_). **Description** es opcional.

Paso 4 En **Permission**, establezca los permisos de rol.

1. Haga clic en **Service Name** y seleccione un nombre en **View Name**.
2. Seleccione uno o más permisos.

NOTA

- El parámetro **Permission** es opcional.
- Si selecciona **View Name** para establecer permisos de componente, puede escribir un nombre de recurso en el cuadro **Search** en la esquina superior derecha y hacer clic en . Se muestra el resultado de la búsqueda.
- El ámbito de búsqueda solo cubre directorios con permisos actuales. No puede buscar subdirectorios. La búsqueda por palabras clave admite la coincidencia difusa y no distingue entre mayúsculas y minúsculas. Los resultados de la siguiente página pueden ser buscados.

Tabla 8-46 Descripción del permiso del Manager

Gestión de permisos de soporte de recursos	Configuraciones de permiso
Alarm	Autoriza la función de alarma del Manager. Puede seleccionar **View** para ver las alarmas y **Management** para gestionar las alarmas.
Audit	Autoriza la función de registro de auditoría del Manager. Puede seleccionar **View** para ver los registros de auditoría y **Management** para gestionar los registros de auditoría.
Dashboard	Autoriza la función de descripción general del Manager. Puede seleccionar **View** para ver la descripción general del clúster.
Hosts	Autoriza la función de gestión de nodos. Puede seleccionar **View** para ver información de nodo y **Management** para gestionar nodos.

Gestión de permisos de soporte de recursos	Configuraciones de permiso
Services	Autoriza la función de gestión del servicio. Puede seleccionar **View** para ver la información del servicio y **Management** para gestionar los servicios.
System_cluster_management	Autoriza la función de gestión de clústeres de MRS. Puede seleccionar **Management** para utilizar la función de gestión de parches de MRS.
System_configuration	Autoriza la función de configuración del clúster de MRS. Puede seleccionar **Management** para configurar clústeres MRS en Manager.
System_task	Autoriza la función de tarea de clúster de MRS. Puede seleccionar **Management** para gestionar tareas periódicas de clústeres MRS en Manager.
Tenant	Autoriza la función de gestión de múltiples tenants del Manager. Puede seleccionar **Management** para gestionar varios tenants.

Tabla 8-47 Descripción del permiso de HBase

Gestión de permisos de soporte de recursos	Configuraciones de permiso
SUPER_USER_GROUP	Le otorga permisos de administrador de HBase.
Global	Tipo de recurso HBase, que indica toda la HBase.
Namespace	Tipo de recurso HBase, que indica espacio de nombres, que se utiliza para almacenar tablas de HBase. Tiene los siguientes permisos: ● **Admin**: permiso para gestionar el espacio de nombres ● **Create**: permiso para crear tablas HBase en el espacio de nombres ● **Read**: permiso para acceder al espacio de nombres ● **Write**: permiso para escribir datos en el espacio de nombres ● **Execute**: permiso para ejecutar el coprocesador (Endpoint)

Gestión de permisos de soporte de recursos	Configuraciones de permiso
Table	Tipo de recurso de HBase, que indica una tabla de datos, que se utiliza para almacenar datos. Tiene los siguientes permisos: ● **Admin**: permiso para gestionar una tabla de datos ● **Create**: permiso para crear familias de columnas y columnas en una tabla de datos ● **Read**: permiso para leer una tabla de datos ● **Write**: permiso para escribir datos en una tabla de datos ● **Execute**: permiso para ejecutar el coprocesador (Endpoint)
ColumnFamily	Tipo de recurso HBase, que indica una familia de columnas, que se utiliza para almacenar datos. Tiene los siguientes permisos: ● **Create**: permiso para crear columnas en una familia de columnas ● **Read**: permiso para leer una familia de columnas ● **Write**: permiso para escribir datos en una familia de columnas
Qualifier	Tipo de recurso de HBase, que indica una columna, que se utiliza para almacenar datos. Tiene los siguientes permisos: ● **Read**: permiso para leer una columna ● **Write**: permiso para escribir datos en una columna

De forma predeterminada, los permisos de un tipo de recurso de HBase de cada nivel son compartidos por tipos de recursos de subniveles. Sin embargo, la opción **Recursive** no está seleccionada de forma predeterminada. Por ejemplo, si los permisos **Read** y **Write** se agregan al espacio de nombres **default**, se agregan automáticamente a las tablas, familias de columnas y columnas del espacio de nombres. Si se establece un recurso secundario después del recurso primario, el permiso del recurso secundario es la unión de los permisos del recurso primario y el recurso secundario actual.

Tabla 8-48 Descripción del permiso de HDFS

Gestión de permisos de soporte de recursos	Configuraciones de permiso
Folder	Tipo de recurso de HDFS, que indica un directorio de HDFS, que se utiliza para almacenar archivos o subdirectorios. Tiene los siguientes permisos: ● **Read**: permiso para acceder al directorio de HDFS ● **Write**: permiso para escribir datos en el directorio de HDFS ● **Execute**: permiso para realizar una operación. Debe seleccionarse al agregar permisos de acceso o escritura.
Files	Tipo de recurso de HDFS, que indica un archivo en HDFS. Tiene los siguientes permisos: ● **Read**: permiso para acceder al archivo ● **Write**: permiso para escribir datos en el archivo ● **Execute**: permiso para realizar una operación. Debe seleccionarse al agregar permisos de acceso o escritura.

Los permisos de un directorio de HDFS de cada nivel no son compartidos por los tipos de directorio de subniveles de forma predeterminada. Por ejemplo, si los permisos **Read** y **Execute** se agregan al directorio **tmp**, debe seleccionar **Recursive** para que los permisos se agreguen a los subdirectorios.

Tabla 8-49 Descripción del permiso de Hive

Gestión de permisos de soporte de recursos	Configuraciones de permiso
Hive Admin Privilege	Le otorga permisos de administrador de Hive.
Database	Tipo de recurso Hive, que indica una base de datos Hive, que se utiliza para almacenar tablas de Hive. Tiene los siguientes permisos: ● **Select**: permiso para consultar la base de datos de Hive ● **Delete**: permiso para realizar la operación de eliminación en la base de datos de Hive ● **Insert**: permiso para realizar la operación de inserción en la base de datos de Hive ● **Create**: permiso para realizar la operación de creación en la base de datos de Hive

Gestión de permisos de soporte de recursos	Configuraciones de permiso
Table	Tipo de recurso de Hive, que indica una tabla de Hive, que se utiliza para almacenar datos. Tiene los siguientes permisos: ● **Select**: permiso para consultar la tabla Hive ● **Delete**: permiso para realizar la operación de eliminación en la tabla Hive ● **Update**: permiso para realizar la operación de actualización en la tabla Hive ● **Insert**: permiso para realizar la operación de inserción en la tabla Hive ● **Grant of Select**: permiso para conceder el permiso **Select** a otros usuarios que usen sentencias de Hive ● **Grant of Delete**: permiso para conceder el permiso **Delete** a otros usuarios que usen sentencias de Hive ● **Grant of Update**: permiso para conceder el permiso **Update** a otros usuarios que usen sentencias de Hive ● **Grant of Insert**: permiso para conceder el permiso **Insert** a otros usuarios que usen sentencias de Hive

De forma predeterminada, los permisos de un tipo de recurso de Hive de cada nivel son compartidos por los tipos de recursos de los subniveles. Sin embargo, la opción **Recursive** no está seleccionada de forma predeterminada. Por ejemplo, si se agregan permisos **Select** y **Insert** a la base de datos **default**, se agregan automáticamente a las tablas y columnas de la base de datos. Si se establece un recurso secundario después del recurso primario, el permiso del recurso secundario es la unión de los permisos del recurso primario y el recurso secundario actual.

Tabla 8-50 Descripción del permiso de Yarn

Gestión de permisos de soporte de recursos	Configuraciones de permiso
Cluster Admin Operations	Le otorga permisos de administrador de Yarn.
root	Cola de raíz de Yarn. Tiene los siguientes permisos: ● **Submit**: permiso para enviar trabajos en la cola ● **Admin**: permiso para gestionar los permisos de la cola actual

Gestión de permisos de soporte de recursos	Configuraciones de permiso
Parent Queue	Tipo de recurso de Yarn, que indica una cola principal que contiene subcolas. Una cola raíz es un tipo de cola principal. Tiene los siguientes permisos: ● **Submit**: permiso para enviar trabajos en la cola ● **Admin**: permiso para gestionar los permisos de la cola actual
Leaf Queue	Tipo de recurso de Yarn, que indica una cola de hoja. Tiene los siguientes permisos: ● **Submit**: permiso para enviar trabajos en la cola ● **Admin**: permiso para gestionar los permisos de la cola actual

De forma predeterminada, los permisos de un tipo de recurso de Yarn de cada nivel son compartidos por los tipos de recursos de los subniveles. Sin embargo, la opción **Recursive** no está seleccionada de forma predeterminada. Por ejemplo, si el permiso **Submit** se agrega a la cola **root**, se agrega automáticamente a la subcola. Los permisos heredados por las subcolas no se mostrarán como seleccionados en la tabla **Permission**. Si se establece un recurso secundario después del recurso primario, el permiso del recurso secundario es la unión de los permisos del recurso primario y el recurso secundario actual.

Tabla 8-51 Descripción del permiso de Hue

Gestión de permisos de soporte de recursos	Configuraciones de permiso
Storage Policy Admin	Le otorga permisos de administrador de política de almacenamiento.

Paso 5 Haga clic en **OK**. Vuelva a **Manage Role**.

----Fin

Tareas relacionadas

Modificación de un rol

Paso 1 En MRS Manager, haga clic en **System**.

Paso 2 En el área **Permission**, haga clic en **Manage Role**.

Paso 3 En la fila del rol que se va a modificar, haga clic en **Modify** para modificar la información del rol.

NOTA

Si modifica los permisos asignados por el rol, se tarda 3 minutos en hacer que las nuevas configuraciones surtan efecto.

Paso 4 Haga clic en **OK**. La modificación está completa.

----Fin

Deleting a role

Paso 1 En MRS Manager, haga clic en **System**.

Paso 2 En el área **Permission**, haga clic en **Manage Role**.

Paso 3 En la fila del rol que se va a eliminar, haga clic en **Delete**.

Paso 4 Haga clic en **OK**. El rol se elimina.

----Fin

8.14.4 Creación de un grupo de usuarios

Escenario

En esta sección se describe cómo crear grupos de usuarios y especificar sus permisos de operación en Manager. La gestión de usuarios únicos o múltiples se puede unificar en los grupos de usuarios. Después de agregarse a un grupo de usuarios, los usuarios pueden obtener permisos de operación propiedad del grupo de usuarios.

Manager admite un máximo de 100 grupos de usuarios.

NOTA

Las operaciones descritas en esta sección solo se aplican a clústeres de versiones anteriores a MRS 3.x.

Para los clústeres de **MRS 3.*x*** o versiones posteriores, véase **Gestión de grupos de usuarios**.

Prerrequisitos

- Los administradores han aprendido los requisitos de servicio y creado los roles requeridos por los escenarios de servicio.
- Ha obtenido un clúster con autenticación de Kerberos activada o un clúster común con la función EIP activada.

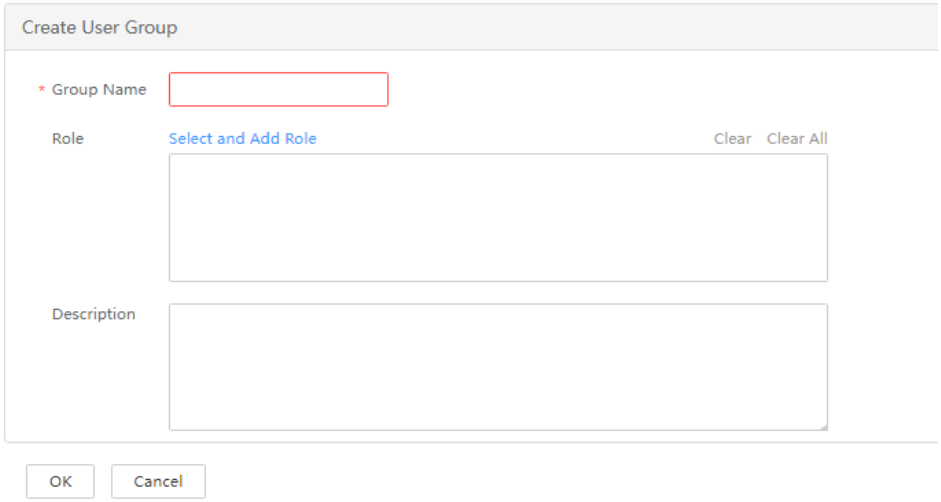
Procedimiento

Paso 1 Acceda a MRS Manager. Para obtener más información, consulte **Acceso a MRS Manager (MRS 2.x o anterior)**.

Paso 2 En MRS Manager, haga clic en **System**.

Paso 3 En el área **Permission**, haga clic en **Manage User Group**.

Paso 4 Encima de la lista de grupos de usuarios, haga clic en **Create User Group**.



Paso 5 Ingrese **Group Name** y **Description**.

Group Name es obligatorio y contiene de 3 a 20 caracteres. Solo se permiten dígitos, letras y guiones bajos (_). **Description** es opcional.

Paso 6 En **Role**, haga clic en **Select and Add Role** para seleccionar y agregar roles especificados.

Si no agrega los roles, el grupo de usuarios que está creando ahora no tiene permiso para usar clústeres MRS.

Paso 7 Haga clic en **OK**.

----Fin

Tareas relacionadas

Modificación de un grupo de usuarios

Paso 1 En MRS Manager, haga clic en **System**.

Paso 2 En el área **Permission**, haga clic en **Manage User Group**.

Paso 3 En la fila de un grupo de usuarios que se va a modificar, haga clic en **Modify**.

NOTA

Si cambia los permisos de rol asignados al grupo de usuarios, se tardan 3 minutos en hacer que las nuevas configuraciones surtan efecto.

Paso 4 Haga clic en **OK**. La modificación está completa.

----Fin

Eliminación de un grupo de usuario

Paso 1 En MRS Manager, haga clic en **System**.

Paso 2 En el área **Permission**, haga clic en **Manage User Group**.

Paso 3 En la fila del grupo de usuarios que se va a eliminar, haga clic en **Delete**.

Paso 4 Haga clic en **OK**. Se elimina el grupo de usuarios.

----Fin

8.14.5 Creación de un usuario

Escenario

En esta sección se describe cómo crear usuarios en Manager según los requisitos del sitio y especificar sus permisos de operación para cumplir con los requisitos de servicio.

Se pueden crear hasta usuarios de 1,000 en Manager.

Si se necesita utilizar una nueva política de contraseñas para la contraseña de un usuario nuevo, siga las instrucciones en **Modificación de una política de contraseñas** para modificar la política de contraseñas y, a continuación, realice las siguientes operaciones para crear un usuario.

NOTA

Las operaciones descritas en esta sección solo se aplican a clústeres de versiones anteriores a MRS 3.x.

Para los clústeres de **MRS 3.*x*** o versiones posteriores, consulte **Creación de un usuario**.

Prerrequisitos

- Los administradores han aprendido los requisitos de servicio y han creado roles y grupos de roles requeridos por los escenarios de servicio.
- Ha obtenido un clúster con autenticación de Kerberos activada o un clúster común con la función EIP activada.

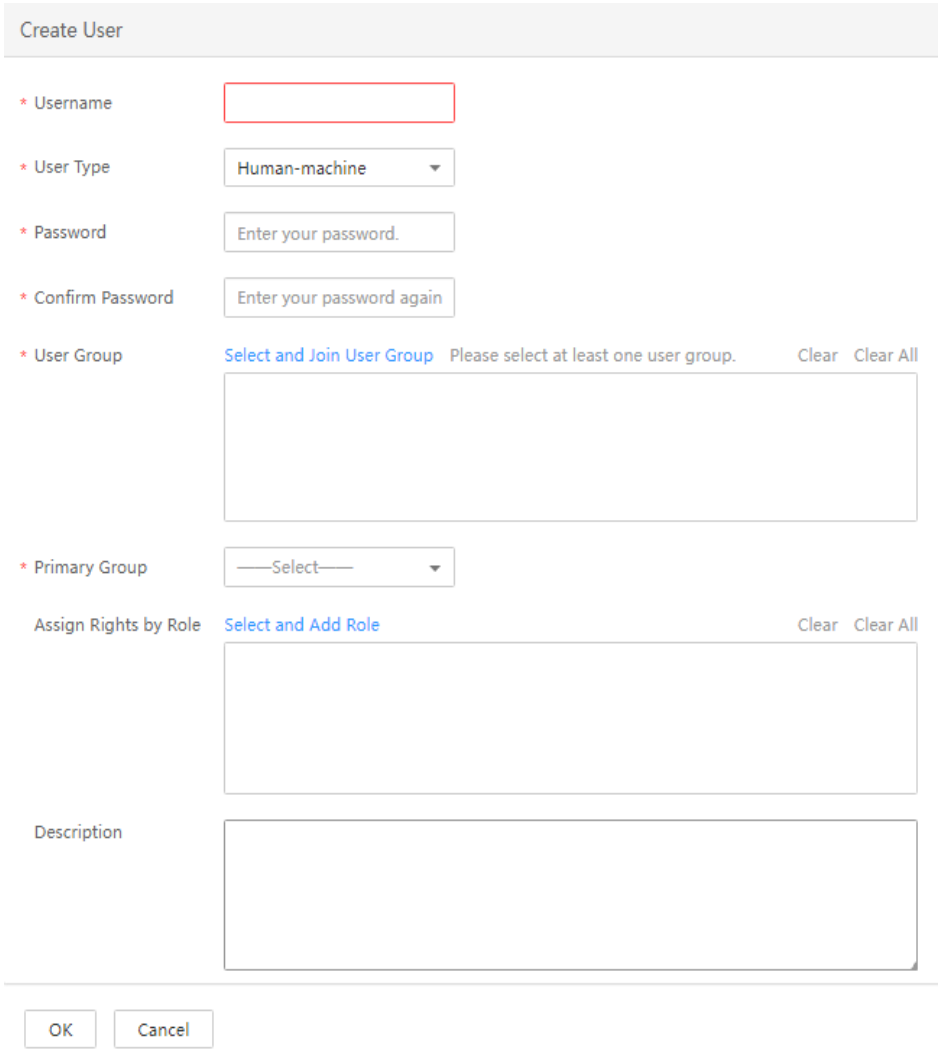
Procedimiento

Paso 1 Acceda a MRS Manager. Para obtener más información, consulte **Acceso a MRS Manager (MRS 2.x o anterior)**.

Paso 2 En MRS Manager, haga clic en **System**.

Paso 3 En el área **Permission**, haga clic en **Manage User**.

Paso 4 Encima de la lista de usuarios, haga clic en **Create User**.



Paso 5 Configure los parámetros según se le solicite e introduzca un nombre de usuario en **Username**.

NOTA

- No se permite un nombre de usuario que difiera solo en mayúsculas y minúsculas de un nombre de usuario existente. Por ejemplo, si **User1** se ha creado, no puede crear **user1**.
- Cuando utilice el usuario que creó, introduzca el nombre de usuario exactamente correcto, que distingue entre mayúsculas y minúsculas.
- **Username** es obligatorio y contiene de 3 a 20 caracteres. Solo se permiten dígitos, letras y guiones bajos (_).
- **root**, **omm** y **ommdba** son usuarios reservados del sistema. Seleccione otro nombre de usuario.

Paso 6 Establezca **User Type** en **Human-machine** o **Machine-machine**.

- Usuario **Human-machine**: utilizado para escenarios O&M de MRS Manager y escenarios de operación del cliente de componentes. Si selecciona este tipo de usuario, debe introducir una contraseña y confirmar la contraseña de **Password** y **Confirm Password** en consecuencia.
- Usuarios de **Machine-machine**: utilizados para escenarios de desarrollo de aplicaciones de MRS. Si selecciona este tipo de usuario, no es necesario introducir una contraseña, ya que la contraseña se genera aleatoriamente.

Paso 7 En **User Group**, haga clic en **Select and Join User Group** para seleccionar grupos de usuarios y agregar usuarios a ellos.

NOTA

- Si se han agregado roles a grupos de usuarios, se puede conceder a los usuarios permisos de los roles.
- Si desea conceder a nuevos usuarios permisos de Hive, agregue los usuarios al grupo de Hive.
- Si un usuario necesita gestionar recursos de tenant, se debe asignar al grupo de usuarios el rol **Manager_tenant** y el rol correspondiente al tenant.
- Los usuarios creados en Manager no se pueden agregar al grupo de usuarios sincronizados mediante la función de sincronización de usuarios de IAM.

Paso 8 En **Primary Group**, seleccione un grupo como grupo principal para que los usuarios creen directorios y archivos. La lista desplegable contiene todos los grupos seleccionados en **User Group**.

Paso 9 En **Assign Rights by Role**, haga clic en **Select and Add Role** para agregar roles para los usuarios según los requisitos de servicio en el sitio.

NOTA

- Cuando crea un usuario, si los permisos de un grupo de usuarios que se concede al usuario no pueden cumplir los requisitos de servicio, puede asignar otros roles creados al usuario. Se tarda 3 minutos en hacer que los permisos de rol otorgados al nuevo usuario tengan efecto.
- Al agregar un rol al crear un usuario se pueden especificar los derechos de usuario.
- Un nuevo usuario puede acceder a las interfaces de usuario web de HDFS, HBase, Yarn, Spark y Hue incluso cuando los roles no están asignados al usuario.

Paso 10 En **Description**, proporcione una descripción basada en los requisitos de servicio en el sitio.

Description es opcional.

Paso 11 Haga clic en **OK**.

Si se utiliza un usuario nuevo en el clúster MRS por primera vez, por ejemplo, para iniciar sesión en MRS Manager o para usar el cliente del clúster, se debe cambiar la contraseña. Para obtener más información, consulte **Cambio de la contraseña de un usuario de operación**.

----Fin

8.14.6 Modificación de la información de usuario

Escenario

En esta sección se describe cómo modificar la información del usuario en Manager, incluida la información sobre el grupo de usuarios, el grupo principal, el rol y la descripción.

Esta operación solo se admite en clústeres con autenticación de Kerberos habilitada o clústeres comunes con la función EIP habilitada.

NOTA

Las operaciones descritas en esta sección solo se aplican a clústeres de versiones anteriores a MRS 3.x.

Para los clústeres de **MRS 3.*x*** o versiones posteriores, véase **Modificación de la información de usuario**.

Procedimiento

Paso 1 Acceda a MRS Manager. Para obtener más información, consulte **Acceso a MRS Manager (MRS 2.x o anterior)**.

Paso 2 En MRS Manager, haga clic en **System**.

Paso 3 En el área **Permission**, haga clic en **Manage User**.

Paso 4 En la fila de un usuario que se va a modificar, haga clic en **Modify**.

NOTA

Si cambia los grupos de usuarios de un usuario o asigna permisos de rol a un usuario, se tarda 3 minutos en hacer que las nuevas configuraciones surtan efecto.

Paso 5 Haga clic en **OK**. La modificación está completa.

----Fin

8.14.7 Bloqueo de un usuario

Esta sección describe cómo bloquear usuarios en clústeres de MRS. Un usuario bloqueado no puede iniciar sesión en Manager ni realizar autenticación de seguridad en el clúster. Esta operación solo se admite en clústeres con autenticación de Kerberos habilitada o clústeres comunes con la función EIP habilitada.

Un usuario bloqueado puede ser desbloqueado por un administrador manualmente o hasta que expire la duración del bloqueo. Puede bloquear a un usuario mediante cualquiera de los métodos siguientes:

- Bloqueo automático: Ajuste **Number of Password Retries** en **Configure Password Policy**. Si los intentos de inicio de sesión del usuario exceden el valor del parámetro, el usuario se bloquea automáticamente. Para obtener más información, consulte **Modificación de una política de contraseñas**.
- Bloqueo manual: El administrador bloquea manualmente a un usuario.

NOTA

Las operaciones descritas en esta sección solo se aplican a clústeres de versiones anteriores a MRS 3.x.

Para los clústeres de **MRS 3.*x*** o versiones posteriores, véase **Bloqueo de un usuario**.

A continuación se describe cómo bloquear manualmente un usuario. Los usuarios de **Machine-Machine** no se pueden bloquear.

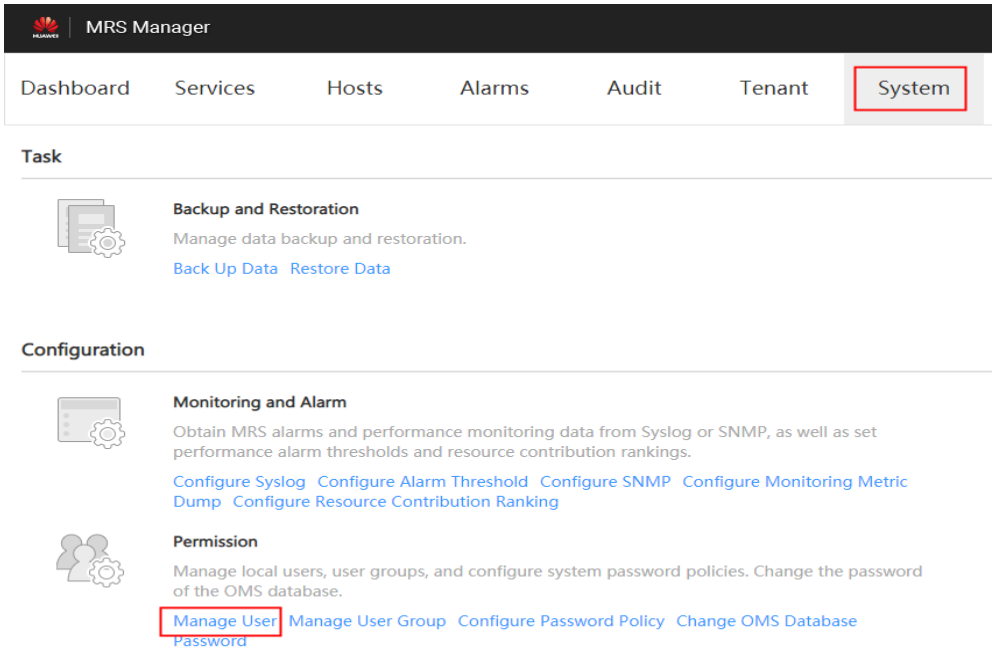
Procedimiento

Paso 1 Acceda a MRS Manager. Para obtener más información, consulte **Acceso a MRS Manager (MRS 2.x o anterior)**.

Paso 2 En MRS Manager, haga clic en **System**.

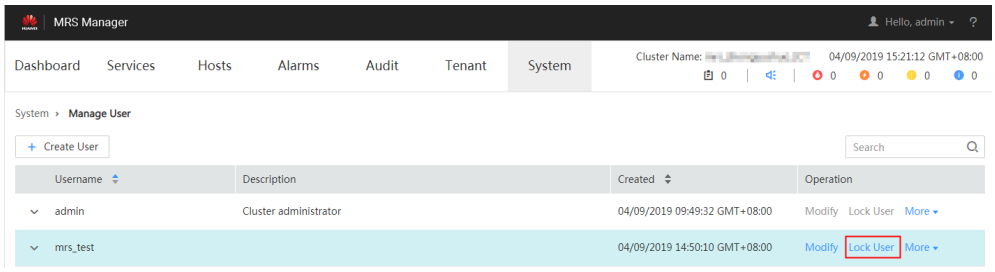
Paso 3 En el área **Permission**, haga clic en **Manage User**.

Figura 8-20 Gestión de un usuario



Paso 4 En la fila de un usuario que desea bloquear, haga clic en **Lock User**.

Figura 8-21 Bloqueo de un usuario



Paso 5 En la ventana que se muestra, haga clic en **OK** para bloquear al usuario.

----Fin

8.14.8 Desbloquear un usuario

Si un usuario está bloqueado porque el número de intentos de inicio de sesión excede el valor de **Number of Password Retries** o el usuario está bloqueado manualmente por el administrador, el administrador puede desbloquear al usuario en Manager. Esta operación solo se admite en clústeres con autenticación de Kerberos habilitada o clústeres comunes con la función EIP habilitada.

NOTA

Las operaciones descritas en esta sección solo se aplican a clústeres de versiones anteriores a MRS 3.x.

Para los clústeres de **MRS 3.*x*** o versiones posteriores, véase **Desbloquear un usuario**.

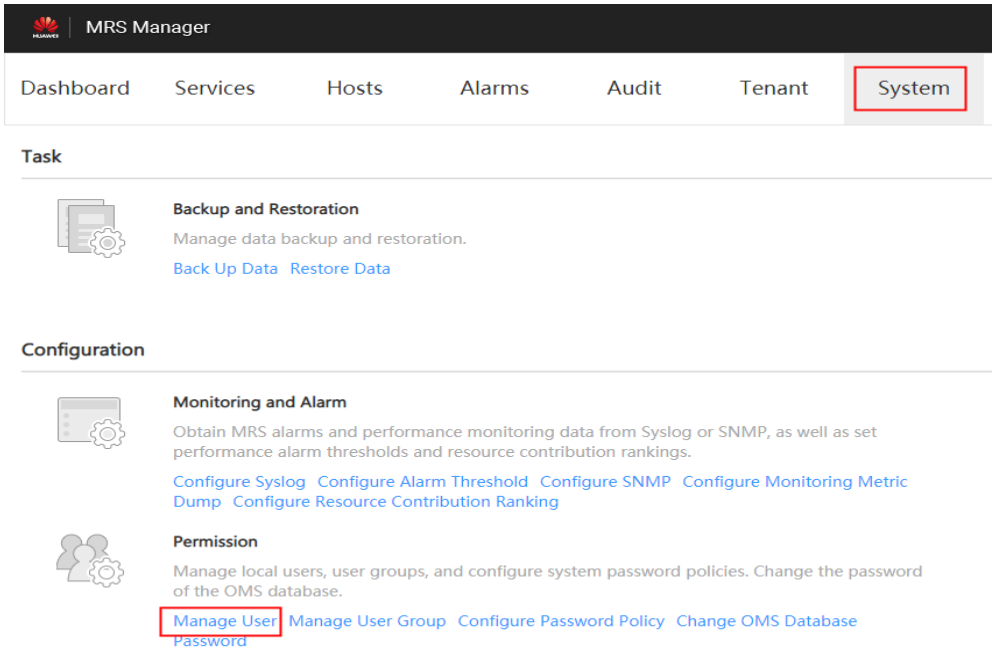
Procedimiento

Paso 1 Acceda a MRS Manager. Para obtener más información, consulte **Acceso a MRS Manager (MRS 2.x o anterior)**.

Paso 2 En MRS Manager, haga clic en **System**.

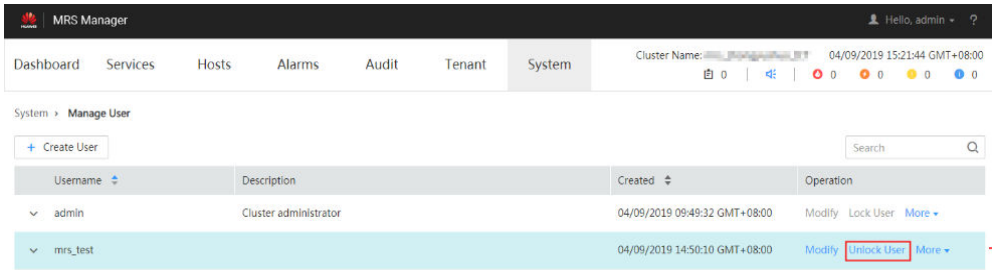
Paso 3 En el área **Permission**, haga clic en **Manage User**.

Figura 8-22 Gestión de un usuario



Paso 4 En la fila de un usuario que se va a desbloquear, haga clic en **Unlock User**.

Figura 8-23 Desbloquear un usuario



Paso 5 En la ventana que se muestra, haga clic en **OK** para desbloquear al usuario.

----Fin

8.14.9 Eliminación de usuarios

El administrador puede eliminar un usuario del clúster de MRS que no sea necesario en MRS Manager. La eliminación de un usuario solo se permite en clústeres con autenticación de Kerberos activada o en clústeres normales con la función EIP activada.

NOTA

Si desea crear un nuevo usuario con el mismo nombre que el usuario A después de eliminar el usuario A que ha enviado un trabajo en el cliente o en la consola de MRS, debe eliminar las carpetas residuales del usuario A al eliminar el usuario A. De lo contrario, el usuario A recién creado puede fallar al enviar un trabajo.

Para eliminar carpetas residuales, inicie sesión en cada nodo de Core del clúster MRS y ejecute los siguientes comandos. En los siguientes comandos **$user** indica la carpeta con el nombre de usuario.

cd /srv/BigData/hadoop/data1/nm/localdir/usercache/

rm -rf $user

Las operaciones descritas en esta sección solo se aplican a clústeres de versiones anteriores a MRS 3.x.

Para los clústeres de **MRS 3.*x*** o versiones posteriores, consulte **Eliminación de usuarios**.

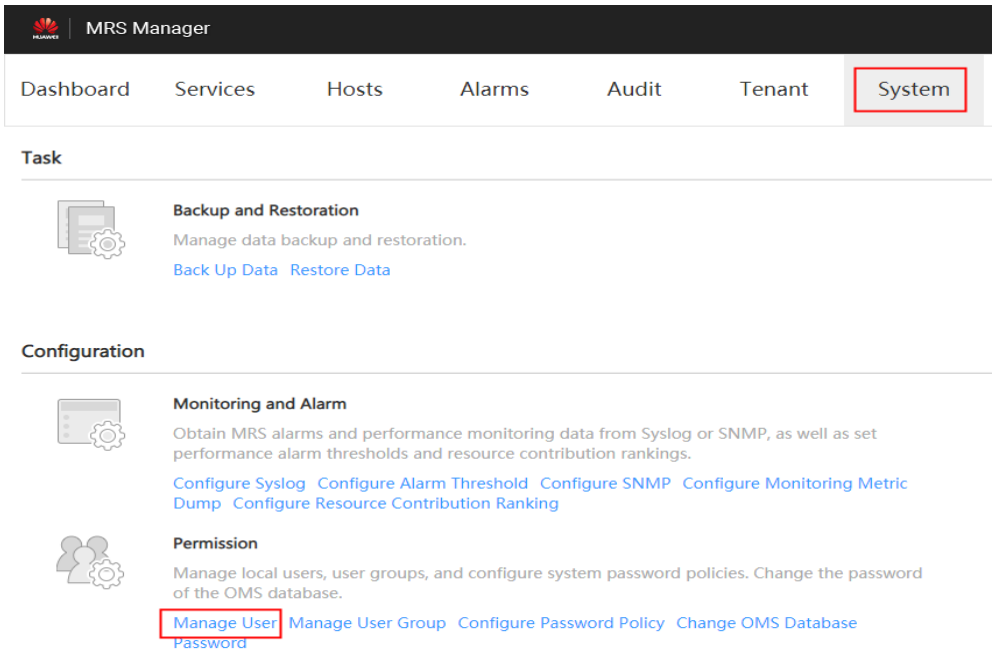
Procedimiento

Paso 1 Acceda a MRS Manager. Para obtener más información, consulte **Acceso a MRS Manager (MRS 2.x o anterior)**.

Paso 2 En MRS Manager, haga clic en **System**.

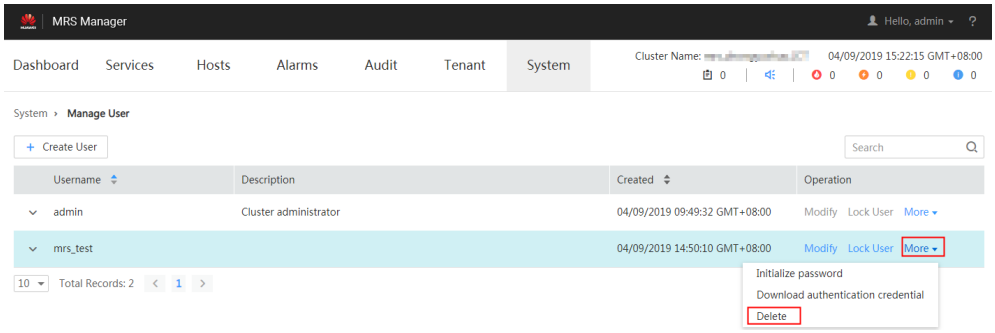
Paso 3 En el área **Permission**, haga clic en **Manage User**.

Figura 8-24 Gestión de usuarios



Paso 4 En la fila que contiene el usuario que se va a eliminar, elija **More** > **Delete**.

Figura 8-25 Eliminación de usuarios



Paso 5 Haga clic en **OK**.

----Fin

8.14.10 Cambio de la contraseña de un usuario de operación

Escenario

Las contraseñas de los usuarios del sistema **Human-machine** deben cambiarse regularmente para garantizar la seguridad del clúster MRS. Esta sección describe cómo cambiar las contraseñas en MRS Manager.

Si es necesario utilizar una nueva política de contraseñas para la contraseña modificada por el usuario, siga las instrucciones en **Modificación de una política de contraseñas** para modificar la política de contraseñas y, a continuación, realice las siguientes operaciones para modificar la contraseña.

NOTA

Las operaciones descritas en esta sección solo se aplican a clústeres de versiones anteriores a MRS 3.x.

Para los clústeres de **MRS 3.*x*** o versiones posteriores, consulte **Modificación de contraseña de un usuario**.

Impacto en el sistema

Si ha descargado un archivo de autenticación de usuario, descárguelo de nuevo y obtenga el archivo keytab después de modificar la contraseña del usuario del clúster MRS.

Prerrequisitos

- Ha obtenido la política de contraseñas actual.
- Usted ha obtenido la URL para acceder a MRS Manager.
- Ha obtenido un clúster con autenticación de Kerberos activada o un clúster común con la función EIP activada.

Procedimiento

Paso 1 Acceda a MRS Manager. Para obtener más información, consulte **Acceso a MRS Manager (MRS 2.x o anterior)**.

Paso 2 En MRS Manager, mueva el cursor del ratón a  en la esquina superior derecha.

En el menú que se muestra, seleccione **Change Password**.

Paso 3 Rellene el **Old Password**, **New Password** y el **Confirm Password**. Haga clic en **OK**.

Para el clúster, los requisitos de complejidad de contraseña predeterminados son los siguientes:

- La contraseña debe contener entre 8 y 32 caracteres.
- La contraseña debe contener al menos tres tipos de los siguientes: letras mayúsculas, minúsculas, dígitos, espacios y caracteres especiales ('~!@#$%^&*()-_=+\|[{}];:'",<.>/?).
- La contraseña no puede ser el nombre de usuario o el nombre de usuario inverso.

----Fin

8.14.11 Inicialización de la contraseña de un usuario del sistema

Escenario

Esta sección describe cómo inicializar una contraseña en Manager si un usuario olvida la contraseña o si la contraseña de una cuenta pública necesita cambiarse regularmente. Después de la inicialización de la contraseña, el usuario debe cambiar la contraseña en el primer inicio de sesión. Esta operación solo se admite en clústeres con autenticación de Kerberos habilitada o clústeres comunes con la función EIP habilitada.

NOTA

Las operaciones descritas en esta sección solo se aplican a clústeres de versiones anteriores a MRS 3.x.

Para los clústeres de **MRS 3.*x*** o versiones posteriores, véase **Inicializar una contraseña**.

Impacto en el sistema

Si ha descargado un archivo de autenticación de usuario, descárguelo de nuevo y obtenga el archivo keytab después de inicializar la contraseña del usuario del clúster de MRS.

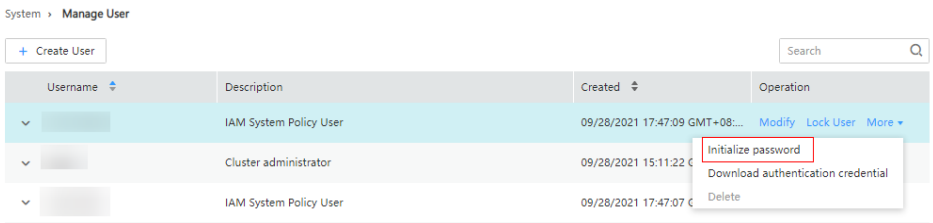
Inicialización de la contraseña de un usuario humano-máquina

Paso 1 Acceda a MRS Manager. Para obtener más información, consulte **Acceso a MRS Manager (MRS 2.x o anterior)**.

Paso 2 En MRS Manager, haga clic en **System**.

Paso 3 En el área **Permission**, haga clic en **Manage User**.

Paso 4 Busque la fila que contiene el usuario cuya contraseña se va a inicializar, elija **More** > **Initialize password** y cambie la contraseña según se le solicite.



En la ventana que se muestra, introduzca la contraseña de la cuenta de administrador actual y haga clic en **OK**. A continuación, en **Initialize password**, haga clic en **OK**.

Para el clúster, los requisitos de complejidad de contraseña predeterminados son los siguientes:

- La contraseña debe contener entre 8 y 32 caracteres.
- La contraseña debe contener al menos tres tipos de los siguientes: letras mayúsculas, minúsculas, dígitos, espacios y caracteres especiales ('~!@#$%^&*()-_=+\|[{}];:'",<.>/?).
- La contraseña no puede ser el nombre de usuario o el nombre de usuario inverso.

----Fin

Inicialización de la contraseña de un usuario máquina-máquina

Paso 1 Prepare un cliente según las condiciones del servicio e inicie sesión en el nodo con el cliente instalado.

Paso 2 Ejecute el siguiente comando para cambiar el usuario:

sudo su - omm

Paso 3 Ejecute el siguiente comando para cambiar al directorio del cliente, por ejemplo **/opt/Bigdata/client**:

cd /opt/Bigdata/client

Paso 4 Ejecute el siguiente comando para configurar las variables de entorno:

source bigdata_env

Paso 5 Ejecute el siguiente comando para iniciar sesión en la consola como usuario **kadmin/admin**:

NOTA

La contraseña predeterminada del usuario **kadmin/admin** es **KAdmin@123**, que caducará en su primer inicio de sesión. Cambie la contraseña según se le indique y mantenga segura la nueva contraseña.

kadmin -p kadmin/admin

Paso 6 Ejecute el siguiente comando para restablecer la contraseña de un usuario que ejecuta un componente. Esta operación tiene efecto en todos los servidores:

cpw *Component running user name*

Por ejemplo, **cpw oms/manager**.

Para el clúster, los requisitos de complejidad de contraseña predeterminados son los siguientes:

- La contraseña debe contener entre 8 y 32 caracteres.
- La contraseña debe contener al menos tres tipos de los siguientes: letras mayúsculas, minúsculas, dígitos, espacios y caracteres especiales ('~!@#$%^&*()-_=+\|[{}];:'",<.>/?).
- La contraseña no puede ser el nombre de usuario o el nombre de usuario inverso.

----Fin

8.14.12 Descargar un archivo de autenticación de usuario

Escenario

Cuando un usuario desarrolla aplicaciones de big data y las ejecuta en un clúster MRS que admite la autenticación de Kerberos, el usuario debe preparar un archivo de autenticación de usuario de **Machine-machine** para acceder al clúster MRS. El archivo keytab en el archivo de autenticación se puede utilizar para la autenticación del usuario.

Esta sección describe cómo descargar un archivo de autenticación de usuario de **Machine-machine** y exportar el archivo keytab en Manager. Esta operación solo se admite en clústeres con autenticación de Kerberos habilitada o clústeres comunes con la función EIP habilitada.

NOTA

Antes de descargar un archivo de autenticación de usuario de **Human-machine**, cambie la contraseña del usuario en MRS Manager para que la contraseña inicial establecida por el administrador no sea válida. De lo contrario, no se puede utilizar el archivo keytab exportado. Para obtener más información, consulte **Cambio de la contraseña de un usuario de operación**.

Las operaciones descritas en esta sección solo se aplican a clústeres de versiones anteriores a MRS 3.x.

Para los clústeres de **MRS 3.*x*** o versiones posteriores, consulte **Exportación de un archivo de credenciales de autenticación**.

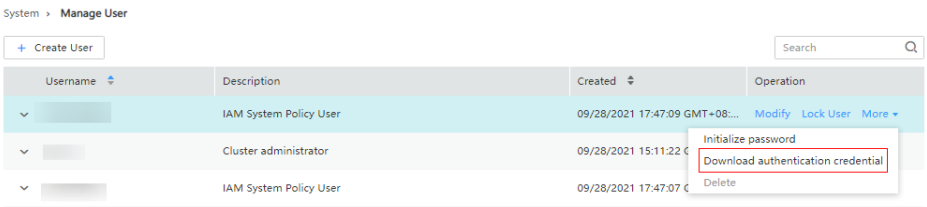
Procedimiento

Paso 1 Acceda a MRS Manager. Para obtener más información, consulte **Acceso a MRS Manager (MRS 2.x o anterior)**.

Paso 2 En MRS Manager, haga clic en **System**.

Paso 3 En el área **Permission**, haga clic en **Manage User**.

Paso 4 En la fila de un usuario para el que desea exportar el archivo keytab, elija **More** > **Download authentication credential** para descargar el archivo de autenticación. Después de que el archivo se genere automáticamente, guárdelo en una ruta especificada y manténgalo seguro.



Paso 5 Abra el archivo de autenticación con un programa de descompresión.

- **user.keytab** indica un archivo keytab del usuario utilizado para la autenticación del usuario.
- **krb5.conf** indica el archivo de configuración del servidor de autenticación. La aplicación se conecta al servidor de autenticación de acuerdo con esta información del archivo de configuración al autenticar usuarios.

----Fin

8.14.13 Modificación de una política de contraseñas

Escenario

AVISO

Debido a que las políticas de contraseñas son fundamentales para la seguridad de gestión de usuarios, modifíquelas en función de los requisitos de seguridad del servicio. De lo contrario, se pueden incurrir en riesgos de seguridad.

Esta sección describe cómo establecer reglas de seguridad de contraseña y inicio de sesión de usuario, así como reglas de bloqueo de usuario. Las políticas de contraseñas establecidas en MRS Manager solo tienen efecto para los usuarios de **Human-machine** porque las contraseñas de los usuarios de **Machine-machine** se generan aleatoriamente. Esta operación solo se admite en clústeres con autenticación de Kerberos habilitada o clústeres comunes con la función EIP habilitada.

Si se necesita utilizar una nueva política de contraseñas para la contraseña de un usuario nuevo o la contraseña modificada por el usuario, realice las siguientes operaciones para modificar la política de contraseñas primero y, a continuación, siga las instrucciones en **Creación de un usuario** o **Cambio de la contraseña de un usuario de operación**.

NOTA

Las operaciones descritas en esta sección solo se aplican a clústeres de versiones anteriores a MRS 3.x.

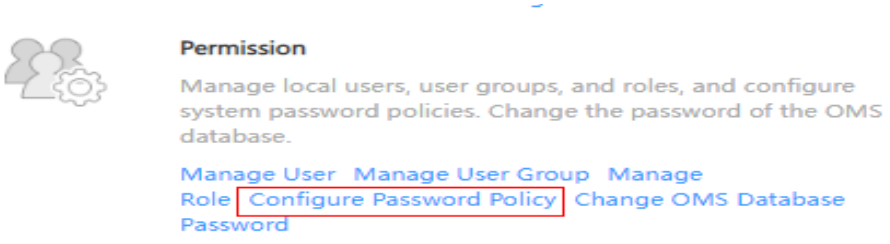
Para los clústeres de **MRS 3.*x*** o versiones posteriores, véase **Configuración de políticas de contraseñas**.

Procedimiento

Paso 1 Acceda a MRS Manager. Para obtener más información, véase **Acceso a MRS Manager (MRS 2.x o anterior)**.

Paso 2 En MRS Manager, haga clic en **System**.

Paso 3 Haga clic en **Configure Password Policy**.



Paso 4 Modifique las políticas de contraseñas según se le solicite. Para obtener más información sobre los parámetros, consulte **Tabla 8-52**.

Tabla 8-52 Descripción del parámetro de política de contraseñas

Parámetro	Descripción
Minimum Password Length	Indica el número mínimo de caracteres que contiene una contraseña. El valor varía de 8 a 32. El valor predeterminado es **8**.
Number of Character Types	Indica el número mínimo de tipos de caracteres que contiene una contraseña. Los tipos de caracteres incluyen letras mayúsculas, minúsculas, dígitos, espacios y caracteres especiales (~`!?,.:;-_'(){}[]/<>@#$%^&*+|\=). El valor puede ser **3** o **4**. El valor predeterminado **3** indica que la contraseña debe contener al menos tres tipos de los siguientes caracteres: letras mayúsculas, minúsculas, dígitos, caracteres especiales y espacios.
Password Validity Period (days)	Indica el período de validez (días) de una contraseña. El valor varía de 0 a 90. El valor **0** significa que la contraseña es válida permanentemente. El valor predeterminado es **90**.
Password Expiration Notification Days	Indica el número de días para notificar la expiración de la contraseña con antelación. Después de establecer el valor, si la diferencia entre el tiempo de clúster y el tiempo de caducidad de la contraseña es menor que este valor, el usuario recibe notificaciones de caducidad de la contraseña. Cuando un usuario inicia sesión en MRS Manager, se muestra un mensaje que indica que la contraseña está a punto de caducar y le pregunta al usuario si desea cambiar la contraseña. El valor varía de **0** a *X* (*X* debe establecerse en la mitad del período de validez de la contraseña y redondearse hacia abajo). El valor **0** indica que no se envía ninguna notificación. El valor predeterminado es **5**.
Interval of Resetting Authentication Failure Count (min)	Indica el intervalo (minutos) de retención de intentos de contraseña incorrectos. El valor varía de 0 a 1440. El valor **0** indica que el número de intentos de contraseña incorrectos se conserva permanentemente y el valor **1440** indica que el número de intentos de contraseña incorrectos se conserva durante un día. El valor predeterminado es **5**.
Number of Password Retries	Indica el número de contraseñas incorrectas consecutivas permitidas antes de que el sistema bloquee al usuario. El valor varía de 3 a 30. El valor predeterminado es **5**.

Parámetro	Descripción
Account Lock Duration (min)	Indica el período de tiempo durante el que un usuario está bloqueado cuando se cumplen las condiciones de bloqueo del usuario. El valor varía de 5 a 120. El valor predeterminado es **5**.

----Fin

8.14.14 Configuración de relaciones de confianza mutua entre clústeres

Escenario

Si el clúster A necesita acceder a los recursos del clúster B, se debe configurar la relación de confianza mutua entre estos dos clústeres.

Si no se configura ninguna relación de confianza, los recursos de un clúster sólo están disponibles para los usuarios de este clúster. MRS asigna automáticamente un **domain name** único para cada clúster para definir el alcance de los recursos para los usuarios.

NOTA

Las operaciones descritas en esta sección solo se aplican a clústeres de versiones anteriores a MRS 3.x.

Para los clústeres de **MRS 3.*x*** o versiones posteriores, véase **Configuración de la confianza mutua Cross-Manager entre clústeres**.

Impacto en el sistema

- Después de configurar la confianza mutua entre clústeres, los recursos de un clúster estarán disponibles para los usuarios de otro clúster. Los permisos de usuario en los clústeres deben comprobarse regularmente en función de los requisitos de servicio y seguridad.
- Después de configurar la confianza mutua entre clústeres, es necesario reiniciar el servicio KrbServer y el clúster no estará disponible durante el reinicio.
- Después de configurar la confianza mutua entre clústeres, los usuarios internos **krbtgt/***Local cluster domain name*@*External cluster domain name* y **krbtgt/***External cluster domain name*@*Local cluster domain name* se agregan a los dos clústeres. Los usuarios internos no se pueden eliminar. La contraseña predeterminada es **Crossrealm@123**.

Prerrequisitos

Ambos clústeres están en la misma VPC. Si no lo son, cree una conexión de pares de VPC entre ellos. Para obtener más información, consulte **Interconexión de VPC**.

Procedimiento

Paso 1 En la consola de gestión de MRS, consulte todos los grupos de seguridad de los dos clústeres.

- Si los grupos de seguridad de los dos clústeres son iguales, vaya a **Paso 3**.
- Si los grupos de seguridad de los dos clústeres son diferentes, vaya a **Paso 2**.

Paso 2 En la consola de gestión de VPC, elija **Access Control** > **Security Groups**. En la página **Security Groups**, busque la fila que contiene el grupo de seguridad de destino, haga clic en **Manage Rule** en la columna **Operation**.

En la página de pestaña **Inbound Rules**, haga clic en **Add Rule**. En el cuadro de diálogo **Add Inbound Rule** que se muestra, configure los parámetros relacionados.

- **Priority**: El valor oscila entre 1 y 100. El valor predeterminado es **1**, que indica la prioridad más alta. Un valor más pequeño indica una prioridad más alta.
- **Action**: Seleccione **Allow**.
- **Protocol & Port**: Elija **Protocols** > **All**.
- **Type**: seleccione **IPv4** o **IPv6**.
- **Source**: Seleccione **Security group** y el grupo de seguridad del clúster del mismo nivel.
  - Para agregar una regla entrante al grupo de seguridad del clúster A, establezca **Source** en **Security group** y el grupo de seguridad del clúster B (clúster de pares).
  - Para agregar una regla entrante al grupo de seguridad del clúster B, establezca **Source** en **Security group** y el grupo de seguridad del clúster A (clúster de pares).

NOTA

Para un clúster común con autenticación de Kerberos deshabilitada, realice el paso **Paso 1** a **Paso 2** para configurar la confianza mutua entre clústeres. Para un clúster de seguridad con autenticación de Kerberos activada, después de completar los pasos anteriores, siga los pasos siguientes para la configuración.

Paso 3 Inicie sesión en MRS Manager de los dos clústeres por separado. Para obtener más información, consulte **Acceso a MRS Manager (MRS 2.x o anterior)**. Haga clic en **Service** y compruebe si el **Health Status** de todos los componentes es **Good**.

- En caso afirmativo, vaya a **Paso 4**.
- En caso negativo, póngase en contacto con el personal de soporte técnico para solucionar problemas.

Paso 4 Consultar información de configuración.

1. En MRS Manager de los dos clústeres, elija **Services** > **KrbServer** > **Instance**. Consultar el **OM IP Address** de los dos hosts de KerberosServer.
2. Haga clic en **Service Configuration**. Ajuste **Type** a **All**. Elija **KerberosServer** > **Port** en el árbol de navegación de la izquierda. Consulte el valor de **kdc_ports**. El valor predeterminado es **21732**.
3. Haga clic en **Realm** y consulte el valor de **default_realm**.

Paso 5 En MRS Manager de cualquier clúster, modifique el parámetro **peer_realms**.

Tabla 8-53 Descripción de parámetros

Parámetro	Descripción
realm_name	Nombre de dominio del clúster de confianza mutua, es decir, el valor de **default_realm** obtenido en el paso **4**.

Parámetro	Descripción
ip_port	Dirección KDC del clúster de pares. Formato: *IP address of a KerberosServer node in the peer cluster:kdc_port* Las direcciones de los dos nodos KerberosServer están separadas por una coma. Por ejemplo, si las direcciones IP de los nodos KerberosServer son 10.0.0.1 y 10.0.0.2 respectivamente, el valor de este parámetro es **10.0.0.1:21732,10.0.0.2:21732**.

NOTA

- Para desplegar relaciones de confianza con varios clústeres, haga clic en para agregar elementos y especificar parámetros relevantes. Para eliminar un elemento, haga clic en .
- Un clúster puede tener relaciones de confianza con un máximo de 16 clústeres. De forma predeterminada, no existe ninguna relación de confianza entre los diferentes clústeres en los que confía un clúster local.

Paso 6 Haga clic en **Save Configuration**. En el cuadro de diálogo que se muestra, seleccione **Restart the affected services or instances** y haga clic en **OK**. Si no selecciona **Restart the affected services or instances**, reinicie manualmente los servicios o instancias afectados.

Una vez que se muestre **Operation successful**, haga clic en **Finish**.

Paso 7 Salga de MRS Manager e inicie sesión de nuevo. Si el inicio de sesión es correcto, las configuraciones son válidas.

Paso 8 Inicie sesión en MRS Manager del otro clúster y repita el paso **Paso 5** a **Paso 7**.

----Fin

Operaciones de seguimiento

Después de configurar la confianza mutua entre clústeres, los parámetros de configuración del servicio se modifican en MRS Manager y se reinicia el servicio. Por lo tanto, debe preparar el archivo de configuración del cliente de nuevo y actualizar el cliente.

Escenario 1:

El clúster A y el clúster B (cluster de pares y clúster de confianza mutua) son del mismo tipo, por ejemplo, clúster de análisis o clúster de streaming. Siga las instrucciones en **Actualización de un cliente (Versiones anteriores a 3.x)** para actualizar los archivos de configuración del cliente del clúster A y B respectivamente.

- Actualice el archivo de configuración del cliente del clúster A.
- Actualice el archivo de configuración del cliente del clúster B.

Escenario 2:

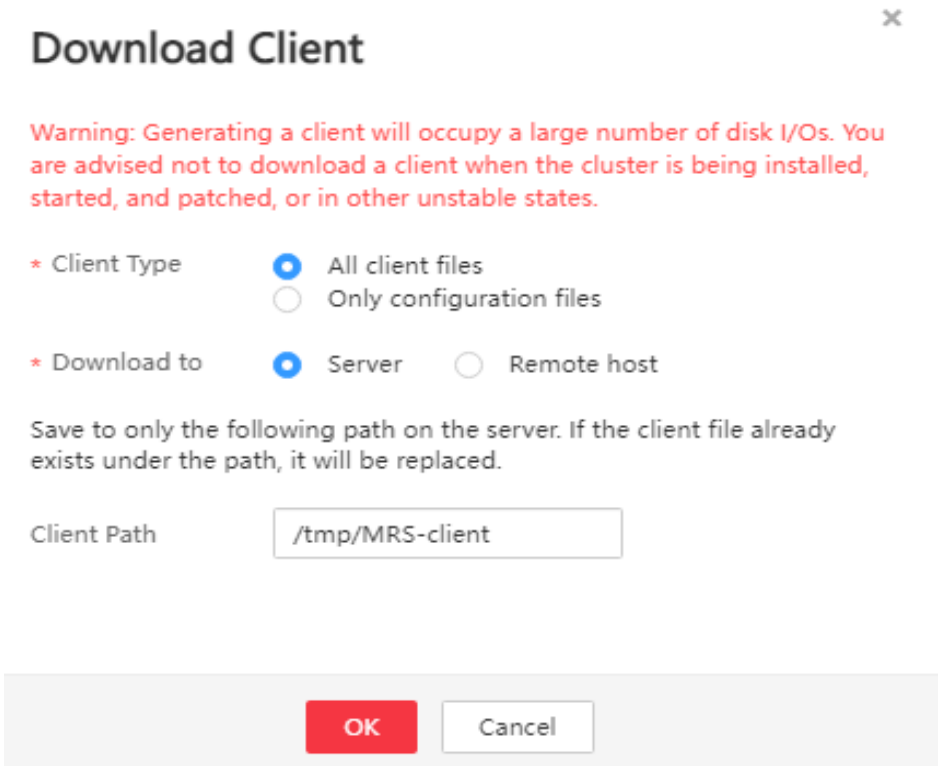
El clúster A y el clúster B (cluster de pares y clúster de confianza mutua) son de tipo diferente. Realice los siguientes pasos para actualizar los archivos de configuración.

- Actualice el archivo de configuración del cliente del clúster A al clúster B.

- Actualice el archivo de configuración del cliente del clúster B al clúster A.
- Actualice el archivo de configuración del cliente del clúster A.
- Actualice el archivo de configuración del cliente del clúster B.

Paso 1 Inicie sesión en MRS Manager del clúster A.

Paso 2 Haga clic en **Services** y, a continuación, en **Download Client**.



Paso 3 Ajuste **Client Type** a **Only configuration files**.

Paso 4 Ajuste **Download to** a **Remote host**.

Paso 5 Establezca **Host IP Address** en la dirección IP del nodo maestro activo del clúster B, **Host Port** en 22 y **Save Path** en **/tmp**.

- Si se cambia el puerto predeterminado **22** para iniciar sesión en el clúster B mediante SSH, establezca **Host Port** en un puerto nuevo.
- El valor de **Save Path** contiene un máximo de 256 caracteres.

Paso 6 Ajuste **Login User** a **root**.

Si se utiliza otro usuario, asegúrese de que el usuario tiene permisos para leer, escribir y ejecutar la ruta de guardado.

Paso 7 Seleccione **Password** o **SSH Private Key** para **Login Mode**.

- **Password**: Ingrese la contraseña del usuario **root** establecida durante la creación del clúster.
- **SSH Private Key**: Seleccione y cargue el archivo de clave utilizado para crear el clúster.

Paso 8 Haga clic en **OK** para generar un archivo de cliente.

Si se muestra la siguiente información, se guardará el archivo de cliente. Haga clic en **Close**.


```
Client files downloaded to the remote host successfully.
```

Si se muestra la siguiente información, compruebe las configuraciones de nombre de usuario, contraseña y grupo de seguridad del host remoto. Asegúrese de que el nombre de usuario y la contraseña sean correctos y de que se haya agregado una regla de entrada del puerto SSH (22) al grupo de seguridad del host remoto. Y luego, vaya a **Paso 2** para descargar el cliente de nuevo.

```
Failed to connect to the server. Please check the network connection or
parameter settings.
```

Paso 9 Inicie sesión en el ECS del clúster B mediante VNC. Para obtener más información, consulte **Inicie sesión en un ECS de Windows mediante VNC**.

Todas las imágenes son compatibles con Cloud-Init. El nombre de usuario preestablecido para Cloud-Init es **root** y la contraseña es la establecida durante la creación del clúster.

Paso 10 Ejecute el siguiente comando para cambiar al directorio del cliente, por ejemplo, **/opt/Bigdata/client**:

cd /opt/Bigdata/client

Paso 11 Ejecute el siguiente comando para actualizar la configuración del cliente del clúster A al clúster B:

sh refreshConfig.sh *Client installation directory Full path of the client configuration file package*

Por ejemplo, ejecute el siguiente comando:

sh refreshConfig.sh /opt/Bigdata/client /tmp/MRS_Services_Client.tar

Si se muestra la siguiente información, las configuraciones se han actualizado correctamente.

```
ReFresh components client config is complete.
Succeed to refresh components client config.
```

NOTA

También puede consultar el método 2 en **Actualización de un cliente (Versiones anteriores a 3.x)** para realizar operaciones de **Paso 1** a **Paso 11**.

Paso 12 Repita el paso **Paso 1** a **Paso 11** para actualizar el archivo de configuración del cliente del clúster B al clúster A.

Paso 13 Siga las instrucciones en **Actualización de un cliente (Versiones anteriores a 3.x)** para actualizar el archivo de configuración del cliente del clúster local.

- Actualice el archivo de configuración del cliente del clúster A.
- Actualice el archivo de configuración del cliente del clúster B.

----Fin

8.14.15 Configuración de usuarios para acceder a los recursos de un clúster de confianza

Escenario

Después de configurar la confianza mutua entre clústeres, se debe configurar el permiso para los usuarios del clúster local, de modo que los usuarios puedan tener acceso a los mismos recursos del clúster de pares que los usuarios del clúster de pares.

NOTA

Las operaciones descritas en esta sección solo se aplican a clústeres de versiones anteriores a MRS 3.x.

Para los clústeres de **MRS 3.*x*** o versiones posteriores, véase **Asignación de permisos de usuario después de configurar la confianza mutua entre clústeres**.

Prerrequisitos

La relación de confianza mutua se ha configurado entre dos clústeres (clusters A y B). Se han actualizado los clientes de los clústeres.

Procedimiento

Paso 1 Inicie sesión en MRS Manager del clúster A y elija **System** > **Manage User**. Compruebe si el clúster A tiene cuentas que son las mismas que las del clúster B.

- En caso afirmativo, vaya a **Paso 2**.
- Si no, vaya a **Paso 3**.

Paso 2 Haga clic en en el lado izquierdo del nombre de usuario para desplegar la información detallada del usuario. Compruebe si el grupo de usuarios y el rol al que pertenece el usuario cumplen los requisitos de servicio.

Por ejemplo, el usuario **admin** del clúster A tiene permiso para acceder y crear archivos en el directorio **/tmp** del clúster A. Entonces vaya a **Paso 4**.

Paso 3 Cree las cuentas en el clúster A y vincule las cuentas al grupo de usuarios y a los roles requeridos por los servicios. Entonces vaya a **Paso 4**.

Paso 4 Elija **Service** > **HDFS** > **Instance**. Consultar el **OM IP Address** de **NameNode (Active)**.

Paso 5 Inicie sesión en el cliente del clúster B.

Por ejemplo, si ha actualizado el cliente en el nodo Master2, inicie sesión en el nodo Master2 para utilizar el cliente. Para obtener más información, consulte **Uso de un cliente de MRS**.

Paso 6 Ejecute el siguiente comando para acceder al directorio **/tmp** del clúster A.

hdfs dfs -ls hdfs://192.168.6.159:9820/tmp

En el comando anterior, **192.168.6.159** es la dirección IP del NameNode activo del clúster A; **9820** es el puerto predeterminado para la comunicación entre el cliente y el NameNode.

Paso 7 Ejecute el siguiente comando para crear un archivo en el directorio **/tmp** del clúster A:

hdfs dfs -touchz hdfs://192.168.6.159:9820/tmp/mrstest.txt

Si puede consultar el archivo **mrstest.txt** en el directorio **/tmp** del clúster A, la confianza mutua entre clústeres se configura correctamente.

----Fin

8.15 Guía de operación de parches

8.15.1 Guía de operación de parches para versiones

Si obtiene información de parches de los siguientes orígenes, actualice el parche según los requisitos reales.

- Obtendrá información sobre el parche publicado por MRS a partir de un mensaje enviado por el servicio del centro de mensajes.
- Para obtener información sobre el parche, acceda al clúster y vea la información del parche.

Preparación para la instalación de parches

- Siga las instrucciones de **Realización de una comprobación de estado** para comprobar el estado del clúster. Si el estado del clúster es normal, instale un parche.
- Debe confirmar que el parche de destino se instale de acuerdo con la información del parche en el contenido del parche.

Instalación de un parche

Paso 1 Inicie sesión en la consola de gestión de MRS.

Paso 2 Elija **Clusters > Active Clusters** y haga clic en el nombre del clúster que se va a consultar para entrar en la página que muestra la información básica del clúster.

Paso 3 En la página **Patch Information**, haga clic en **Install** en la columna **Operation** para instalar el parche de destino.

NOTA

- Para obtener más información sobre las operaciones de parches enrollables, consulte **Soporte de parches rodantes**.
- Para los nodos host aislados del clúster, siga las instrucciones en **Restauración de parches para los hosts aislados** para restaurar el parche.

----Fin

Desinstalación de un parche

Paso 1 Inicie sesión en la consola de gestión de MRS.

Paso 2 Elija **Clusters > Active Clusters** y haga clic en el nombre del clúster que se va a consultar para entrar en la página que muestra la información básica del clúster.

Paso 3 En la página **Patch Information**, haga clic en **Uninstall** en la columna **Operation** para desinstalar el parche de destino.

NOTA

- Para obtener más información sobre las operaciones de parches enrollables, consulte **Soporte de parches rodantes**.
- Para los nodos host aislados del clúster, siga las instrucciones en **Restauración de parches para los hosts aislados** para restaurar el parche.

----Fin

8.15.2 Soporte de parches rodantes

La función de parche rodante indica que los parches se instalan o desinstalan para uno o más servicios en un clúster realizando un reinicio de servicio rodante (reiniciar servicios o instancias en lotes), sin interrumpir los servicios o dentro de un intervalo de interrupción de servicio minimizado. Los servicios de un clúster se dividen en los tres tipos siguientes en función de si admiten parches continuos:

- Servicios que admiten la instalación o desinstalación de parches continuos: Todas las empresas o parte de ellas (variando en función de los diferentes servicios) de los servicios no se interrumpen durante la instalación o desinstalación de parches.
- Servicios que no admiten la instalación o desinstalación de parches continuos: los negocios de los servicios se interrumpen durante la instalación o desinstalación de parches.
- Servicios con algunas funciones que admiten la instalación o desinstalación de parches continuos: Algunas empresas de los servicios no se interrumpen durante la instalación o desinstalación de parches.

Tabla 8-54 proporciona servicios e instancias que admiten o no admiten reinicio continuo en el clúster de MRS.

Tabla 8-54 Servicios e instancias que admiten o no admiten reinicio continuo

Servicio	Instancia	Si se admite el reinicio continuo
HDFS	NameNode	Sí
	ZKFC	
	JournalNode	
	HttpFS	
	DataNode	
Yarn	ResourceManager	Sí
	NodeManager	
Hive	MetaStore	Sí
	WebHCat	
	HiveServer	
MapReduce	JobHistoryServer	Sí

Servicio	Instancia	Si se admite el reinicio continuo
HBase	HMaster	Sí
	RegionServer	
	ThriftServer	
	RESTServer	
Spark	JobHistory	Sí
	JDBCServer	
	SparkResource	No
Hue	Hue	No
Tez	TezUI	No
Loader	Sqoop	No
ZooKeeper	QuorumPeer	Sí
Kafka	Broker	Sí
	MirrorMaker	No
Flume	Flume	Sí
	MonitorServer	
Storm	Nimbus	Sí
	UI	
	Supervisor	
	LogViewer	

Instalación de un parche

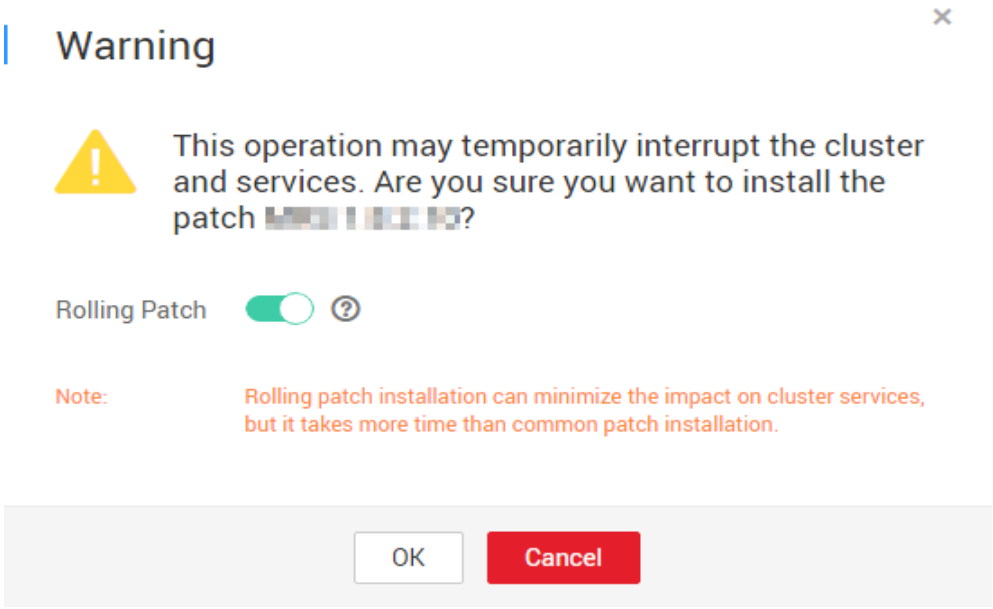
Paso 1 Inicie sesión en la consola de gestión de MRS.

Paso 2 Seleccione **Clusters** > **Active Clusters** y haga clic en el nombre del clúster que se va a consultar para entrar en la página que muestra la información básica del clúster.

Paso 3 En la página **Patch Information**, haga clic en **Install** en la columna **Operation**.

Paso 4 En la página **Warning**, active o desactive **Rolling Patch**.

Figura 8-26 Instalación de parches rodantes



NOTA

- Activación de la función de instalación de parches continuos: los servicios no se detienen antes de la instalación del parche y el reinicio del servicio continuo se realiza después de la instalación del parche. Esto minimiza el impacto en los servicios de clúster, pero lleva más tiempo que la instalación de parches común.
- Desactivación de la función de desinstalación continua de parches: todos los servicios se detienen antes de la desinstalación de parches y todos los servicios se reinician después de la desinstalación de parches. Esto interrumpe temporalmente el clúster y los servicios, pero toma menos tiempo que la desinstalación continua de parches.
- La función de instalación de parches continuos no está disponible en clústeres con menos de dos nodos de Master y tres nodos de Core.

Paso 5 Haga clic en **OK** para instalar el parche de destino.

Paso 6 Vea el progreso de la instalación del parche.

1. Acceda a MRS Manager. Para obtener más información, consulte **Acceso a MRS Manager (MRS 2.x o anterior)**.
2. Elija **System** > **Manage Patch**. En la página **Manage Patch**, puede ver el progreso de la instalación del parche.

NOTA

Para los nodos host aislados del clúster, siga las instrucciones en **Restauración de parches para los hosts aislados** para restaurar el parche.

----Fin

Desinstalación de un parche

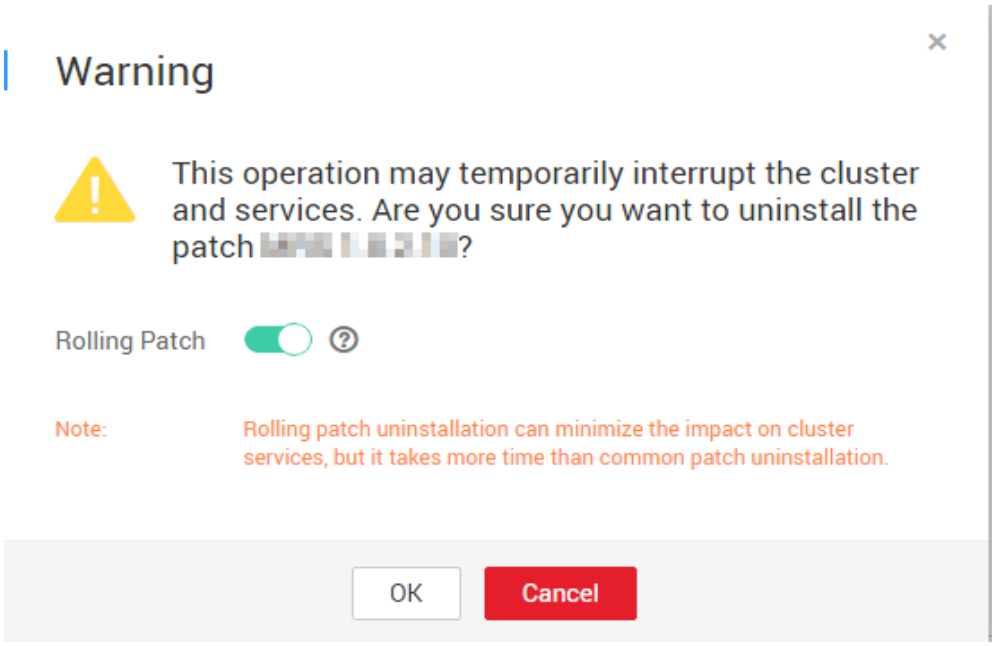
Paso 1 Inicie sesión en la consola de gestión de MRS.

Paso 2 Seleccione **Clusters** > **Active Clusters** y haga clic en el nombre del clúster que se va a consultar para entrar en la página que muestra la información básica del clúster.

Paso 3 En la página **Patch Information**, haga clic en **Uninstall** en la columna **Operation**.

Paso 4 En la página **Warning**, active o desactive **Rolling Patch**.

Figura 8-27 Desinstalación de parche rodante



NOTA

- Activación de la función de desinstalación de parches continuos: los servicios no se detienen antes de la desinstalación de parches y el reinicio de servicio continuo se realiza después de la desinstalación de parches. Esto minimiza el impacto en los servicios de clúster, pero lleva más tiempo que la desinstalación de parches común.
- Desactivación de la función de desinstalación continua de parches: todos los servicios se detienen antes de la desinstalación de parches y todos los servicios se reinician después de la desinstalación de parches. Esto interrumpe temporalmente el clúster y los servicios, pero toma menos tiempo que la desinstalación continua de parches.
- La función de desinstalación de parches continuos no está disponible en clústeres con menos de dos nodos de Master y tres nodos de Core.

Paso 5 Haga clic en **OK** para desinstalar el parche de destino.

Paso 6 Vea el progreso de la desinstalación del parche.

1. Acceda a MRS Manager. Para obtener más información, consulte **Acceso a MRS Manager (MRS 2.x o anterior)**.
2. Elija **System** > **Manage Patch**. En la página **Manage Patch**, puede ver el progreso de la desinstalación del parche.

NOTA

Para los nodos host aislados del clúster, siga las instrucciones en **Restauración de parches para los hosts aislados** para restaurar el parche.

----Fin

8.16 Restauración de parches para los hosts aislados

Si algunos hosts están aislados en un clúster, realice las siguientes operaciones para restaurar los parches para estos hosts aislados después de la instalación de parches en otros hosts del clúster. Después de la restauración de parches, las versiones de los nodos host aislados son consistentes con aquellos no están aislados.

Paso 1 Acceda a MRS Manager. Para obtener más información, consulte **Acceso a MRS Manager (MRS 2.x o anterior)**.

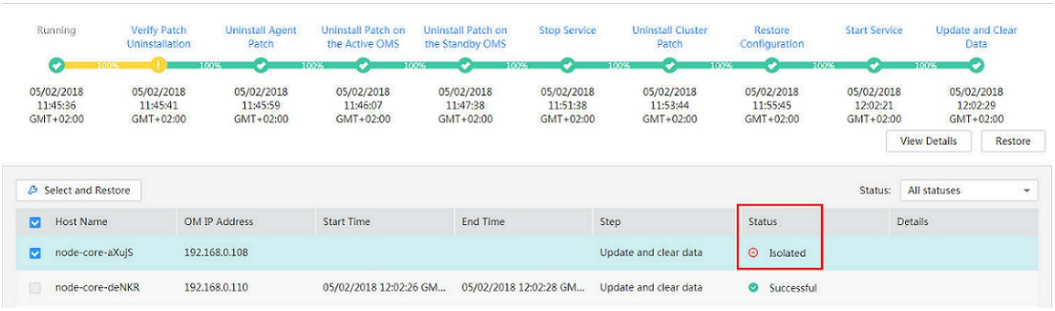
Paso 2 Elija **System** > **Manage Patch**. Se muestra la página **Manage Patch**.

Paso 3 En la columna **Operation**, haga clic en **View Details**.

Paso 4 En la página de detalles del parche, seleccione los nodos de host cuyo **Status** sea **Isolated**.

Paso 5 Haga clic en **Select and Restore** para restaurar los nodos de host aislados.

Figura 8-28 Restauración de parches para los hosts aislados



----Fin

8.17 Reinicio rodante

Después de modificar los elementos de configuración de un componente de big data, debe reiniciar el servicio correspondiente para que las nuevas configuraciones surtan efecto. Si utiliza un modo de reinicio normal, todos los servicios o instancias se reinician simultáneamente, lo que puede provocar una interrupción del servicio. Para asegurarse de que los servicios no se vean afectados durante el reinicio del servicio, puede reiniciar servicios o instancias en lotes mediante el reinicio continuo. Para las instancias en modo activo/en espera, una instancia en espera se reinicia primero y luego se reinicia una instancia activa. El reinicio continuo tarda más de lo normal.

Tabla 8-55 proporciona servicios e instancias que admiten o no admiten reinicio continuo en el clúster de MRS.

Tabla 8-55 Servicios e instancias que admiten o no admiten reinicio continuo

Servicio	Instancia	Si se admite el reinicio continuo
HDFS	NameNode	Sí

Servicio	Instancia	Si se admite el reinicio continuo
	ZKFC	
	JournalNode	
	HttpFS	
	DataNode	
Yarn	ResourceManager	Sí
	NodeManager	
Hive	MetaStore	Sí
	WebHCat	
	HiveServer	
MapReduce	JobHistoryServer	Sí
HBase	HMaster	Sí
	RegionServer	
	ThriftServer	
	RESTServer	
Spark	JobHistory	Sí
	JDBCServer	
	SparkResource	No
Hue	Hue	No
Tez	TezUI	No
Loader	Sqoop	No
ZooKeeper	Quorumpeer	Sí
Kafka	Broker	Sí
	MirrorMaker	No
Flume	Flume	Sí
	MonitorServer	
Storm	Nimbus	Sí
	UI	
	Supervisor	
	Logviewer	

Restricciones

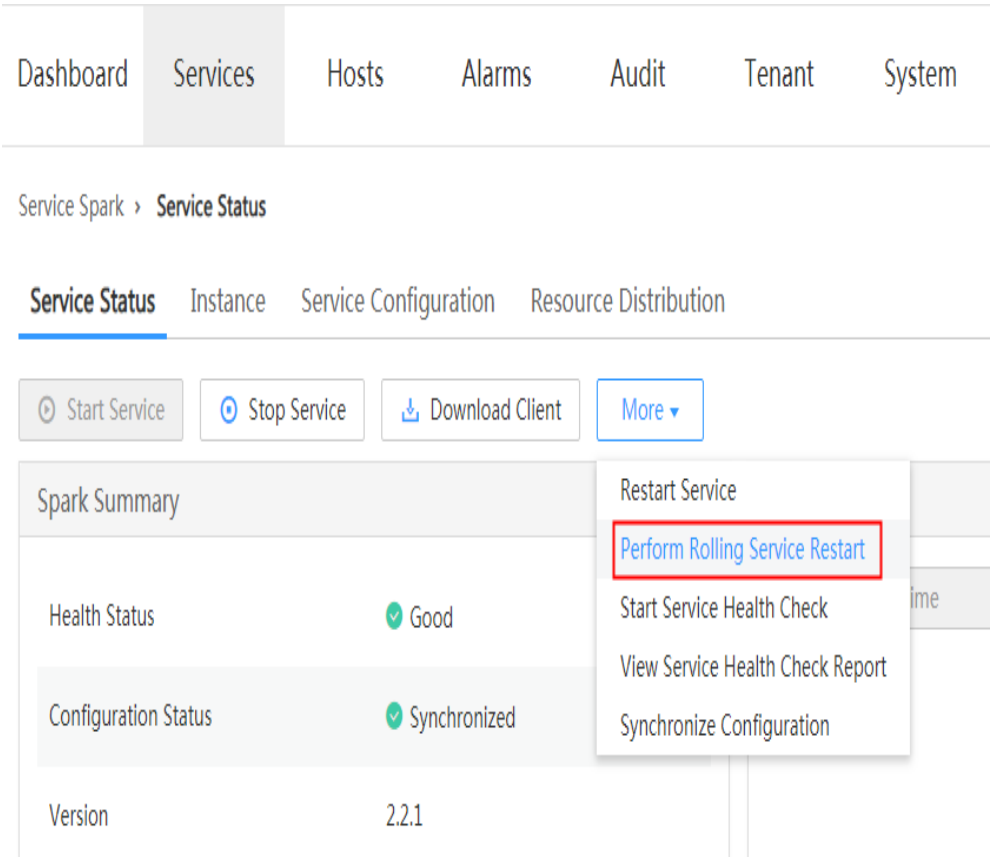
- Realice un reinicio continuo durante las horas fuera de pico.
  - De lo contrario, puede producirse una falla de reinicio continuo. Por ejemplo, si el rendimiento de Kafka es alto (más de 100 MB/s) durante el reinicio de balanceo de Kafka, el reinicio de balanceo de Kafka puede fallar.
  - Por ejemplo, si las solicitudes por segundo de cada RegionServer en la interfaz nativa exceden 10,000 durante el reinicio continuo de HBase, debe aumentar el número de identificadores para evitar una falla de reinicio de RegionServer causado por cargas pesadas durante el reinicio.
- Antes del reinicio, compruebe el número de solicitudes actuales de HBase. Si las solicitudes de cada RegionServer en la interfaz nativa superan los 10,000 aumente el número de identificadores para evitar una falla.
- Si el número de nodos de Core en un clúster es inferior a seis, los servicios pueden verse afectados durante un corto período de tiempo.
- Preferentemente, realice un reinicio de instancia o servicio continuo y seleccione **Only restart instances whose configurations have expired**.

Realización de un reinicio de servicio continuo

Paso 1 En MRS Manager, haga clic en **Services** y seleccione un servicio para el que desee realizar un reinicio continuo.

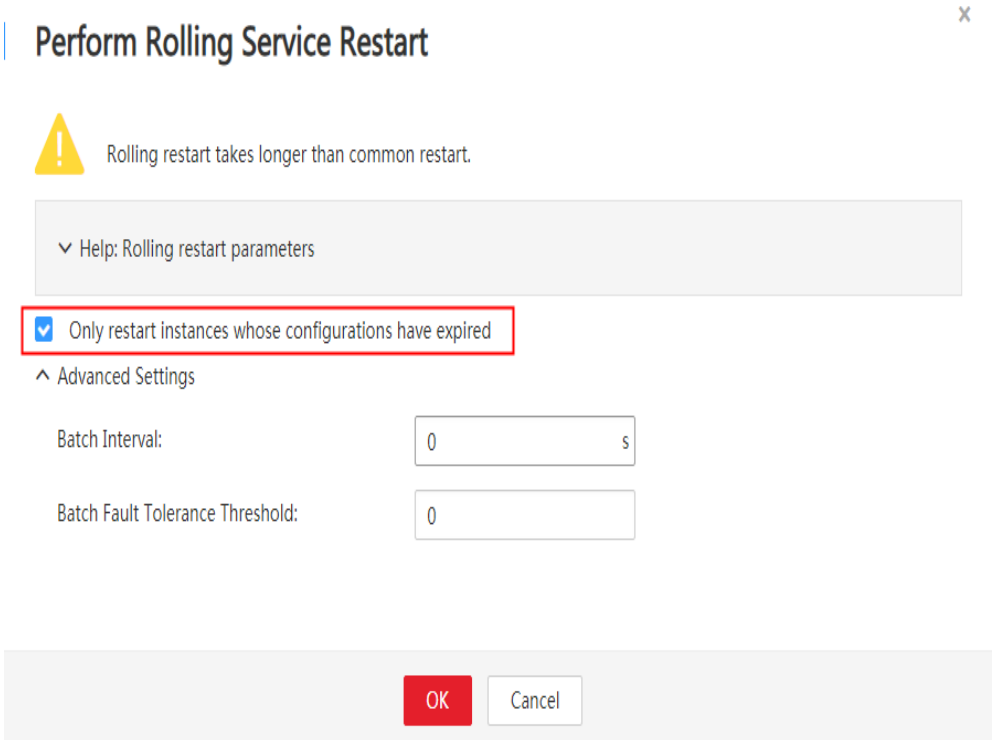
Paso 2 En la página de la pestaña **Service Status**, haga clic en **More** y seleccione **Perform Rolling Service Restart**.

Figura 8-29 Estado del servicio



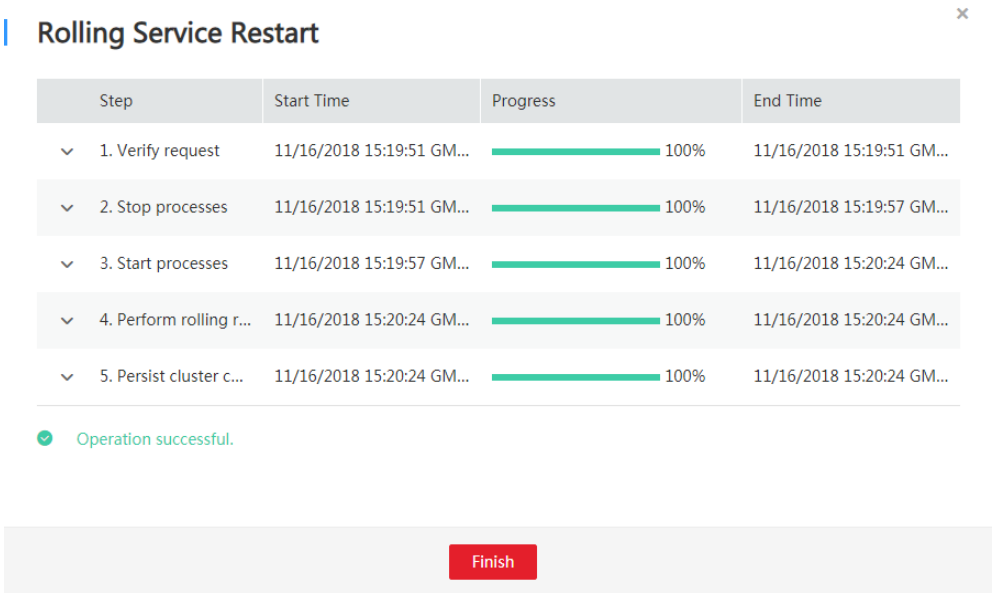
Paso 3 Después de introducir la contraseña de administrador, se muestra la página **Perform Rolling Service Restart**. Seleccione **Only restart instances whose configurations have expired** y haga clic en **OK** para realizar el reinicio continuo del servicio.

Figura 8-30 Realización de un reinicio de servicio continuo



Paso 4 Una vez completada la tarea de reinicio continuo, haga clic en **Finish**.

Figura 8-31 Finalización del reinicio del servicio continuo



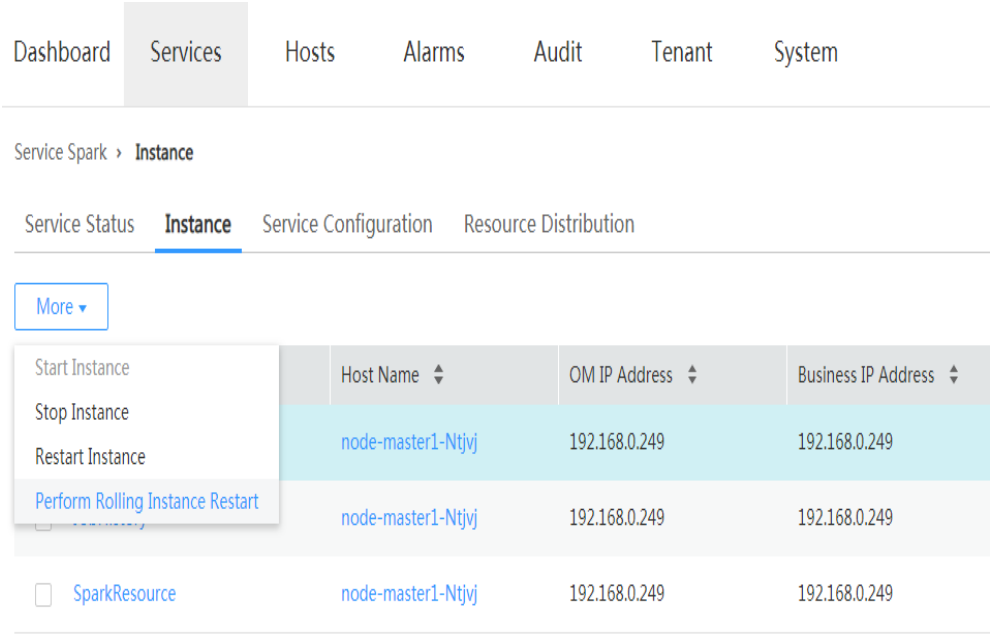
----Fin

Realización de un reinicio continuo de instancia

Paso 1 En MRS Manager, haga clic en **Services** y seleccione un servicio para el que desee realizar un reinicio continuo.

Paso 2 En la página de pestaña **Instance**, seleccione la instancia que desea reiniciar. Haga clic en **More** y seleccione **Perform Rolling Instance Restart**.

Figura 8-32 Instancia del servicio



Paso 3 Después de introducir la contraseña de administrador, se muestra la página **Perform Rolling Instance Restart**. Seleccione **Only restart instances whose configurations have expired** y haga clic en **OK** para realizar el reinicio continuo de la instancia.

Paso 4 Una vez completada la tarea de reinicio continuo, haga clic en **Finish**.

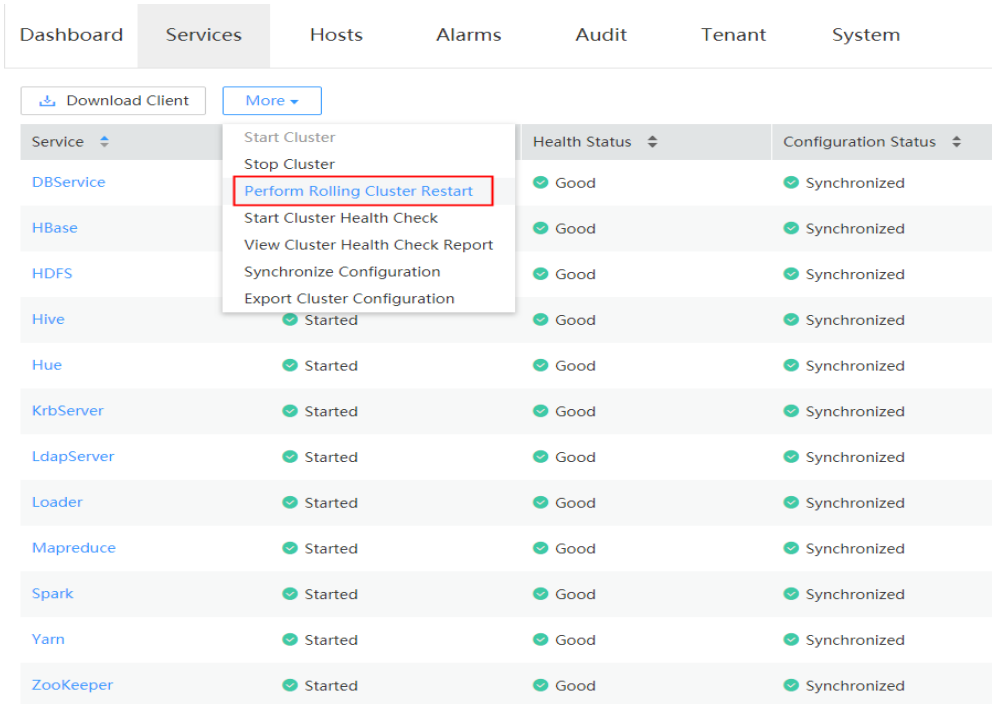
----Fin

Realizar un reinicio de clúster continuo

Paso 1 En el Administrador de MRS, haga clic en **Services**. Se muestra la página **Services**.

Paso 2 Haga clic en **More** y seleccione **Perform Rolling Cluster Restart**.

Figura 8-33 Servicios



Paso 3 Después de introducir la contraseña de administrador, se muestra la página **Perform Rolling Cluster Restart**. Seleccione **Only restart instances whose configurations have expired** y haga clic en **OK** para realizar el reinicio continuo del clúster.

Paso 4 Una vez completada la tarea de reinicio continuo, haga clic en **Finish**.

----Fin

Descripción del parámetro de reinicio continuo

Tabla 8-56 describe los parámetros de reinicio continuo.

Tabla 8-56 Descripción del parámetro de reinicio de balanceo

Parámetro	Descripción
Only restart instances whose configurations have expired	Especifica si se deben reiniciar solo las instancias de un clúster que se hayan modificado.
Data Node Instances to Be Batch Restarted	Especifica la cantidad de instancias que se reinician en cada lote cuando se utiliza la estrategia de reinicio secuencial por lotes. El valor predeterminado es **1**. El valor varía de 1 a 20. Este parámetro solo es válido para nodos de datos.

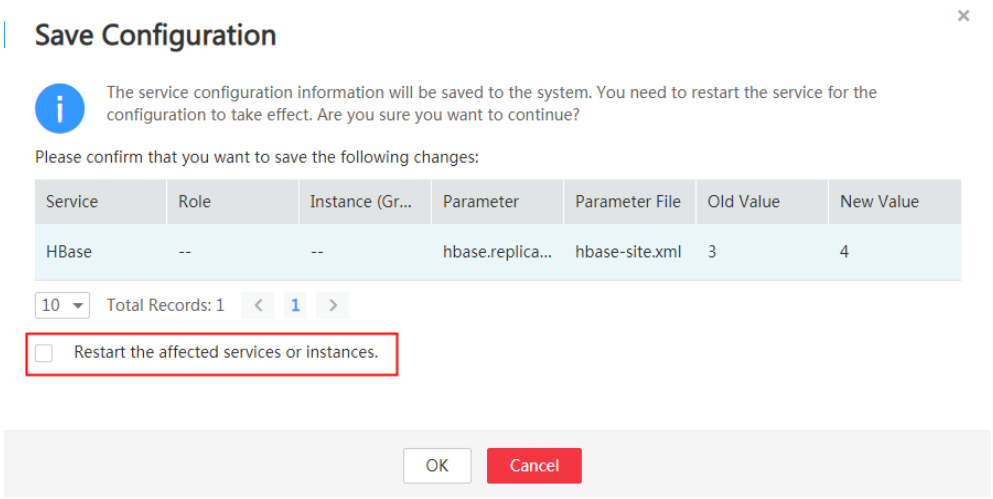
Parámetro	Descripción
Batch Interval	Especifica el intervalo entre dos lotes de instancias para el reinicio continuo. El valor predeterminado es **0**. El valor oscila entre 0 y 2147483647. La unidad es segunda. Nota: Establecer el parámetro de intervalo por lotes puede aumentar la estabilidad del proceso de componente de big data durante el reinicio continuo. Se recomienda establecer este parámetro en un valor no predeterminado, por ejemplo, 10.
Batch Fault Tolerance Threshold	Especifica los tiempos de tolerancia cuando el reinicio continuo de instancias no se ejecuta en lotes. El valor predeterminado es **0**, que indica que la tarea de reinicio continuo finaliza después de que no se reinicie ningún lote de instancias. El valor oscila entre 0 y 214748364.

Procedimiento en un escenario típico

Paso 1 En MRS Manager, haga clic en **Services** y seleccione HBase. Se muestra la página de servicio HBase.

Paso 2 Haga clic en la pestaña **Service Configuration** y modifique un parámetro de HBase. Después de mostrar el siguiente cuadro de diálogo, haga clic en **OK** para guardar las configuraciones.

Figura 8-34 Guardar configuraciones



NOTA

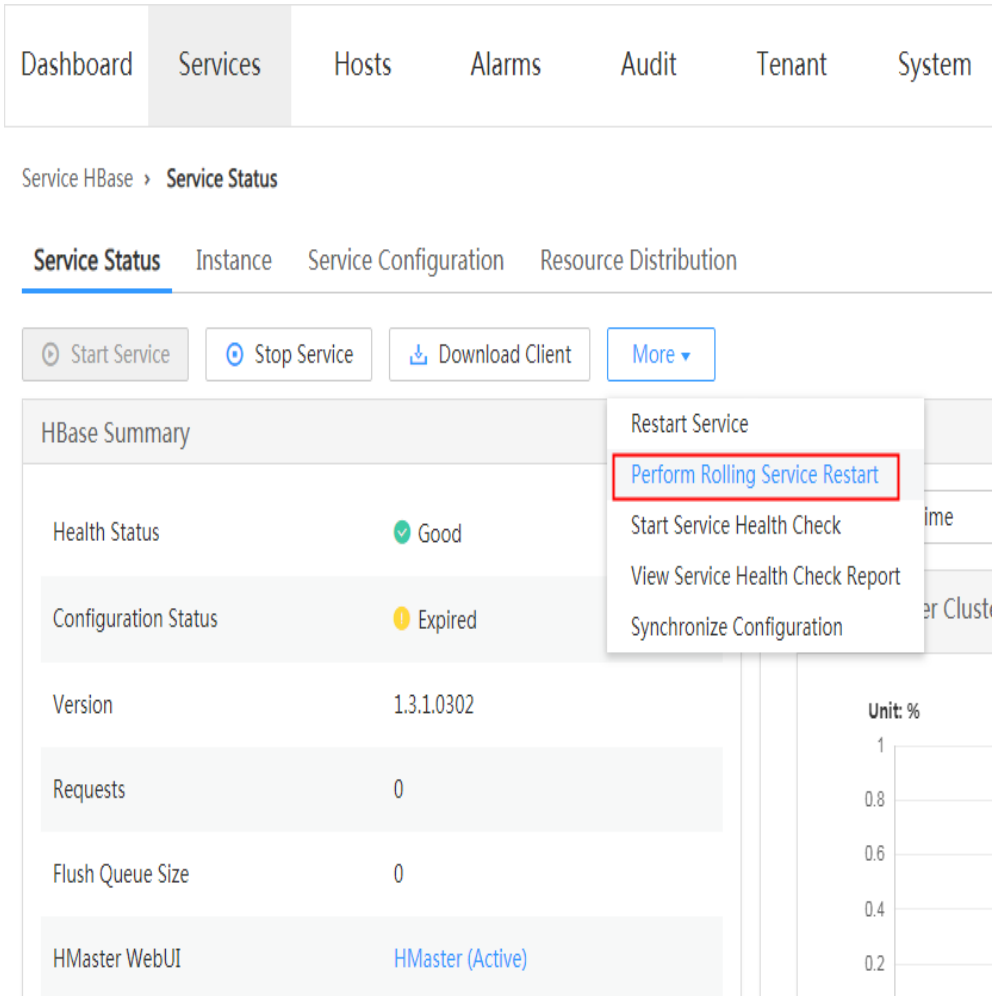
No seleccione **Restart the affected services or instances**. Esta opción indica un reinicio normal. Si selecciona esta opción, se reiniciarán todos los servicios o instancias, lo que puede provocar una interrupción del servicio.

Paso 3 Después de guardar las configuraciones, haga clic en **Finish**.

Paso 4 Haga clic en la pestaña **Service Status**.

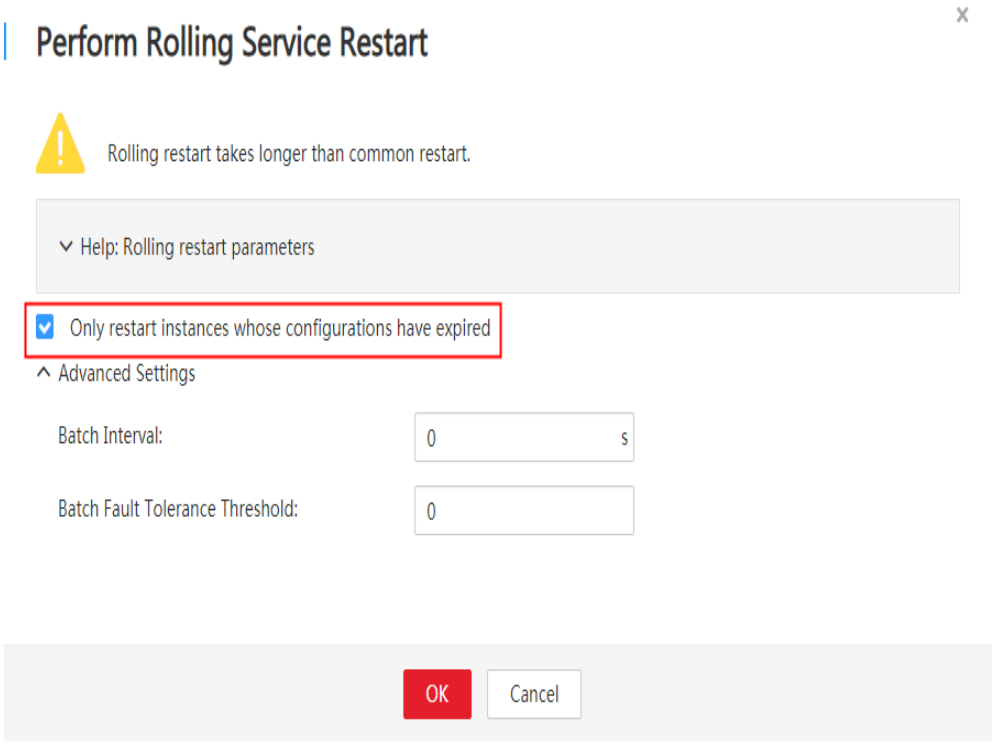
Paso 5 En la página de la pestaña **Service Status**, haga clic en **More** y seleccione **Perform Rolling Service Restart**.

Figura 8-35 Estado del servicio: reinicio continuo



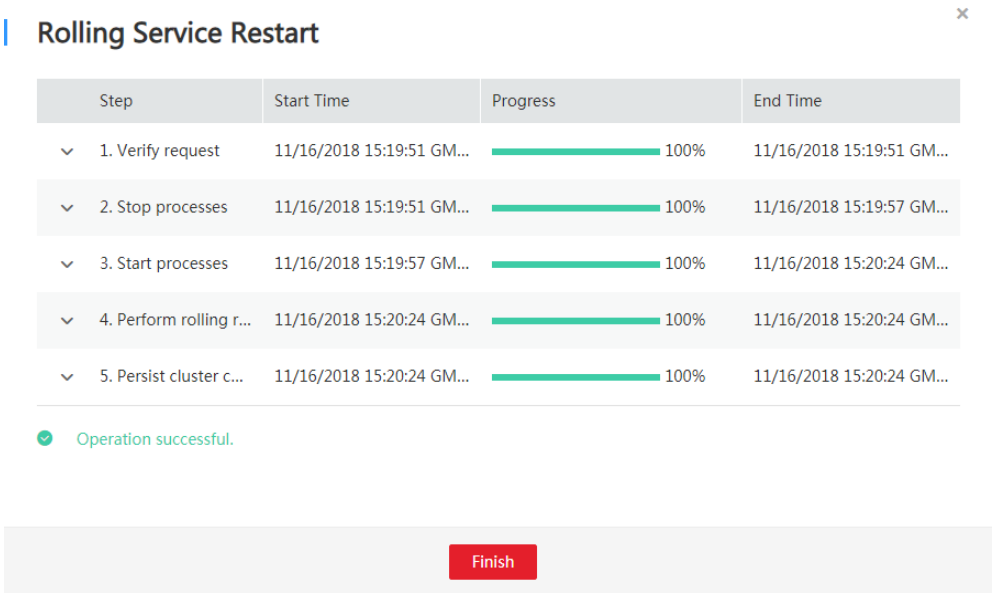
Paso 6 Después de introducir la contraseña de administrador, se muestra la página **Perform Rolling Service Restart**. Seleccione **Only restart instances whose configurations have expired** y haga clic en **OK** para realizar el reinicio continuo del servicio.

Figura 8-36 Configuración del reinicio continuo del servicio



Paso 7 Una vez completada la tarea de reinicio continuo, haga clic en **Finish**.

Figura 8-37 Finalización del reinicio del servicio continuo



----Fin

9 Referencia de alarma (aplicable a MRS 3.x)

9.1 ALM-12001 Error de volcado del registro de auditoría

Descripción

Los registros de auditoría de clúster deben volcarse en un servidor de terceros debido a la política de copia de respaldo de datos históricos locales. El sistema comienza a comprobar el servidor de volcado a las 3 a.m. todos los días. Si el servidor de volcado cumple las condiciones de configuración, los registros de auditoría se pueden volcar correctamente. Esta alarma se genera cuando el volcado del registro de auditoría falla si el espacio en disco del directorio de volcado en el servidor de terceros es insuficiente o si un usuario cambia el nombre de usuario, la contraseña o el directorio de volcado del servidor de volcado.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
12001	Leves	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster o sistema para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

El sistema puede almacenar un máximo de solo 50 archivos de volcado localmente. Si el error persiste en el servidor de volcado, es posible que se pierdan los registros de auditoría locales.

Causas posibles

- La conexión de red es anormal.
- El nombre de usuario, contraseña o directorio de volcado del servidor de volcado no cumple las condiciones de configuración.
- El espacio en disco del directorio de volcado es insuficiente.

Procedimiento

Comprobar si la conexión de red es normal.

Paso 1 En la página de inicio del FusionInsight Manager, seleccione **Audit > Configurations**.

Paso 2 Compruebe si la SFTP IP en la página de configuración de volcado es válida.

Inicie sesión en el nodo donde se encuentra Manager como usuario **root** y ejecute el comando **ping** para comprobar si la conexión de red entre el servidor SFTP y el clúster es normal.

- En caso afirmativo, vaya a **Paso 5**.
- Si no, vaya a **Paso 3**.

Paso 3 Repare la conexión de red, restablezca la contraseña SFTP y haga clic en **OK**.

Paso 4 Espere 2 minutos y compruebe si la alarma está desactivada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 5**.

Compruebe si el nombre de usuario, la contraseña o el directorio de volcado son correctos.

Paso 5 En la página de configuración de volcado, compruebe si el nombre de usuario, la contraseña y el directorio de volcado del servidor de terceros son correctos.

- En caso afirmativo, vaya a **Paso 8**.
- Si no, vaya a **Paso 6**.

Paso 6 Cambie el nombre de usuario, la contraseña o el directorio de volcado, restablezca la contraseña SFTP y haga clic en **OK**.

Paso 7 Espere 2 minutos y compruebe si la alarma está desactivada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 8**.

Compruebe si el espacio en disco del directorio de volcado es suficiente.

Paso 8 Inicie sesión en el servidor de terceros como usuario **root** y ejecute el comando **df** para comprobar si el espacio en disco del directorio de volcado del servidor de terceros supera los 100 MB.

- En caso afirmativo, vaya a **Paso 11**.
- Si no, vaya a **Paso 9**.

Paso 9 Amplíe la capacidad de espacio en disco para el servidor de terceros, restablezca la contraseña SFTP y haga clic en **OK**

Paso 10 Espere 2 minutos, vea las alarmas en tiempo real y compruebe si la alarma está desactivada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 11**.

Restablezca la regla de volcado.

Paso 11 En la página de inicio del FusionInsight Manager, seleccione **Audit > Configurations**.

Paso 12 Reinicie las reglas de volcado, establezca los parámetros correctamente y haga clic en **OK**.

Paso 13 Espere 2 minutos, vea las alarmas en tiempo real y compruebe si la alarma está desactivada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 14**.

Recopilar información de fallas.

Paso 14 En el FusionInsight Manager, elija **O&M** > **Log > Download**.

Paso 15 Seleccione **OmmServer** en el **Service** y haga clic en **OK**.

Paso 16 Haga clic en  en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 17 Póngase en contacto con el y envíe la información de registro recopilada.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.2 ALM-12004 Recurso OLdap anormal

Descripción

El sistema comprueba los recursos LDAP cada 60 segundos. Esta alarma se genera cuando el sistema detecta que los recursos LDAP en Manager son anormales durante seis veces consecutivas.

Esta alarma se borra cuando el recurso Ldap en el Manager se recupera y se completa el manejo de alarmas.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
12004	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster o sistema para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

Los servicios de autenticación Manager y WebUI del componente no están disponibles y no pueden proporcionar funciones de autenticación de seguridad y gestión de usuarios para los servicios web de capa superior. Es posible que los usuarios no puedan iniciar sesión en los WebUIs de Manager y componentes.

Causas posibles

El proceso LdapServer en el Manager es anormal.

Procedimiento

Comprobar si el proceso de LdapServer en el Manager es normal.

Paso 1 Inicie sesión en el nodo Manager en el clúster como usuario **omm**.

Inicie sesión en el FusionInsight Manager con la dirección IP flotante y ejecute el comando **sh ${BIGDATA_HOME}/om-server/om/sbin/status-oms.sh** para comprobar la información sobre el clúster actual de dos nodos del Manager.

Paso 2 Ejecute el comando **ps -ef | grep slapd** para comprobar si el proceso de recursos LdapServer en **${BIGDATA_HOME}/om-server/om/** en el archivo de configuración del proceso se está ejecutando correctamente.

NOTA

Puede determinar que el recurso es normal comprobando la siguiente información:

1. Después de que se ejecute el comando **sh ${BIGDATA_HOME}/om-server/om/sbin/status-oms.sh**, **ResHAStatus** del OLdap es **Normal**.
2. Después de ejecutar el comando **ps -ef | grep slapd**, se puede ver el proceso de slapd del puerto 21750.
   - En caso afirmativo, vaya a **Paso 3**.
   - Si no, vaya a **Paso 4**.

Paso 3 Ejecute el comando **kill -2** *ldap pid* para reiniciar el proceso LdapServer y espere 20 segundos. El HA inicia el proceso OLdap automáticamente. Compruebe si el recurso OLdap actual está en estado normal.

- En caso afirmativo, la operación se ha completado.
- Si no, vaya a **Paso 4**.

Recopilar información de fallas.

Paso 4 En la página de inicio del FusionInsight Manager, elija **O&M** > **Log > Download**.

Paso 5 Seleccione **OmsLdapServer** y **OmmServer** del **Service** y haga clic en **OK**.

Paso 6 Haga clic en  en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 1 hora antes y después del tiempo de generación de alarma, respectivamente. A continuación, haga clic en **Download**.

Paso 7 Póngase en contacto con el y envíe la información de registro recopilada.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.3 ALM-12005 OKerberos Resource Anormal

Descripción

El módulo de alarma comprueba el estado del recurso Kerberos en Manager cada 80 segundos. Esta alarma se genera cuando el módulo de alarma detecta que los recursos de Kerberos son anormales durante seis veces consecutivas.

Esta alarma se borra cuando se recupera el recurso Kerberos y se completa el manejo de alarmas.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
12005	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster o sistema para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

Los servicios de autenticación WebUI del componente no están disponibles y no pueden proporcionar funciones de autenticación de seguridad para los servicios web de capa superior. Es posible que los usuarios no puedan iniciar sesión en el FusionInsight Manager y en los WebUI de los componentes.

Causas posibles

El recurso OLdap del que depende el Okerberos es anormal.

Procedimiento

Compruebe si el recurso OLdap del que depende Okerberos es anómalo en el Manager.

Paso 1 Inicie sesión en el nodo Manager en el clúster como usuario **omm**.

Inicie sesión en el FusionInsight Manager con la dirección IP flotante y ejecute el comando **sh ${BIGDATA_HOME}/om-server/om/sbin/status-oms.sh** para comprobar la información sobre el clúster actual de dos nodos del Manager.

Paso 2 Ejecute el comando **sh ${BIGDATA_HOME}/om-server/OMS/workspace0/ha/module/hacom/script/status_ha.sh** para comprobar si el estado del recurso OLdap gestionado por HA es normal. (En el modo de nodo único, el recurso OLdap está en el estado Active_normal; en el modo de dos nodos, el recurso OLdap está en el estado Active_normal en el nodo activo y en el estado Standby_normal en el nodo de espera.)

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 3**.

Paso 3 Consulte el procedimiento de **ALM-12004 Recurso OLdap anormal** para resolver el problema. Después de recuperar el estado del recurso OLdap, compruebe si el estado del recurso OKerberos es normal.

- En caso afirmativo, la operación se ha completado.
- Si no, vaya a **Paso 4**.

Recopilar información de fallas.

Paso 4 En la página de inicio del Administrador FusionInsight, elija **O&M** > **Log > Download**.

Paso 5 Seleccione **OmsKerberos** y **OmmServer** del **Service** y haga clic en **OK**.

Paso 6 Haga clic en  en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 1 hora antes y después del tiempo de generación de alarma, respectivamente. A continuación, haga clic en **Download**.

Paso 7 Póngase en contacto con el y envíe la información de registro recopilada.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.4 ALM-12006 Falla de nodo

Descripción

El Controller comprueba el latido del corazón de NodeAgent cada 30 segundos. Si el Controller no recibe mensajes de latidos de un NodeAgent, intenta reiniciar el proceso de NodeAgent. Esta alarma se genera si el NodeAgent no se reinicia durante tres veces consecutivas.

Esta alarma se borra cuando el Controller puede recibir correctamente el informe de estado del NodeAgent.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
12006	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster o sistema para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

Los servicios del nodo no están disponibles.

Causas posibles

- La red está desconectada, el hardware está defectuoso o el sistema operativo se ejecuta lentamente.
- La memoria del proceso de NodeAgent es insuficiente.

Procedimiento

Compruebe si la red está desconectada, si el hardware está defectuoso o si el sistema operativo ejecuta los comandos con lentitud.

Paso 1 En FusionInsight Manager, seleccione **O&M** > **Alarm** > **Alarms**. En la página que se muestra, haga clic en ⌄ en la fila que contiene la alarma, haga clic en el nombre del host y vea la dirección IP del host para el que se genera la alarma.

Paso 2 Inicie sesión en el nodo de gestión activo como usuario **root**.

NOTA

Si el nodo defectuoso es el nodo de gestión activo y falla el inicio de sesión, la red del nodo de gestión activo puede estar defectuosa. En este caso, vaya a **Paso 4**.

Paso 3 Ejecute el comando **ping** *IP address of the faulty host* para comprobar si el nodo defectuoso es accesible.

- En caso afirmativo, vaya a **Paso 12**.
- Si no, vaya a **Paso 4**.

Paso 4 Póngase en contacto con el administrador de la red para comprobar si la red es defectuosa.

- En caso afirmativo, vaya a **Paso 5**.
- Si no, vaya a **Paso 6**.

Paso 5 Rectifique la falla de la red y compruebe si la alarma está borrada de la lista de alarmas.

- De ser así, no se requiere ninguna acción adicional.

- Si no, vaya a **Paso 6**.

Paso 6 Póngase en contacto con el administrador de hardware para comprobar si el hardware (CPU o memoria) del nodo está defectuoso.

- En caso afirmativo, vaya a **Paso 7**.
- Si no, vaya a **Paso 12**.

Paso 7 Repare o reemplace los componentes defectuosos y reinicie el nodo. Verifique si la alarma se ha borrado.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 8**.

Paso 8 Si se notifica un gran número de fallas de nodo en el clúster, las direcciones IP flotantes pueden ser anormales. Como resultado, Controller no puede detectar el latido del corazón de NodeAgent.

Inicie sesión en cualquier nodo de gestión y vea el registro **/var/log/Bigdata/omm/oms/ha/scriptlog/floatip.log** para comprobar si los registros generados uno o dos minutos antes y después de que se produzcan los errores están completos.

Por ejemplo, un registro completo tiene el siguiente formato:

```
2017-12-09 04:10:51,000 INFO (floatip) Read from ${BIGDATA_HOME}/om-
server_*/om/etc/om/routeSetConf.ini,value is : yes
2017-12-09 04:10:51,000 INFO (floatip) check wsNetExport : eth0 is up.
2017-12-09 04:10:51,000 INFO (floatip) check omNetExport : eth0 is up.
2017-12-09 04:10:51,000 INFO (floatip) check wsInterface : eRth0:oms, wsFloatIp:
XXX.XXX.XXX.XXX.
2017-12-09 04:10:51,000 INFO (floatip) check omInterface : eth0:oms, omFloatIp:
XXX.XXX.XXX.XXX.
2017-12-09 04:10:51,000 INFO (floatip) check  wsFloatIp : XXX.XXX.XXX.XXX is
reachable.
2017-12-09 04:10:52,000 INFO (floatip) check  omFloatIp : XXX.XXX.XXX.XXX is
reachable.
```

- En caso afirmativo, vaya a **Paso 12**.
- Si no, vaya a **Paso 9**.

Paso 9 Compruebe si el registro de omNetExport se imprime después de detectar wsNetExport o si el intervalo para imprimir dos registros supera los 10 segundos o más.

- En caso afirmativo, vaya a **Paso 10**.
- Si no, vaya a **Paso 12**.

Paso 10 Vea el archivo **/var/log/message** del sistema operativo para comprobar si sssd se reinicia con frecuencia o si se muestra información de excepción nscd cuando se produce el error. Para Red Hat, compruebe información de sssd. Para SUSE, compruebe la información de nscd.

ejemplo de reinicio de sssd

```
Feb  7 11:38:16 10-132-190-105 sssd[pam]: Shutting down
Feb  7 11:38:16 10-132-190-105 sssd[nss]: Shutting down
Feb  7 11:38:16 10-132-190-105 sssd[nss]: Shutting down
Feb  7 11:38:16 10-132-190-105 sssd[be[default]]: Shutting down
Feb  7 11:38:16 10-132-190-105 sssd: Starting up
Feb  7 11:38:16 10-132-190-105 sssd[be[default]]: Starting up
Feb  7 11:38:16 10-132-190-105 sssd[nss]: Starting up
Feb  7 11:38:16 10-132-190-105 sssd[pam]: Starting up
```

Ejemplo de información de excepción de nscd

```
Feb 11 11:44:42 10-120-205-33 nscd: nss_ldap: failed to bind to LDAP server
ldaps://10.120.205.55:21780: Can't contact LDAP server
```



```
Feb 11 11:44:43 10-120-205-33 ntpq: nss_ldap: failed to bind to LDAP server
ldaps://10.120.205.55:21780: Can't contact LDAP server
Feb 11 11:44:44 10-120-205-33 ntpq: nss_ldap: failed to bind to LDAP server
ldaps://10.120.205.92:21780: Can't contact LDAP server
```

- En caso afirmativo, vaya a **Paso 11**.
- Si no, vaya a **Paso 14**.

Paso 11 Compruebe si el nodo LdapServer es defectuoso, por ejemplo, la dirección IP del servicio es inalcanzable o la latencia de la red es demasiado alta. Si la falla se produce periódicamente, ubique y elimínelo y ejecute el comando **top** para comprobar si existe software anormal.

Compruebe si la memoria del proceso NodeAgent es insuficiente.

Paso 12 Inicie sesión en el nodo defectuoso como usuario **root** y ejecute el siguiente comando para ver los registros del proceso de NodeAgent:

vi /var/log/Bigdata/nodeagent/scriptlog/agent_gc.log.*.current

Paso 13 Compruebe si el archivo de registro contiene un error que indica que el tamaño del metaespacio o el tamaño de la memoria heap es insuficiente.

- En caso afirmativo, póngase en contacto con el personal de para cambiar el tamaño de la memoria.
- Si no, vaya a **Paso 14**.

Recopilar información de fallas.

Paso 14 En FusionInsight Manager, seleccione **O&M**. En el panel de navegación de la izquierda, elija **Log** > **Download**.

Paso 15 Seleccione los siguientes nodos de **Services** y haga clic en **OK**.

- NodeAgent
- Controller
- OS

Paso 16 Haga clic en  en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 17 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

Información relacionada

Ninguna

9.5 ALM-12007 Falla de proceso

Descripción

Esta alarma se genera cuando el módulo de comprobación de estado de proceso detecta que el estado de conexión de proceso es **Bad** tres veces consecutivas. El módulo de comprobación de estado del proceso comprueba el estado del proceso cada 5 segundos.

Esta alarma se borra cuando se puede conectar el proceso.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
12007	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster o sistema para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

El servicio proporcionado por el proceso no está disponible.

Causas posibles

- El proceso de instancia es anormal.
- El espacio del disco no es suficiente.

NOTA

Si existe un gran número de alarmas de falla de proceso en un segmento de tiempo, los archivos en el directorio de instalación pueden borrarse por error o el permiso en el directorio puede modificarse.

Procedimiento

Comprobar si el proceso de instancia es anormal.

Paso 1 En el portal del FusionInsight Manager, haga clic en **O&M > Alarm > Alarms**, haga clic en ⌄ en la fila donde se encuentra la alarma y haga clic en el nombre del host para ver la dirección del host para la que se genera la alarma

Paso 2 En la página **Alarms**, compruebe si se ha generado el **ALM-12006 Falla de nodo**.

- En caso afirmativo, vaya a **Paso 3**.
- Si no, vaya a **Paso 4**.

Paso 3 Manejar la alarma según **ALM-12006 Falla de nodo**.

Paso 4 Inicie sesión en el host para el que se genera la alarma como usuario **root**. Compruebe si el usuario del directorio de instalación, el grupo de usuarios y el permiso del rol de alarma son correctos. El usuario, el grupo de usuarios y el permiso deben ser **omm:ficommon 750**.

Por ejemplo, el directorio de instalación NameNode es *${BIGDATA_HOME}*/**FusionInsight_Current**/*1_8_NameNode*/**etc**.

- En caso afirmativo, vaya a **Paso 6**.
- Si no, vaya a **Paso 5**.

Paso 5 Ejecute el siguiente comando para establecer el permiso para **750** y **User:Group** para **omm:ficommon**:

chmod 750 <*folder_name*>

chown omm:ficommon <*folder_name*>

Paso 6 Espere 5 minutos. En la lista de alarmas, compruebe si **ALM-12007 Falla de proceso** está borrado.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 7**.

Comprobar si el espacio de disco es suficiente.

Paso 7 En el FusionInsight Manager, compruebe si la lista de alarmas contiene **ALM-12017 Capacidad de disco no suficiente**.

- En caso afirmativo, vaya a **Paso 8**.
- Si no, vaya a **Paso 11**.

Paso 8 Rectifique la falla siguiendo los pasos indicados en el documento **ALM-12017 Capacidad de disco insuficiente**.

Paso 9 Espere 5 minutos. En la lista de alarmas, compruebe si **ALM-12017 Capacidad de disco no suficiente** está borrado.

- En caso afirmativo, vaya a **Paso 10**.
- Si no, vaya a **Paso 11**.

Paso 10 Espere 5 minutos. En la lista de alarmas, compruebe si la alarma está borrada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 11**.

Recopilar información de fallas.

Paso 11 En el FusionInsight Manager, elija **O&M** > **Log > Download**.

Paso 12 De acuerdo con el nombre del servicio obtenido en **Paso 1**, seleccione el componente y el **NodeAgent** del **Service** y haga clic en **OK**.

Paso 13 Haga clic en  en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 14 Póngase en contacto con el y envíe la información de registro recopilada.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.6 ALM-12010 Interrupción del latido del corazón de Manager entre los nodos activo y en espera

Descripción

Esta alarma se genera cuando el Manager activo no recibe la señal de latido del Manager de espera en 7 segundos.

Esta alarma se borra cuando el Manager activo recibe señales de latidos del Manager en espera.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
12010	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster o sistema para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.

Nombre	Significado
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

Cuando el proceso activo de Manager es anormal, no se puede realizar una conmutación por error activa/en espera y los servicios se ven afectados.

Causas posibles

- El enlace entre el Manager activo y en espera es anormal.
- La configuración del nombre de nodo es incorrecta.
- El puerto está deshabilitado por el firewall.

Procedimiento

Comprobar si la red entre el servidor Manager activo y en espera es normal.

Paso 1 En el portal del FusionInsight Manager, haga clic en **O&M > Alarm > Alarms**, haga clic en ⌄ en la fila que contiene la alarma y vea la dirección IP del servidor del Manager de espera (Peer Manager) en los detalles de la alarma.

Paso 2 Inicie sesión en el servidor de Manager activo como usuario **root**.

Paso 3 Ejecute el comando **ping** *standby Manager heartbeat IP address* para comprobar si el servidor de Manager en espera es accesible.

- En caso afirmativo, vaya a **Paso 6**.
- Si no, vaya a **Paso 4**.

Paso 4 Póngase en contacto con el administrador de la red para comprobar si la red es defectuosa.

- En caso afirmativo, vaya a **Paso 5**.
- Si no, vaya a **Paso 6**.

Paso 5 Rectifique la falla de la red y compruebe si la alarma está borrada de la lista de alarmas.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 6**.

Paso 6 Ejecute el siguiente comando para ir al directorio de instalación del software:

cd /opt

Paso 7 Ejecute el siguiente comando para encontrar el directorio del archivo de configuración de los nodos activo y en espera.

find -name hacom_local.xml

Paso 8 Ejecute el siguiente comando para ir al directorio **workspace**:

cd${BIGDATA_HOME}/om-server/OMS/workspace0/ha/local/hacom/conf/

Paso 9 Ejecute el comando **vim** para abrir el archivo **hacom_local.xml**. Compruebe si los nodos local y de otro extremo están configurados correctamente. El nodo local se configura como el nodo activo, y el nodo peer se configura como el nodo en espera.

- En caso afirmativo, vaya a **Paso 12**.
- Si no, vaya a **Paso 10**.

Paso 10 Modifique la configuración de los nodos activo y en espera en el archivo **hacom_local.xml** y pulse **Esc** para volver al modo de comando. Ejecute el comando **:wq** para guardar la modificación y salir.

Paso 11 Compruebe si la alarma se borra automáticamente.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 12**.

Comprobar si el puerto está deshabilitado por el firewall.

Paso 12 Ejecute el comando **lsof -i :20012** para comprobar si los puertos de latido de corazón de los nodos activo y en espera están habilitados. Si se muestra la salida del comando, los puertos están habilitados. De lo contrario, el firewall deshabilita los puertos.

- En caso afirmativo, vaya a **Paso 13**.
- Si no, vaya a **Paso 16**.

Paso 13 Ejecute el comando **iptables -P INPUT ACCEPT** para evitar la desconexión del servidor.

Paso 14 Ejecute el siguiente comando para borrar el firewall:

iptables -F

Paso 15 Compruebe si la alarma está borrada de la lista de alarmas.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 16**.

Recopilar información de fallas.

Paso 16 En el FusionInsight Manager, elija **O&M** > **Log > Download**.

Paso 17 Seleccione los siguientes nodos en el **Service** y haga clic en **OK**:

- OmmServer
- Controller
- NodeAgent

Paso 18 Haga clic en  en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 19 Póngase en contacto con el y envíe la información de registro recopilada.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.7 ALM-12011 Excepción de sincronización de datos de Manager entre los nodos activo y en espera

Descripción

El sistema comprueba la sincronización de datos entre los nodos de Manager activo y en espera cada 60 segundos. Esta alarma se genera cuando el Manager en espera no puede sincronizar archivos con el Manager activo.

Esta alarma se borra cuando el Manager en espera sincroniza los archivos con el Manager activo.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
12011	Crítica	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster o sistema para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

Algunas configuraciones se perderán después de una conmutación activa/en espera porque los archivos de configuración del Manager en espera no están actualizados. Tal vez Manager y algunos componentes no se pueden ejecutar correctamente.

Causas posibles

- El enlace entre los Managers activo y en espera se interrumpe o el espacio de almacenamiento del directorio **/srv/BigData/LocalBackup** está lleno.

- El archivo de sincronización no existe o el permiso del archivo es incorrecto.

Procedimiento

Compruebe si la red entre el servidor de Manager activo y el servidor de Manager en espera es normal.

Paso 1 En el portal del administrador FusionInsight, haga clic en **O&M > Alarm > Alarms**, haga clic en ⌄ en la fila donde se encuentra la alarma y obtenga la dirección IP del servidor del Manager en espera (dirección IP del Peer Manager) en los detalles de la alarma.

Paso 2 Inicie sesión en el servidor de Manager activo como usuario **root**.

Paso 3 Ejecute el comando **ping** *standby Manager IP address* para comprobar si el servidor de Manager en espera es accesible.

- En caso afirmativo, vaya a **Paso 6**.
- Si no, vaya a **Paso 4**.

Paso 4 Póngase en contacto con el administrador de la red para comprobar si la red es defectuosa.

- En caso afirmativo, vaya a **Paso 5**.
- Si no, vaya a **Paso 6**.

Paso 5 Rectifique la falla de la red y compruebe si la alarma está borrada de la lista de alarmas.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 6**.

Compruebe si el espacio de almacenamiento del directorio /srv/BigData/LocalBackup está lleno.

Paso 6 Ejecute el siguiente comando para comprobar si el espacio de almacenamiento del directorio **/srv/BigData/LocalBackup** está lleno:

df -hl /srv/BigData/LocalBackup

- En caso afirmativo, vaya a **Paso 7**.
- Si no, vaya a **Paso 10**.

Paso 7 Ejecute el siguiente comando para borrar archivos de copia de respaldo innecesarios:

rm -rf *Directory to be cleared*

Ejemplo:

rm -rf /srv/BigData/LocalBackup/0/default-oms_20191211143443

Paso 8 En FusionInsight Manager, seleccione **O&M** > **Backup and Restoration** > **Backup Management**.

En la columna **Operation** de la tarea de copia de respaldo que se va a realizar, haga clic en **Configure** y cambie el valor de **Maximum Number of Backup Copies** para reducir el número de conjuntos de archivos de copia de respaldo.

Paso 9 Espere aproximadamente 1 minuto y compruebe si la alarma está desactivada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 10**.

Compruebe si existe el archivo de sincronización y si el permiso del archivo es normal.

Paso 10 Ejecute el siguiente comando para comprobar si existe el archivo de sincronización.

find /srv/BigData/ -name "sed*"

find /opt -name "sed*"

- En caso afirmativo, vaya a **Paso 11**.
- Si no, vaya a **Paso 12**.

Paso 11 Ejecute el siguiente comando para ver la información del archivo de sincronización y el permiso obtenido en **Paso 10**.

ll *path of the file to be found*

- Si el tamaño del archivo es 0 y la columna de permisos es de **-**, el archivo es un archivo no deseado. Ejecute el siguiente comando para eliminarlo.

  rm -rf *files to be deleted*

  Espere varios minutos y compruebe si la alarma está desactivada. Si la alarma persiste, vaya a **Paso 12**.
- Si el tamaño del archivo no es 0, vaya a **Paso 12**.

Paso 12 Vea los archivos de registro generados cuando se genera la alarma.

1. Ejecute el siguiente comando para cambiar a la ruta del archivo de registro de ejecución de HA.

   cd /var/log/Bigdata/omm/oms/ha/runlog/

2. Descomprima y vea los archivos de registro generados cuando se genera la alarma.

   Por ejemplo, si el nombre del archivo que se va a ver es **ha.log.2021-03-22_12-00-07.gz**, ejecute el siguiente comando:

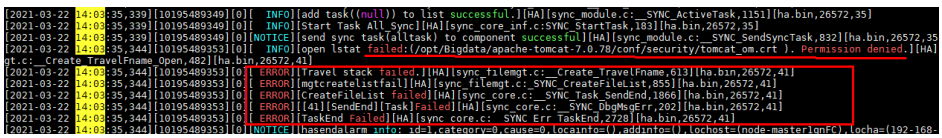
   gunzip *ha.log.2021-03-22_12-00-07.gz*

   vi *ha.log.2021-03-22_12-00-07*

   Compruebe si la información de error se notifica antes y después del tiempo de generación de alarma.

   – En caso afirmativo, rectifique la falla basándose en la información de error. Entonces vaya a **Paso 13**.

     Por ejemplo, si se muestra la siguiente información de error, el permiso de directorio es insuficiente. En este caso, cambie el permiso de directorio para que sea el mismo que en el nodo normal.

   – Si no, vaya a **Paso 14**.

Paso 13 Espere unos 10 minutos y compruebe si la alarma está desactivada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 14**.

Recopilar información de fallas.

Paso 14 En el FusionInsight Manager, elija **O&M** > **Log > Download**.

Paso 15 Seleccione los siguientes nodos en el **Service** y haga clic en **OK**:

- OmmServer
- Controller
- NodeAgent

Paso 16 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 17 Póngase en contacto con el y envíe la información de registro recopilada.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.8 ALM-12012 El servicio NTP es anormal

Descripción

El sistema comprueba si el servicio NTP en un nodo sincroniza el tiempo con el servicio NTP en el nodo OMS activo cada 60 segundos. Esta alarma se genera cuando el servicio NTP no sincroniza el tiempo durante dos veces consecutivas.

Esta alarma se genera cuando la diferencia de tiempo entre el servicio NTP en un nodo y el servicio NTP en el nodo OMS activo es mayor o igual a 20s durante dos veces consecutivas. Esta alarma se borra cuando la diferencia de tiempo es inferior a 20s.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
12012	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster o sistema para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.

Nombre	Significado
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

El tiempo en el nodo es inconsistente con el de otros nodos del clúster. Por lo tanto, es posible que algunas aplicaciones de FusionInsight en el nodo no se ejecuten correctamente.

Causas posibles

- El servicio NTP en el nodo actual no puede iniciarse correctamente.
- El nodo actual no puede sincronizar la hora con el servicio NTP en el nodo OMS activo.
- El valor de clave autenticado por el servicio NTP en el nodo actual es incompatible con el del nodo OMS activo.
- El desplazamiento de tiempo entre el nodo y el servicio NTP en el nodo OMS activo es grande.

Procedimiento

Compruebe el modo de servicio NTP del nodo.

Paso 1 Inicie sesión en el nodo de gestión activo como usuario **root**, ejecute el comando **su - omm** para cambiar a usuario **omm** y ejecute el siguiente comando para comprobar el estado de los recursos en los nodos activo y en espera:

sh ${BIGDATA_HOME}/om-server/om/sbin/status-oms.sh

- Si aparece "chrony" en la columna **ResName** de la salida del comando, vaya a **Paso 2**.
- Si aparece "ntp" en la columna **ResName**, vaya a **Paso 20**.

NOTA

Si tanto "chrony" como "ntp" se muestran en la columna **ResName** de la salida del comando, el modo de servicio NTP se está conmutando. Espere 10 minutos y vaya de nuevo a **Paso 1**. Si tanto la "chrony" como la "ntp" persisten, comuníquese con el personal de.

Verifique si el servicio chrony en el nodo se inició correctamente.

Paso 2 En FusionInsight Manager, seleccione **O&M** > **Alarm** > **Alarms**. En la página que se muestra, haga clic en ⌄ en la fila que contiene la alarma y vea el nombre del host para el que se genera la alarma en **Location**.

Paso 3 Compruebe si el proceso chronyd se está ejecutando en el nodo donde se genera la alarma. Inicie sesión en el nodo para el que se genera la alarma como usuario **root** y ejecute el comando **ps -ef | grep chronyd | grep -v grep** para comprobar si la salida del comando contiene el proceso chronyd.

- En caso afirmativo, vaya a **Paso 6**.

- Si no, vaya a **Paso 4**.

Paso 4 Ejecute el comando **systemctl chronyd start** para iniciar el servicio NTP. (Actualmente, solo se admiten CentOS y Red Hat Enterprise Linux 7.0 o posterior.)

Paso 5 Compruebe si la alarma se borra 10 minutos después.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 6**.

Compruebe si el nodo actual puede sincronizar la hora correctamente con el servicio chrony en el nodo OMS activo.

Paso 6 Compruebe si el nodo puede sincronizar la hora con el servicio NTP en el nodo OMS activo basado en información adicional de la alarma.

- En caso afirmativo, vaya a **Paso 7**.
- Si no, vaya a **Paso 17**.

Paso 7 Compruebe si la sincronización con el servicio chrony en el nodo OMS activo es defectuosa.

Inicie sesión en el nodo para el que se genera la alarma como usuario **root** y ejecute el comando **chronyc sources**.

En la salida del comando, si hay un asterisco (*) antes de la dirección IP del servicio chrony en el nodo OMS activo, la sincronización es normal. La salida del comando es la siguiente:

```
MS Name/IP address         Stratum Poll Reach LastRx Last sample
===============================================================================
^* 10.10.10.162              10  10   377   626    +16us[  +15us] +/-  308us
```

En la salida del comando, si no hay un asterisco (*) antes de la dirección IP del servicio NTP en el nodo OMS activo y el valor de **Reach** es de **0**, la sincronización es anormal.

```
MS Name/IP address         Stratum Poll Reach LastRx Last sample
===============================================================================
^? 10.1.1.1                      0  10     0     -     +0ns[   +0ns] +/-    0ns
```

- En caso afirmativo, vaya a **Paso 8**.
- Si no, vaya a **Paso 38**.

Paso 8 La falla de sincronización de la chrony suele ser causado por el firewall del sistema. Si el firewall se puede desactivar, desactívelo. Si el firewall no se puede deshabilitar, compruebe la política de configuración del firewall y asegúrese de que los puertos UDP 123 y 323 no estén deshabilitados. (Para obtener más información, consulte la política de configuración del firewall de cada sistema.)

Paso 9 Compruebe si la alarma se borra 10 minutos después.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 10**.

Paso 10 Inicie sesión en el nodo OMS activo como usuario **root** y ejecute el siguiente comando para ver el código de autenticación cuyo índice de valor de clave sea **1M**:

En Red Hat Enterprise Linux, ejecute el comando **cat ${BIGDATA_HOME}/om-server/OMS/workspace/conf/chrony.keys**.

Paso 11 Ejecute el siguiente comando para comprobar si el valor de clave es el mismo que el consultado en **Paso 10**:

En Red Hat Enterprise Linux, ejecute el comando **diff ${BIGDATA_HOME}/om-server/OMS/workspace/conf/chrony.keys /etc/chrony.keys**.

NOTA

Si los valores de clave son los mismos, no se devuelve ningún resultado después de ejecutar el comando. Por ejemplo:

```
host01:~ # cat ${BIGDATA_HOME}/om-server/OMS/workspace/conf/chrony.keys
1 M sdYbq;o^CzEAWo<U=Tw5
host01:~ # diff ${BIGDATA_HOME}/om-server/OMS/workspace/conf/chrony.keys /etc/
chrony.keys
host01:~ #
```

- En caso afirmativo, vaya a **Paso 12**.
- Si no, vaya a **Paso 38**.

Paso 12 Ejecute el comando **cat ${BIGDATA_HOME}/om-server/om/packaged-distributables/ntpKeyFile** para comprobar si el valor de la clave es el mismo que el consultado en **Paso 10**. (Compare el valor de clave con el del campo de índice de clave de autenticación **1M** consultado en **Paso 10**.)

- En caso afirmativo, vaya a **Paso 13**.
- Si no, vaya a **Paso 15**.

Paso 13 Inicie sesión en el nodo defectuoso como usuario **root** y ejecute el comando **cat /etc/chrony.keys** en Red Hat Enterprise Linux para comprobar si el valor de la clave es el mismo que el valor consultado en **Paso 12** (utiliza el valor de clave del campo de índice de clave de autenticación **1M** para comparar).

- En caso afirmativo, vaya a **Paso 38**.
- Si no, vaya a **Paso 14**.

Paso 14 Ejecute el comando **su - omm** para cambiar al usuario **omm**, cambie el valor de clave del campo de índice de clave de autenticación **1M** en **${NODE_AGENT_HOME}/chrony.keys** al valor de clave de **ntpKeyFile** en **Paso 12**, y vaya a **Paso 16**.

Paso 15 Ejecute los siguientes comandos como usuario **root** o **omm** para cambiar el valor de clave NTP del nodo OMS activo (cambie **ntp.keys** a **ntpkeys** en Red Hat Enterprise Linux):

cd ${BIGDATA_HOME}/om-server/OMS/workspace/conf

sed -i "`cat chrony.keys | grep -n '1 M'|awk -F ':' '{print $1}'`d" chrony.keys

echo "1 M `cat ${BIGDATA_HOME}/om-server/om/packaged-distributables/ntpKeyFile`" >> chrony.keys

Compruebe si el valor de clave del campo de índice de clave de autenticación **1M** en **chrony.keys** es el mismo que el de **ntpKeyFile**.

- En caso afirmativo, vaya a **Paso 16**.
- Si no, cambie el valor de clave del campo de índice de clave de autenticación **1M** en **chrony.keys** al valor de clave de **ntpKeyFile** y vaya a **Paso 16**.

Paso 16 Después de 5 minutos, ejecute el comando **systemctl chronyd restart** para reiniciar el servicio chrony en el nodo OMS activo. Después de 15 minutos, compruebe si la alarma está desactivada.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 38**.

Compruebe si la desviación de tiempo entre el nodo y el servicio chrony en el nodo OMS activo es grande.

Paso 17 Compruebe si la desviación de tiempo es grande en la información adicional de la alarma.

- En caso afirmativo, vaya a **Paso 18**.
- Si no, vaya a **Paso 38**.

Paso 18 En la página de pestaña **Hosts**, seleccione el host para el que se genera la alarma y elija **More** > **Stop All Instances** para detener todos los servicios en el nodo.

Si el tiempo en el nodo de alarma es posterior al del servicio de chrony del nodo OMS activo, ajuste el tiempo del nodo de alarma. Después de ajustar el tiempo, elija **More** > **Start All Instances** para iniciar los servicios en el nodo.

Si el tiempo en el nodo de alarma es anterior al del servicio de chrony del nodo OMS activo, espere hasta que se deba la desviación de tiempo y ajuste el tiempo del nodo de alarma. Después de ajustar el tiempo, elija **More** > **Start All Instances** para iniciar los servicios en el nodo.

NOTA

Si no espera, puede ocurrir la pérdida de datos.

Paso 19 Después de 10 minutos, compruebe si la alarma está borrada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 38**.

Compruebe si el servicio NTP en el nodo se inicia correctamente.

Paso 20 En FusionInsight Manager, seleccione **O&M** > **Alarm** > **Alarms**. En la página que se muestra, haga clic en ⌄ en la fila que contiene la alarma y vea el nombre del host para el que se genera la alarma en **Location**.

Paso 21 Compruebe si el proceso ntpd se está ejecutando en el nodo mediante el siguiente método. Inicie sesión en el nodo de alarma como usuario **root** y ejecute el comando **ps -ef | grep ntpd | grep -v grep** para comprobar si la salida del comando contiene el proceso ntpd.

- En caso afirmativo, vaya a **Paso 24**.
- Si no, vaya a **Paso 22**.

Paso 22 Ejecute el comando **service ntp start** (o el comando **service ntpd start** en Red Hat Enterprise Linux) para iniciar el servicio NTP.

Paso 23 Después de 10 minutos, compruebe si la alarma está borrada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 24**.

Compruebe si el nodo puede sincronizar la hora correctamente con el servicio NTP en el nodo OMS activo.

Paso 24 Compruebe si el nodo puede sincronizar la hora con el servicio NTP en el nodo OMS activo basado en información adicional de la alarma.

- En caso afirmativo, vaya a **Paso 25**.
- Si no, vaya a **Paso 35**.

Paso 25 Compruebe si la sincronización con el servicio NTP en el nodo OMS activo es defectuosa.

Inicie sesión en el nodo de alarma como usuario **root** y ejecute el comando **ntpq -np**.

Si existe un asterisco (*) antes de la dirección IP del servicio NTP en el nodo OMS activo en la salida del comando, la sincronización está en estado normal. La salida del comando es la siguiente:

```
remote refid st t when poll reach delay offset jitter
==============================================================================
*10.10.10.162 .LOCL. 1 u 1 16 377 0.270 -1.562 0.014
```

Si no hay un asterisco (*) antes de la dirección IP del servicio NTP en el nodo OMS activo, como se muestra en la siguiente salida del comando, y el valor de **refid** es de **.INIT.**, la sincronización es anormal.

```
remote refid st t when poll reach delay offset jitter
==============================================================================
10.10.10.162 .INIT. 1 u 1 16 377 0.270 -1.562 0.014
```

- En caso afirmativo, vaya a **Paso 26**.
- Si no, vaya a **Paso 38**.

Paso 26 La falla de sincronización NTP es causado típicamente por el firewall del sistema. Si el firewall se puede deshabilitar, ejecute el comando **iptables -F** para deshabilitarlo. Si el firewall no se puede deshabilitar, ejecute el comando **iptables -L** para comprobar la política de configuración del firewall y asegurarse de que el puerto UDP 123 no esté deshabilitado. (Para obtener más información, consulte la política de configuración del firewall de cada sistema.)

Paso 27 Después de 10 minutos, compruebe si la alarma está borrada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 28**.

Paso 28 Inicie sesión en el nodo OMS activo como usuario **root** y ejecute el siguiente comando para ver el campo de índice de clave de autenticación **1M**:

En SUSE Linux, ejecute el comando **cat ${BIGDATA_HOME}/om-server/OMS/workspace/conf/ntp.keys**.

En Red Hat Enterprise Linux o EulerOS, ejecute el comando **cat ${BIGDATA_HOME}/om-server/OMS/workspace/conf/ntpkeys**.

Paso 29 Ejecute el siguiente comando para comprobar si el valor de clave es el mismo que el consultado en **Paso 28**:

En SUSE Linux, ejecute el comando **diff ${BIGDATA_HOME}/om-server/OMS/workspace/conf/ntp.keys /etc/ntp.keys**.

En Red Hat Enterprise Linux o EulerOS, ejecute el comando **diff ${BIGDATA_HOME}/om-server/OMS/workspace/conf/ntpkeys /etc/ntp/ntpkeys**.

NOTA

Si los valores de clave son los mismos, no se devuelve ningún resultado después de ejecutar el comando. Por ejemplo:

```
host01:~ # cat ${BIGDATA_HOME}/om-server/OMS/workspace/conf/ntp.keys
1 M sdYbq;o^CzEAWo<U=Tw5
host01:~ # diff ${BIGDATA_HOME}/om-server/OMS/workspace/conf/ntp.keys /etc/
ntp.keys
host01:~ #
```


- En caso afirmativo, vaya a **Paso 30**.
- Si no, vaya a **Paso 38**.

Paso 30 Ejecute el comando **cat ${BIGDATA_HOME}/om-server/om/packaged-distributables/ntpKeyFile** para comprobar si el valor de la clave es el mismo que el consultado en **Paso 28**. (Compare el valor de clave con el del campo de índice de clave de autenticación **1M** consultado en **Paso 28**.)

- En caso afirmativo, vaya a **Paso 31**.
- Si no, vaya a **Paso 33**.

Paso 31 Inicie sesión en el nodo defectuoso como usuario **root** y ejecute el comando **cat /etc/ntp.keys** en SUSE Linux (o el comando **cat /etc/ntp/ntpkeys** en Red Hat Enterprise Linux) para comprobar si el valor de la clave es el mismo que el valor consultado en el **Paso 30** (utiliza el valor de clave del campo índice de clave de autenticación **1M** para comparar).

- En caso afirmativo, vaya a **Paso 38**.
- Si no, vaya a **Paso 32**.

Paso 32 Ejecute el comando **su - omm** para cambiar al usuario **omm**, cambie el valor de clave del campo de índice de clave de autenticación **1M** en **${NODE_AGENT_HOME}/ntp.keys** (**${NODE_AGENT_HOME}/ntpkeys** en Red Hat Enterprise Linux) al valor clave de **ntpKeyFile** en **Paso 30**, y vaya a **Paso 34**.

Paso 33 Ejecute los siguientes comandos como usuario **root** o **omm** para cambiar el valor de clave NTP del nodo OMS activo (cambie **ntp.keys** a **ntpkeys** en Red Hat Enterprise Linux):

cd ${BIGDATA_HOME}/om-server/OMS/workspace/conf

sed -i "`cat ntp.keys | grep -n '1 M'|awk -F ':' '{print $1}'`d" ntp.keys

echo "1 M `cat ${BIGDATA_HOME}/om-server/om/packaged-distributables/ntpKeyFile`" >>ntp.keys

Compruebe si el valor de clave del campo índice de clave de autenticación **1M** de **ntp.keys** es el mismo que el de **ntpKeyFile**.

- En caso afirmativo, vaya a **Paso 34**.
- Si no, cambie el valor de clave del campo de índice de clave de autenticación **1M** en **ntp.keys** al valor de clave de **ntpKeyFile** y vaya a **Paso 34**.

Paso 34 Después de 5 minutos, ejecute el comando **service ntp restart** para reiniciar el servicio NTP en el nodo OMS activo. Después de 15 minutos, compruebe si la alarma está desactivada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 38**.

Compruebe si la desviación de tiempo entre el nodo y el servicio NTP en el nodo OMS activo es grande.

Paso 35 Compruebe si la desviación de tiempo es grande en la información adicional de la alarma.

- En caso afirmativo, vaya a **Paso 36**.
- Si no, vaya a **Paso 38**.

Paso 36 En la página de pestaña **Hosts**, seleccione el host para el que se genera la alarma y elija **More** > **Stop All Instances** para detener todos los servicios en el nodo.

Si el tiempo en el nodo de alarma es posterior al del servicio NTP del nodo OMS activo, ajuste el tiempo del nodo de alarma. Después de ajustar el tiempo, elija **More** > **Start All Instances** para iniciar los servicios en el nodo.

Si el tiempo en el nodo de alarma es anterior al del servicio NTP del nodo OMS activo, espere hasta que venza la desviación de tiempo y ajuste el tiempo del nodo de alarma. Después de ajustar el tiempo, elija **More** > **Start All Instances** para iniciar los servicios en el nodo.

NOTA

Si no espera, puede ocurrir la pérdida de datos.

Paso 37 Después de 10 minutos, compruebe si la alarma está borrada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 38**.

Recopilar información de fallas.

Paso 38 En FusionInsight Manager, seleccione **O&M**. En el panel de navegación de la izquierda, elija **Log** > **Download**.

Paso 39 En el área **Services**, seleccione **NodeAgent** y **OmmServer** y haga clic en **OK**. Expanda el cuadro de diálogo **Hosts** y seleccione el nodo de alarma y el nodo OMS activo.

Paso 40 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 30 minutos antes y después del tiempo de generación de alarmas respectivamente. A continuación, haga clic en **Download**.

Paso 41 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

Información relacionada

Ninguna

9.9 ALM-12014 Partición perdida

Descripción

El sistema comprueba el estado de la partición cada 60 segundos. Esta alarma se genera cuando el sistema detecta que se ha perdido una partición en la que se montan los directorios de servicio (porque el dispositivo se quita o se desconecta, o la partición se elimina). El sistema comprueba periódicamente el estado de la partición.

Esta alarma debe borrarse manualmente.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
12014	Importante	No

Parámetros

Nombre	Significado
Source	Especifica el clúster o sistema para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
DirName	Especifica el directorio para el que se genera la alarma.
PartitionName	Especifica la partición de dispositivo para la que se genera la alarma.

Impacto en el sistema

Los datos de servicio no se pueden escribir en la partición y el sistema de servicio se ejecuta de forma anormal.

Causas posibles

- Se quita el disco duro.
- El disco duro está fuera de línea o existe un sector defectuoso en el disco duro.

Procedimiento

Paso 1 En FusionInsight Manager, haga clic en **O&M > Alarm > Alarms** y haga clic en ⌄ en la fila donde se encuentra la alarma.

Paso 2 Obtenga **HostName**, **PartitionName** y **DirName** a partir de **Location**.

Paso 3 Compruebe si el disco de **PartitionName** de **HostName** está insertado en la ranura del servidor correcta.

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 5**.

Paso 4 Póngase en contacto con los ingenieros de hardware para quitar el disco defectuoso.

Paso 5 Inicie sesión en el nodo **HostName** donde se notifica una alarma y compruebe si hay una línea que contiene **DirName** en el archivo **/etc/fstab** como usuario **root**.

- En caso afirmativo, vaya a **Paso 6**.
- Si no, vaya a **Paso 7**.

Paso 6 Ejecute el comando **vi /etc/fstab** para editar el archivo y eliminar la línea que contiene **DirName**.

Paso 7 Póngase en contacto con los ingenieros de hardware para insertar un nuevo disco. Para obtener más información, consulte el documento del producto de hardware del modelo correspondiente. Si el disco defectuoso está en un grupo RAID, configure el grupo RAID. Para obtener más información, consulte los métodos de configuración de la tarjeta controladora de RAID relevante.

Paso 8 Espere de 20 a 30 minutos (el tamaño del disco determina el tiempo de espera) y ejecute el comando **mount** para comprobar si el disco se ha montado en el directorio **DirName**.

- En caso afirmativo, borre la alarma manualmente. No se requiere ninguna operación adicional.
- Si no, vaya a **Paso 9**.

Recopilar información de fallas.

Paso 9 En el FusionInsight Manager, elija **O&M** > **Log > Download**.

Paso 10 Seleccione el **OmmServer** en la lista desplegable Servicios y haga clic en **OK**.

Paso 11 Establezca Start Date para la recopilación de registros en 10 minutos antes de la hora de generación de alarmas y End Date en 10 minutos antes de la hora de generación de alarmas y haga clic en **Download**.

Paso 12 Póngase en contacto con el y envíe la información de registro recopilada.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema no borra automáticamente esta alarma, y es necesario borrar manualmente la alarma.

Información relacionada

Ninguna

9.10 ALM-12015 Sistema de archivos de partición de sólo lectura

Descripción

El sistema comprueba el estado de la partición cada 60 segundos. Esta alarma se genera cuando el sistema detecta que una partición en la que están montados los directorios de servicio entra en el modo de solo lectura (debido a un sector defectuoso o a un sistema de archivos defectuoso). El sistema comprueba periódicamente el estado de la partición.

Esta alarma se borra cuando el sistema detecta que la partición en la que se montan los directorios de servicio sale del modo de solo lectura (debido a que el sistema de archivos se restaura al modo de lectura/escritura, se quita el dispositivo o se formatea el dispositivo).

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
12015	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster o sistema para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
DirName	Especifica el directorio para el que se genera la alarma.
PartitionName	Especifica la partición de dispositivo para la que se genera la alarma.

Impacto en el sistema

Los datos de servicio no se pueden escribir en la partición y el sistema de servicio se ejecuta de forma anormal.

Causas posibles

El disco duro está defectuoso, por ejemplo, existe un sector defectuoso.

Procedimiento

Paso 1 En FusionInsight Manager, seleccione **O&M** > **Alarm > Alarms**, haga clic en ⌄ en la fila donde se encuentra la alarma.

Paso 2 Obtenga **HostName** y **PartitionName** de **Location**. **HostName** es el nodo donde se informa la alarma, y **PartitionName** es la partición del disco defectuoso.

Paso 3 Póngase en contacto con los ingenieros de hardware para comprobar si el disco está defectuoso. Si el disco está defectuoso, elimínelo del servidor.

Paso 4 Después de quitar el disco, se notifica la alarma **ALM-12014 Partición pérdida**. Maneje de la alarma. Para obtener más información, consulte **ALM-12014 Partición perdida**. Después de que la alarma **ALM-12014 Partición pérdida** se borra, la alarma **ALM-12015 Sistema de archivos de partición de solo lectura** se borra automáticamente.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.11 ALM-12016 El uso de la CPU supera el umbral

Descripción

El sistema comprueba el uso de la CPU cada 30 segundos y compara el uso real de la CPU con el umbral. El uso de la CPU tiene un umbral predeterminado. Esta alarma se genera cuando el uso de la CPU excede el umbral varias veces (configurable, 10 veces por defecto) consecutivamente.

La alarma se borra en los dos escenarios siguientes: El valor de **Trigger Count** es 1 y el uso de CPU es menor o igual que el umbral; el valor de **Trigger Count** es mayor que 1 y el uso de CPU es menor o igual que el 90% del umbral.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
12016	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster o sistema para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Nombre	Significado
Trigger Condition	Especifica el umbral que activa la alarma. Si el valor del indicador actual excede este umbral, se genera la alarma.

Impacto en el sistema

Los procesos de servicio responden lentamente o no están disponibles.

Causas posibles

- El umbral de alarma o los tiempos de suavizado de alarma son incorrectos.
- La configuración de la CPU no puede cumplir los requisitos de servicio. El uso de la CPU alcanza el límite superior.

Procedimiento

Compruebe si el umbral de alarma o alarma de Trigger Count son correctos.

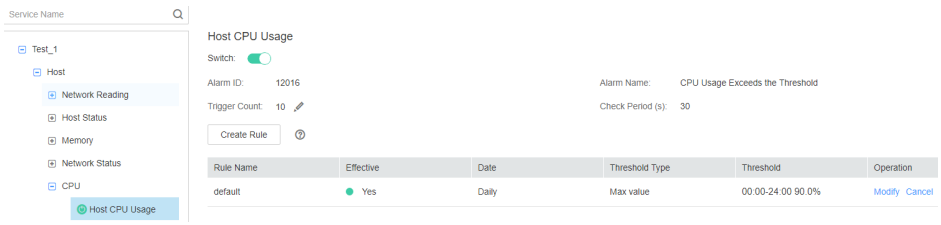
Paso 1 Cambie el umbral de alarma y **Trigger Count** de alarma según el uso de la CPU.

En FusionInsight Manager, elija **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster* > **Host** > **CPU** > **Host CPU Usage** y cambie los tiempos de suavizado de alarma basados en en el uso de la CPU, como se muestra en **Figura 9-1**.

NOTA

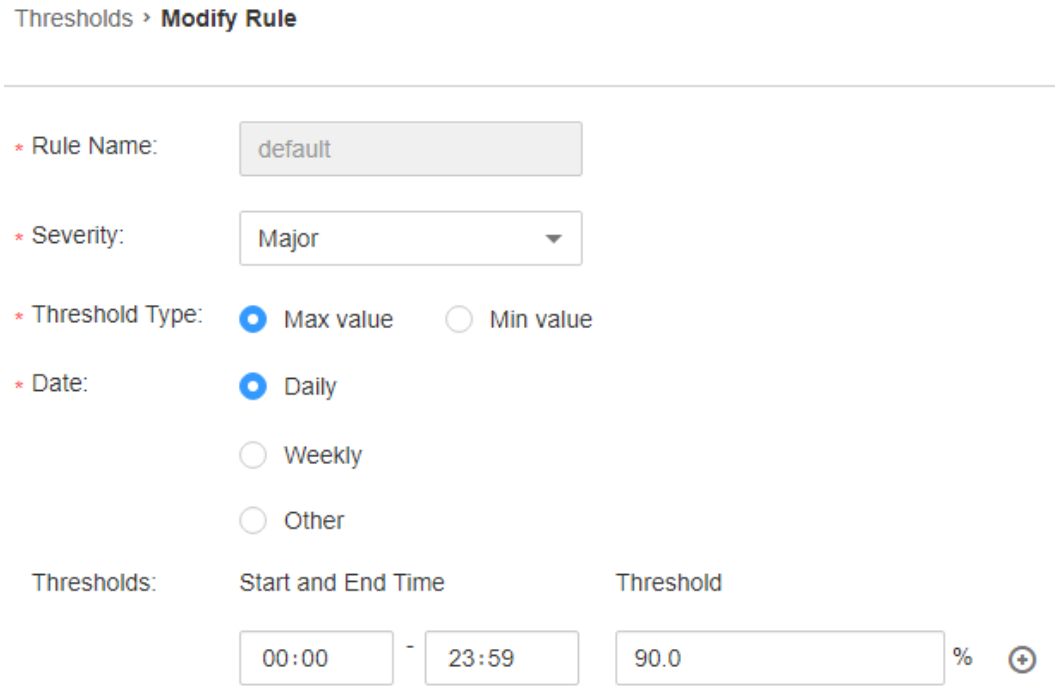
Esta opción define la fase de comprobación de alarma. **Trigger Count** indica el umbral de comprobación de alarma. Se genera una alarma cuando el número de veces de comprobación excede el umbral.

Figura 9-1 Ajuste de los tiempos de suavizado de alarma



En la página **Host CPU Usage** y haga clic en **Modify** en la columna **Operation** para cambiar el umbral de alarma, como se muestra en **Figura 9-2**.

Figura 9-2 Establecer un umbral de alarma



Paso 2 Después de 2 minutos, compruebe si la alarma está borrada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 3**.

Comprobar si el uso de la CPU alcanza el límite superior.

Paso 3 En la lista de alarmas del FusionInsight Manager, haga clic en ⌄ en la fila donde se encuentra la alarma para ver la dirección del host de alarma en los detalles de la alarma.

Paso 4 En la página **Hosts**, haga clic en el nodo en el que se reporta la alarma.

Paso 5 Vea el uso de la CPU durante 5 minutos. Si el uso de CPU excede el umbral varias veces, póngase en contacto con el administrador del sistema para agregar más CPU.

Paso 6 Verifique si la alarma se ha borrado.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 7**.

Recopilar información de fallas.

Paso 7 En el FusionInsight Manager del clúster activo, elija **O&M** > **Log > Download**.

Paso 8 Seleccione **OmmServer** en **Service** y haga clic en **OK**.

Paso 9 Establezca **Start Date** para la recopilación de registros a 10 minutos antes de la hora de generación de alarmas y **End Date** a 10 minutos después de la hora de generación de alarmas de **Time Range** y haga clic en **Download**.

Paso 10 Póngase en contacto con el y envíe la información de registro recopilada.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.12 ALM-12017 Capacidad de disco insuficiente

Descripción

El sistema comprueba el uso del disco host del sistema cada 30 segundos y compara el uso real del disco con el umbral. El uso del disco tiene un umbral predeterminado, esta alarma se genera cuando el uso del disco host excede el umbral especificado.

Cuando el **Trigger Count** es 1, esta alarma se borra cuando el uso de una partición de disco host es menor o igual al umbral. Cuando el **Trigger Count** es mayor que 1, esta alarma se borra cuando el uso de una partición de disco host es menor o igual al 90% del umbral.

Atributo

ID de alarma	Gravedad de la alarma	Borrado automático
12017	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster o sistema para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
PartitionName	Especifica la partición de dispositivo para la que se genera la alarma.
Trigger Condition	Especifica el umbral que activa la alarma. Si el valor del indicador actual excede este umbral, se genera la alarma.

Impacto en el sistema

Los procesos de servicio no están disponibles.

Causas posibles

- El umbral de alarma es incorrecto.
- La configuración de disco del servidor no puede cumplir los requisitos de servicio.

Procedimiento

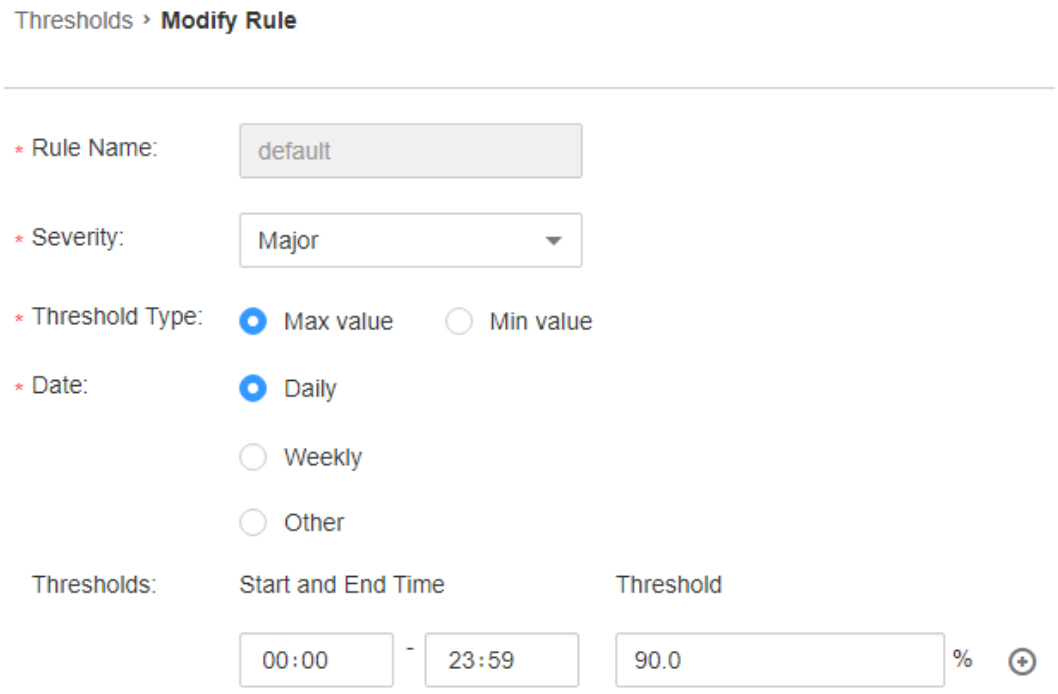
Comprobar si el umbral de alarma es adecuado.

Paso 1 Inicie sesión en FusionInsight Manager, elija **O&M** > **Alarm > Thresholds >** *Name of the desired cluster* > **Host** > **Disk** > **Disk Usage** y compruebe si el umbral (configurable, 90% por defecto) es apropiado.

- En caso afirmativo, vaya a **Paso 2**.
- Si no, vaya a **Paso 4**.

Paso 2 Elija **O&M** > **Alarm > Thresholds >** *Name of the desired cluster* > **Host** > **Disk** > **Disk Usage** y haga clic en **Modify** en la columna **Operation** para cambiar el umbral de alarma según los requisitos del sitio. Como se muestra en **Figura 9-3**:

Figura 9-3 Establecer un umbral de alarma



Paso 3 Después de 2 minutos, compruebe si la alarma está borrada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 4**.

Comprobar si el uso del disco alcanza el límite superior.

Paso 4 En la lista de alarmas del Administrador de FusionInsight, haga clic en ⌄ en la fila donde se encuentra la alarma para ver el nombre del host de la alarma y la información de la partición del disco en los detalles de la alarma.

Paso 5 Inicie sesión en el nodo donde se genera la alarma como **root**.

Paso 6 Ejecute el comando **df -lmPT | awk '$2!= "iso9660"' | grep '^/dev/' | awk '{"readlink -m "$1 | getline real }{$1=real; print $0}' | sort -u -k 1,1** para comprobar el uso de la partición del disco del sistema. Compruebe si el disco está montado en los siguientes directorios basándose en el nombre de partición de disco obtenido en **Paso 4**: /, **/opt**, **/tmp**, **/var**, **/var/log** y **/srv/BigData**(puede personalizarse).

- En caso afirmativo, el disco es un disco del sistema. Entonces vaya a **Paso 10**.
- Si no, el disco no es un disco del sistema. Entonces vaya a **Paso 7**.

Paso 7 Ejecute el comando **df -lmPT | awk '$2!= "iso9660"' | grep '^/dev/' | awk '{"readlink -m "$1 | getline real }{$1=real; print $0}' | sort -u -k 1,1** para comprobar el uso de la partición del disco del sistema. Determine el rol del disco basado en el nombre de la partición de disco obtenido en **Paso 4**.

Paso 8 Compruebe el servicio de disco.

En , compruebe si el servicio de disco es HDFS, Yarn, Kafka, Supervisor.

- En caso afirmativo, ajuste la capacidad. Entonces vaya a **Paso 9**.
- Si no, vaya a **Paso 12**.

Paso 9 Después de 2 minutos, compruebe si la alarma está borrada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 12**.

Paso 10 Ejecute el comando **find / -xdev -size +500M -execls -l {} \;** para comprobar si existe un archivo de más de 500 MB en el nodo y en el disco.

- En caso afirmativo, vaya a **Paso 11**.
- Si no, vaya a **Paso 12**.

Paso 11 Maneje el archivo grande y comprobar si la alarma se borra 2 minutos más tarde.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 12**.

Paso 12 Póngase en contacto con el administrador del sistema para ampliar la capacidad del disco.

Paso 13 Después de 2 minutos, compruebe si la alarma está borrada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 14**.

Recopilar información de fallas.

Paso 14 En FusionInsight Manager, elija **O&M** > **Log > Download**.

Paso 15 Seleccione **OMS** en el **Service** y haga clic en **OK**.

Paso 16 Haga clic en  en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 17 Póngase en contacto con el y envíe la información de registro recopilada.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.13 ALM-12018 El uso de memoria supera el umbral

Descripción

El sistema comprueba el uso de memoria del sistema cada 30 segundos y compara el uso real de memoria con el umbral. El uso de memoria tiene un umbral predeterminado, esta alarma se genera cuando el valor del uso de memoria excede el umbral.

Cuando el **Trigger Count** es 1, esta alarma se borra cuando el uso de la memoria del host es menor o igual al umbral. Cuando el **Trigger Count** es mayor que 1, esta alarma se borra cuando el uso de memoria central es menor o igual al 90% del umbral.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
12018	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster o sistema para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger Condition	Especifica el umbral que activa la alarma. Si el valor del indicador actual excede este umbral, se genera la alarma.

Impacto en el sistema

Los procesos de servicio responden lentamente o no están disponibles.

Causas posibles

- La configuración de la memoria no puede cumplir con los requisitos de servicio. El uso de memoria alcanza el límite superior.
- El SUSE 12.X OS tiene un comando **free** anterior. El uso de memoria calculado no puede reflejar el uso de memoria del mundo real.

Procedimiento

Realice las siguientes operaciones si se utiliza SUSE 12.X.

Paso 1 Inicie sesión en cualquier nodo del clúster como usuario **root** y ejecute el comando **cat /etc/*-release** para comprobar si el sistema operativo es SUSE 12.X como usuario **root**.

- En caso afirmativo, vaya a **Paso 2**.
- Si no, vaya a **Paso 4**.

Paso 2 Ejecute el comando **cat /proc/meminfo | grep Mem** para comprobar el uso de memoria real del sistema operativo.

```
MemTotal: 263576192 kB
MemFree: 198283116 kB
MemAvailable: 227641452 kB
```

Paso 3 Calcule el uso de memoria del mundo real: Uso de memoria = 1 - (Memoria disponible/Memoria total)

- Si el uso de la memoria es inferior al 90%, deshabilite manualmente la transferencia de indicadores de monitoreo a alarmas.
- Si el uso de memoria es superior al 90%, vaya a **Paso 4**.

Expandir el sistema.

Paso 4 En la lista de alarmas del FusionInsight Manager, haga clic en ⌄ en la fila donde se encuentra la alarma para ver la dirección del host de alarma en los detalles de la alarma.

Paso 5 Inicie sesión en el host donde se genera la alarma como usuario **root**.

Paso 6 Si el uso de memoria excede el umbral, realice la ampliación de la capacidad de memoria.

Paso 7 Ejecute el comando **free -m | grep Mem\: | awk '{printf("%s,", $3 * 100 / $2)}'** para comprobar el uso de la memoria del sistema.

Paso 8 Espere 5 minutos, compruebe si la alarma está borrada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 9**.

Recopilar información de fallas.

Paso 9 En el FusionInsight Manager del clúster activo, elija **O&M** > **Log > Download**.

Paso 10 Seleccione **OmmServer** en el **Service** y haga clic en **OK**.

Paso 11 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 12 Póngase en contacto con el y envíe la información de registro recopilada.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.14 ALM-12027 El uso de PID de host supera el umbral

Descripción

El sistema comprueba el uso del PID cada 30 segundos y compara el uso real del PID con el umbral de uso predeterminado del PID. Esta alarma se genera cuando el sistema detecta que el uso de PID excede el umbral.

Cuando el **Trigger Count** es 1, esta alarma se borra cuando el uso de PID es menor o igual que el umbral. Cuando el **Trigger Count** es mayor que 1, esta alarma se borra cuando el uso de PID es menor o igual al 90% del umbral.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
12027	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster o sistema para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Nombre	Significado
Trigger Condition	Especifica el umbral que activa la alarma. Si el valor del indicador actual excede este umbral, se genera la alarma.

Impacto en el sistema

No hay ningún PID disponible para los nuevos procesos y los procesos de servicio no están disponibles.

Causas posibles

Se están ejecutando demasiados procesos en el nodo. Necesita aumentar el valor de **pid_max**.

Procedimiento

Aumentar el valor de pid_max.

Paso 1 En la lista de alarmas del FusionInsight Manager, haga clic en ⌄ en la fila donde se encuentra la alarma para ver la dirección del host de alarma en los detalles de la alarma.

Paso 2 Inicie sesión en el host donde se genera la alarma como usuario **root**.

Paso 3 Ejecute el comando **cat /proc/sys/kernel/pid_max** para comprobar el valor de **pid_max**.

Paso 4 Si el uso de PID excede el umbral, ejecute el comando **echo** *new value* **> /proc/sys/kernel/pid_max** para ampliar el valor de **pid_max**.

Ejemplo: **echo 65536 > /proc/sys/kernel/pid_max**

NOTA

El valor máximo de **pid_max** es el siguiente:

- On 32-bit systems: 32768
- On 64-bit systems: 4194304 (2^22)

Paso 5 Espere 5 minutos y compruebe si la alarma está desactivada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 6**.

Recopilar información de fallas.

Paso 6 En la página principal del FusionInsight Manager del clúster activo, elija **O&M** > **Log** > **Download**.

Paso 7 Seleccione todos los servicios en el **Service** y haga clic en **OK**.

Paso 8 Haga clic en ✎ en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 30 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 9 Póngase en contacto con el y envíe la información de registro recopilada.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.15 ALM-12028 Número de procesos en el Estado D en un host supera el umbral

Descripción

El sistema comprueba el número de procesos en el estado D del usuario **omm** en el host cada 30 segundos y compara el número real con el umbral. El número de procesos en el estado D en el host tiene un rango de umbral predeterminado. Esta alarma se genera cuando el número de procesos excede el umbral.

Esta alarma se borra cuando el **Trigger Count** es **1** y el número total de procesos en el estado D del usuario **omm** en el host no excede el umbral. Esta alarma se borra cuando el **Trigger Count** es mayor que 1 y el número total de procesos en el estado D del usuario **omm** en el host es menor o igual al 90% del umbral.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
12028	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster o sistema para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger Condition	Especifica el umbral para activar la alarma.

Impacto en el sistema

Se utilizan recursos excesivos del sistema y los procesos de servicio responden lentamente.

Causas posibles

El host responde lentamente a las solicitudes de E/S (E/S de disco y E/S de red) y algunos procesos están en estado D y estado Z.

Procedimiento

Comprobar el proceso en el estado D.

Paso 1 En la lista de alarmas del FusionInsight Manager, busque la fila que contiene la alarma y haga clic en para ver la dirección IP del host para el que se genera la alarma.

Paso 2 Inicie sesión en el host para el que se genera la alarma como usuario **root**. () A continuación, ejecute el comando **su - omm** para cambiar a usuario **omm**.

Paso 3 Ejecute el siguiente comando como usuario **omm** para ver el PID del proceso que está en el estado D:

ps -elf | grep -v "\[thread_checkio\]" | awk 'NR!=1 {print $2, $3, $4}' | grep omm | awk -F' ' '{print $1, $3}' | grep -E "Z|D" | awk '{print $2}'

Paso 4 Compruebe si la salida del comando está vacía.

- En caso afirmativo, el proceso de servicio se está ejecutando correctamente. Entonces vaya a **Paso 6**.
- Si no, vaya a **Paso 5**.

Paso 5 Cambie a usuario **root** y ejecute el comando **reboot** para reiniciar el host para el que se genera la alarma. (Reiniciar un host es arriesgado. Asegúrese de que el proceso de servicio es normal después del reinicio.)

Paso 6 Compruebe si la alarma se borra 5 minutos más tarde.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 7**.

Recopilar información de fallas.

Paso 7 En FusionInsight Manager, seleccione **O&M**. En el panel de navegación de la izquierda, elija **Log** > **Download**.

Paso 8 Seleccione **OMS** para **Service** y haga clic en **OK**.

Paso 9 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 1 hora antes y después del tiempo de generación de alarma, respectivamente. A continuación, haga clic en **Download**.

Paso 10 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

Información relacionada

Ninguna

9.16 ALM-12033 Falla de disco lento

Descripción

- En el caso de HDDs, la alarma se activa cuando se cumple alguna de las siguientes condiciones:
  - El sistema ejecuta el comando **iostat** cada 3 segundos y detecta que el valor **svctm** supera los 1000 ms durante 7 períodos consecutivos en 30 segundos.
  - El sistema ejecuta el comando **iostat** cada 3 segundos y detecta que más del 50% de las E/S tardan más de 150 ms dentro de 300s.
- Para las SSD, la alarma se activa cuando se cumple alguna de las siguientes condiciones:
  - El sistema ejecuta el comando **iostat** cada 3 segundos y detecta que el valor **svctm** supera los 1000 ms durante 10 períodos consecutivos en 30 segundos.
  - El sistema ejecuta el comando **iostat** cada 3 segundos y detecta que más del 60% de las E/S tardan más de 20 ms en 300 segundos.

Esta alarma se borra automáticamente cuando las condiciones anteriores no se han cumplido durante 15 minutos.

NOTA

El valor **svctm** se puede obtener de la siguiente manera:

- MRS 3.1.0:

  Ejecute el comando **iostat -x -t** en el sistema operativo.
- Versiones posteriores a MRS 3.1.0:

svctm = (tot_ticks_new - tot_ticks_old)/(rd_ios_new + wr_ios_new - rd_ios_old - wr_ios_old)

Si **rd_ios_new + wr_ios_new - rd_ios_old - wr_ios_old** es el nombre de **0**, entonces **svctm** es el nombre de **0**.

Los parámetros se pueden obtener de la siguiente manera:

El sistema ejecuta el comando **cat /proc/diskstats** cada 3 segundos para recopilar datos. Por ejemplo:

En estos dos comandos:

En los datos recopilados por primera vez, el número en la cuarta columna es el valor **rd_ios_old**, el número en la octava columna es el valor **wr_ios_old** y el número en la decimotercera columna es el valor **tot_ticks_old**.

En los datos recopilados por segunda vez, el número en la cuarta columna es el valor **rd_ios_new**, el número en la octava columna es el valor **wr_ios_new** y el número en la decimotercera columna es el valor **tot_ticks_new**.

En este caso, el valor de **svctm** es el siguiente:

(19571460 - 19569526)/(1101553 + 28747977 - 1101553 - 28744856) = 0.6197

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
12033	Leves	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster o sistema para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
DiskName	Especifica el disco para el que se genera la alarma.

Impacto en el sistema

El rendimiento del servicio se deteriora, las capacidades de procesamiento de servicios se vuelven deficientes y es posible que los servicios no estén disponibles.

Causas posibles

El disco está envejecido o tiene sectores defectuosos.

Procedimiento

Comprobar el estado de disco.

Paso 1 En FusionInsight Manager, seleccione **O&M**. En el panel de navegación de la izquierda, elija **Alarm** > **Alarms**.

Paso 2 Vea la información detallada sobre la alarma. Compruebe los valores de **HostName** y **DiskName** en la información de ubicación para obtener la información sobre el disco defectuoso para el que se genera la alarma.

Paso 3 Compruebe si el nodo para el que se genera la alarma se encuentra en un entorno de virtualización.

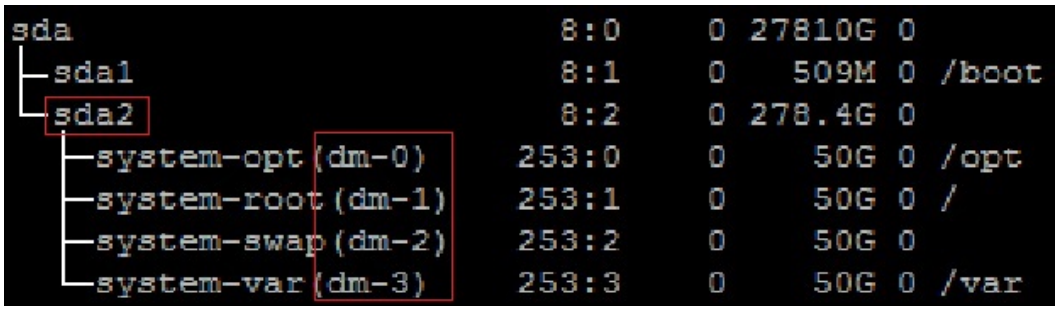
- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 7**.

Paso 4 Compruebe si el rendimiento de almacenamiento proporcionado por el entorno de virtualización cumple con los requisitos de hardware. A continuación, vaya a **Paso 5**.

Paso 5 Inicie sesión en el nodo de alarma como usuario **root**, ejecute el comando **df -h** y compruebe si la salida del comando contiene el valor del campo **DiskName**.

- En caso afirmativo, vaya a **Paso 7**.
- Si no, vaya a **Paso 6**.

Paso 6 Ejecute el comando **lsblk** para comprobar si se ha creado la asignación entre el valor de **DiskName** y el disco.



- En caso afirmativo, vaya a **Paso 7**. .
- Si no, vaya a **Paso 22**.

Paso 7 Inicie sesión en el nodo de alarma como usuario **root**, ejecute el comando **lsscsi | grep "/dev/sd[x]"** para ver la información del disco y compruebe si se ha configurado RAID.

NOTA

En el comando **/dev/sd[x]** indica el nombre del disco obtenido en el archivo **Paso 2**.

Ejemplo:

lsscsi | grep "/dev/sda"

En la salida del comando, si se muestra **ATA**, **SATA** o **SAS** en la tercera línea, el disco no se ha organizado en un grupo RAID. Si se muestra otra información, se ha configurado RAID.

- En caso afirmativo, vaya a **Paso 12**.
- Si no, vaya a **Paso 8**.

Paso 8 Ejecute el comando **smartctl -i /dev/sd[x]** para comprobar si el hardware admite la herramienta SMART.

Ejemplo:

smartctl -i /dev/sda

En la salida del comando, si se muestra "SMART support is: Enabled", el hardware soporta SMART. Si "Device does not support SMART" o se muestra otra información, el hardware no admite SMART.

- En caso afirmativo, vaya a **Paso 9**.
- Si no, vaya a **Paso 17**.

Paso 9 Ejecute el comando **smartctl -H --all /dev/sd[x]** para comprobar la información básica de SMART y determinar si el disco funciona correctamente.

Ejemplo:

smartctl -H --all /dev/sda

Compruebe el valor de **SMART overall-health self-assessment test result** en la salida del comando. Si el valor es de **FAILED**, el disco está defectuoso y necesita ser reemplazado. Si el valor es **PASSED**, compruebe el valor de **Reallocated_Sector_Ct** o **Elements in grown defect list**. Si el valor es mayor que 100, el disco está defectuoso y necesita ser reemplazado.

- En caso afirmativo, vaya a **Paso 10**.
- Si no, vaya a **Paso 18**.

Paso 10 Ejecute el comando **smartctl -l error -H /dev/sd[x]** para comprobar Glist del disco y determinar si el disco es normal.

Ejemplo:

smartctl -l error -H /dev/sda

Compruebe la columna **Command/Feature_name** en la salida del comando. Si se muestra **READ SECTOR(S)** o **WRITE SECTOR(S)**, el disco tiene sectores defectuosos. Si se producen otros errores, la placa de circuito de disco está defectuosa. Ambos errores indican que el disco es anormal y necesita ser reemplazado.

Si se muestra "No Errors Logged", no existe ningún registro de errores. Puede activar la autocomprobación SMART del disco.

- En caso afirmativo, vaya a **Paso 11**.
- Si no, vaya a **Paso 18**.

Paso 11 Ejecute el comando **smartctl -t long /dev/sd[x]** para activar la autocomprobación SMART del disco. Después de ejecutar el comando, se muestra el tiempo en el que se va a completar la autocomprobación. Una vez completada la autocomprobación, repita **Paso 9** y **Paso 10** para comprobar si el disco funciona correctamente.

Ejemplo:

smartctl -t long /dev/sda

- En caso afirmativo, vaya a **Paso 17**.
- Si no, vaya a **Paso 18**.

Paso 12 Ejecute el comando **smartctl -d [sat|scsi]+megaraid,[DID] -H --all /dev/sd[x]** para comprobar si el hardware admite SMART.

NOTA

- En el comando **[sat|scsi]** indica el tipo de disco. Ambos tipos necesitan ser utilizados.
- **[DID]** indica la información de intervalo. Las ranuras 0 a 15 necesitan ser utilizadas.

Por ejemplo, ejecute los siguientes comandos en secuencia:

smartctl -d sat+megaraid,0 -H --all /dev/sda

smartctl -d sat+megaraid,1 -H --all /dev/sda

smartctl -d sat+megaraid,2 -H --all /dev/sda

...

Pruebe las combinaciones de comandos de diferentes tipos de disco e información de ranura. Si se muestra "SMART support is: Enabled" en la salida del comando, el disco soporta SMART. Registre los parámetros del tipo de disco y la información de ranura cuando se ejecuta correctamente un comando. Si "SMART support is: Enabled" no se muestra en la salida del comando, el disco no soporta SMART.

- En caso afirmativo, vaya a **Paso 13**.
- Si no, vaya a **Paso 16**.

Paso 13 Ejecute el comando **smartctl -d [sat|scsi]+megaraid,[DID] -H --all /dev/sd[x]** grabado en **Paso 12** para comprobar la información básica de SMART y determinar si el disco es normal.

Ejemplo:

smartctl -d sat+megaraid,2 -H --all /dev/sda

Compruebe el valor de **SMART overall-health self-assessment test result** en la salida del comando. Si el valor es de **FAILED**, el disco está defectuoso y necesita ser reemplazado. Si el valor es **PASSED**, compruebe el valor de **Reallocated_Sector_Ct** o **Elements in grown defect list**. Si el valor es mayor que 100, el disco está defectuoso y necesita ser reemplazado.

- En caso afirmativo, vaya a **Paso 14**.
- Si no, vaya a **Paso 18**.

Paso 14 Ejecute el comando **smartctl -d [sat|scsi]+megaraid,[DID] -l error -H /dev/sd[x]** para comprobar la lista G del disco y determinar si el disco duro funciona correctamente.

Ejemplo:

smartctl -d sat+megaraid,2 -l error -H /dev/sda

Compruebe la columna **Command/Feature_name** en la salida del comando. Si se muestra **READ SECTOR(S)** o **WRITE SECTOR(S)**, el disco tiene sectores defectuosos. Si se producen otros errores, la placa de circuito de disco está defectuosa. Ambos errores indican que el disco es anormal y necesita ser reemplazado.

Si se muestra "No Errors Logged", no existe ningún registro de errores. Puede activar la autocomprobación SMART del disco.

- En caso afirmativo, vaya a **Paso 15**.
- Si no, vaya a **Paso 18**.

Paso 15 Ejecute el comando **smartctl -d [sat|scsi]+megaraid,[DID] -t long /dev/sd[x]** para activar la autocomprobación SMART del disco. Después de ejecutar el comando, se muestra el tiempo en el que se va a completar la autocomprobación. Una vez completada la autocomprobación, repita **Paso 13** y **Paso 14** para comprobar si el disco funciona correctamente.

Ejemplo:

smartctl -d sat+megaraid,2 -t long /dev/sda

- En caso afirmativo, vaya a **Paso 17**.
- Si no, vaya a **Paso 18**.

Paso 16 Si la tarjeta controladora RAID configurada no es compatible con SMART, el disco no es compatible con SMART. En este caso, utilice la herramienta de comprobación proporcionada por el proveedor de tarjeta controladora RAID correspondiente para rectificar la falla. A continuación, vaya a **Paso 17**.

Por ejemplo, LSI es una herramienta de MegaCLI.

Paso 17 En FusionInsight Manager, seleccione **O&M** > **Alarm** > **Alarms**, haga clic en **Clear** en la columna **Operation** de la alarma y compruebe si la alarma se notifica de nuevo en el mismo disco.

Si la alarma se notifica tres veces, cambie el disco.

- En caso afirmativo, vaya a **Paso 18**.
- En caso negativo, no se requiere ninguna otra acción.

Reemplazar el disco.

Paso 18 En FusionInsight Manager, seleccione **O&M**. En el panel de navegación de la izquierda, elija **Alarm** > **Alarms**.

Paso 19 Vea la información detallada sobre la alarma. Compruebe los valores de **HostName** y **DiskName** en la información de ubicación para obtener la información sobre el disco defectuoso para el que se informa la alarma.

Paso 20 Reemplace el disco.

Paso 21 Verifique si la alarma se ha borrado.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 22**.

Recopilar información de fallas.

Paso 22 En FusionInsight Manager, seleccione **O&M**. En el panel de navegación de la izquierda, elija **Log** > **Download**.

Paso 23 Seleccione **OMS** para **Service** y haga clic en **OK**.

Paso 24 Haga clic en  en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 25 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

Información relacionada

Ninguna

9.17 ALM-12034 Error de copia de respaldo periódica

Descripción

El sistema ejecuta la tarea de copia de respaldo periódica cada 60 minutos. Esta alarma se genera cuando no se puede ejecutar una tarea de copia de respaldo periódica. Esta alarma se borra cuando la siguiente tarea de copia de respaldo se ejecuta correctamente.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
12034	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster o sistema para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
TaskName	Especifica la tarea.

Impacto en el sistema

No hay paquetes de copia de respaldo disponibles durante mucho tiempo, por lo que el sistema no se puede restaurar en caso de excepciones.

Causas posibles

La causa de la alarma depende de los detalles de la tarea. Manejar la alarma de acuerdo con los registros y detalles de alarma.

Procedimiento

Comprobar si el espacio en disco es suficiente.

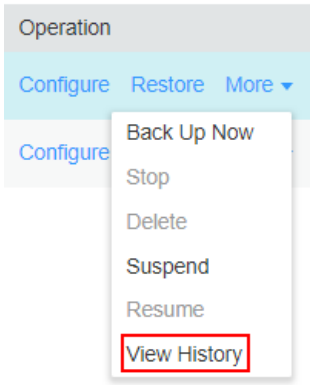
Paso 1 En el portal de FusionInsight Manager, haga clic en **O&M > Alarm > Alarms**.

Paso 2 En la lista de alarmas, haga clic en ⌄ en la fila donde se encuentra la alarma y obtenga **TaskName** de **Location**.

Paso 3 Elija **O&M** > **Backup and Restoration > Backup Management**.

Paso 4 Busque la tarea de copia de respaldo basada en **TaskName** y haga clic en **More** en la columna **Operation**. En el cuadro de diálogo mostrado, haga clic en **View History** y vea los detalles de la tarea.

Figura 9-4 Consultar historial



Paso 5 En el cuadro de diálogo mostrado y haga clic en para comprobar si se muestra el siguiente mensaje: Failed to backup xx due to insufficient disk space, move the data in the xx directory to other directories.

- En caso afirmativo, vaya a **Paso 6**.
- Si no, vaya a **Paso 13**.

Paso 6 Elija **Backup Path** > **View** y obtenga la **Backup Path**.

Paso 7 Inicie sesión en el nodo como usuario **root** y ejecute el siguiente comando para comprobar los detalles de montaje del nodo:

df -h

Paso 8 Compruebe si el espacio disponible del nodo en el que está montado la ruta de copia de respaldo es inferior a 20 GB.

- En caso afirmativo, vaya a **9**.
- Si no, vaya a **Paso 13**.

Paso 9 Compruebe si hay muchos paquetes de copia de respaldo en el directorio de copia de respaldo.

- En caso afirmativo, vaya a **Paso 10**.
- Si no, vaya a **Paso 13**.

Paso 10 Habilite el espacio disponible del nodo en el que está montado el directorio de copia de respaldo para que sea superior a 20 GB moviendo los paquetes de copia de respaldo fuera del directorio de copia de respaldo o elimine los paquetes de copia de respaldo.

Paso 11 Una vez resuelto el problema, vuelva a realizar la tarea de copia de respaldo y compruebe si la ejecución de la tarea de copia de respaldo se realiza correctamente.

- En caso afirmativo, vaya a **Paso 12**.
- Si no, vaya a **Paso 13**.

Paso 12 Después de 2 minutos, compruebe si la alarma está borrada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 13**.

Recopilar información de fallas.

Paso 13 En el portal del FusionInsight Manager, elija **O&M** > **Log > Download**.

Paso 14 Seleccione **Controller** en el **Service** y haga clic en **OK**.

Paso 15 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 16 Póngase en contacto con el y envíe la información de registro recopilada.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.18 ALM-12035 Estado de datos desconocido después de un error de tarea de recuperación

Descripción

Después de que la tarea de recuperación falla, el sistema se revierte automáticamente cada 60 minutos. Si la reversión falla, los datos pueden perderse. Si esto ocurre, se informa de una alarma. Esta alarma se borra cuando se ejecuta correctamente la siguiente tarea de recuperación.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
12035	Crítica	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster o sistema para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
TaskName	Especifica la tarea.

Impacto en el sistema

Una vez que la tarea de recuperación falla, el sistema se revierte automáticamente. Si la reversión falla, los datos pueden perderse o el estado de los datos puede ser desconocido, lo que puede afectar a los servicios.

Causas posibles

La causa de la alarma depende de los detalles de la tarea. Manejar la alarma de acuerdo con los registros y detalles de alarma.

Procedimiento

Recopilar información de fallas.

Paso 1 En el FusionInsight Manager, elija **Cluster >** *Name of the desired cluster* **> Services** y compruebe si el estado de ejecución del componente cumple los requisitos. (El OMS y DBService deben estar en el estado normal y los demás componentes deben estar detenidos.)

- En caso afirmativo, vaya a **Paso 9**.
- Si no, vaya a **Paso 2**.

Paso 2 Restaure el estado del componente según sea necesario e inicie de nuevo la tarea de recuperación.

Paso 3 Inicie sesión en el portal del FusionInsight Manager y haga clic en **O&M > Alarm > Alarms**.

Paso 4 En la lista de alarmas, haga clic en en la fila donde se encuentra la alarma para obtener **TaskName** de **Location**.

Paso 5 Elija **O&M** > **Backup and Restoration > Restoration Management**.

Paso 6 Busque la tarea de restauración por **Task Name** y vea los detalles de la tarea.

Paso 7 Vuelva a realizar la tarea de recuperación y compruebe si la ejecución de la tarea de recuperación se realiza correctamente.

- En caso afirmativo, vaya a **8**.
- Si no, vaya a **9**.

Paso 8 Después de 2 minutos, compruebe si la alarma está borrada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **9**.

Recopilar información de fallas.

Paso 9 En el portal del FusionInsight Manager, elija **O&M** > **Log > Download**.

Paso 10 Seleccione **Controller** en el **Service** y haga clic en **OK**.

Paso 11 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 12 Póngase en contacto con el y envíe la información de registro recopilada.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.19 ALM-12037 Servidor NTP anormal

Descripción

El sistema comprueba el estado del servidor NTP cada 60 segundos. Esta alarma se genera cuando el sistema detecta que el servidor NTP es anormal durante 10 veces consecutivas.

Esta alarma se borra cuando el servidor NTP se recupera.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
12037	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster o sistema para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica la dirección IP del servidor NTP para el que se genera la alarma.

Impacto en el sistema

El servidor NTP configurado en el nodo OMS activo es anormal. En este caso, el nodo OMS activo no puede sincronizar el tiempo con el servidor NTP y se puede generar un desplazamiento de tiempo en el clúster.

Causas posibles

- La red del servidor NTP es anormal.
- La autenticación del servidor NTP falla.
- No se puede obtener la hora del servidor NTP.
- El tiempo obtenido del servidor NTP no se actualiza continuamente.

Procedimiento

Comprobar la red de servidor NTP.

Paso 1 En el portal del FusionInsight Manager, haga clic en **O&M > Alarm > Alarms** y haga clic en ⌄ en la fila donde se encuentra la alarma.

Paso 2 Vea la información adicional de la alarma para comprobar si el servidor NTP no se puede hacer ping.

- En caso afirmativo, vaya a **Paso 3**.
- Si no, vaya a **Paso 4**.

Paso 3 Póngase en contacto con el administrador de la red para comprobar la configuración de la red y asegurarse de que la red entre el servidor NTP y el nodo OMS activo es normal. Luego, verifique si la alarma se rectificó.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 4**.

Comprobar si la autenticación de servidor NTP falla.

Paso 4 Inicie sesión en el nodo OMS activo como usuario **root**.

Paso 5 Ejecute el siguiente comando para comprobar el estado de los recursos en los nodos activo y en espera:

su - omm

sh ${BIGDATA_HOME}/om-server/om/sbin/status-oms.sh

- Si aparece "chrony" en la columna **ResName** de la salida del comando, vaya a **Paso 6**.
- Si aparece "ntp" en la columna **ResName**, vaya a **Paso 7**.

NOTA

Si tanto "chrony" como "ntp" se muestran en la columna **ResName** de la salida del comando, el modo de servicio NTP se está conmutando. Espera 10 minutos y vuelve a realizar **Paso 5**. Si tanto "chrony" como "ntp" todavía existen en la columna **ResName**, póngase en contacto con.

Paso 6 Ejecute el comando **chronyc sources** para comprobar si falla la autenticación del servidor NTP.

Si el valor de **Reach** para chrony es de **0**, se produce un error en la conexión o autenticación.

- En caso afirmativo, vaya a **Paso 12**.
- Si no, vaya a **Paso 8**.

Paso 7 Ejecute el comando **ntpq -np** para comprobar si falla la autenticación del servidor NTP.

Si **refid** del servidor NTP es**.AUTH.**, la autenticación falla.

- En caso afirmativo, vaya a **Paso 12**.
- Si no, vaya a **Paso 8**.

Comprobar si se puede obtener la hora del servidor NTP.

Paso 8 Ver la información adicional de la alarma para comprobar si la hora se puede obtener del servidor NTP.

- En caso afirmativo, vaya a **Paso 9**.
- Si no, vaya a **Paso 10**.

Paso 9 Póngase en contacto con el proveedor del servidor NTP para rectificar la falla del servidor NTP. Después de que el servidor NTP sea normal, compruebe si la alarma está borrada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 10**.

Comprobar si la hora obtenida del servidor NTP no se actualiza continuamente.

Paso 10 Ver la información adicional de la alarma para comprobar si la hora obtenida del servidor NTP no se actualiza continuamente.

- En caso afirmativo, vaya a **Paso 11**.
- Si no, vaya a **Paso 12**.

Paso 11 Póngase en contacto con el proveedor del servidor NTP para rectificar la falla del servidor NTP. Después de que el servidor NTP sea normal, compruebe si la alarma está borrada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 12**.

Recopilar información de fallas.

Paso 12 En el FusionInsight Manager, elija **O&M** > **Log > Download**.

Paso 13 Seleccione **NodeAgent** y **OmmServer** en el **Service** y haga clic en **OK**.

Paso 14 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 30 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 15 Póngase en contacto con el y envíe la información de registro recopilada.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.20 ALM-12038 Error de volcado de indicador de monitoreo

Descripción

Después de configurar el volcado del indicador de monitoreo en FusionInsight Manager, el sistema comprueba el resultado del volcado del indicador de monitoreo en el intervalo de volcado (60 segundos por defecto). Esta alarma se genera cuando falla el volcado.

Esta alarma se borra cuando el volcado tiene éxito.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
12038	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster o sistema para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

El sistema de gestión de la capa superior no puede obtener indicadores de monitorización del sistema de FusionInsight Manager.

Causas posibles

- No se puede conectar el servidor.
- No se puede acceder a la ruta de guardado del servidor.
- El archivo indicador de monitorización no se puede cargar.

Procedimiento

Comprobar si la conexión de servidor es normal.

Paso 1 Compruebe si la red entre el sistema de FusionInsight Manager y el servidor es normal.

- En caso afirmativo, vaya a **Paso 3**.
- Si no, vaya a **Paso 2**.

Paso 2 Póngase en contacto con el administrador de la red para recuperar la red y comprobar si la alarma está desactivada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 3**.

Paso 3 Elija **System** > **Interconnection > Upload Performance Data** y compruebe si el nombre de usuario, la contraseña, el puerto, el modo de volcado y la clave pública de FTP configurados en la página de datos de rendimiento de carga son coherentes con la configuración del servidor.

- En caso afirmativo, vaya a **Paso 5**.
- Si no, vaya a **Paso 4**.

Paso 4 Ingrese la información de configuración correcta, haga clic en **OK** y compruebe si la alarma está desactivada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 5**.

Comprobar el permiso de ruta guardada en el servidor es correcto.

Paso 5 Elija **System** > **Interconnection > Upload Performance Data** y compruebe los elementos de configuración **FTP Username**, **Save Path** y **Dump Mode**.

- Si el modo de volcado es FTP, vaya a **Paso 6**.
- Si el modo de volcado es SFTP, vaya a **Paso 7**.

Paso 6 Inicie sesión en el servidor en modo FTP. En la ruta predeterminada, compruebe si **FTP Username** tiene el permiso de lectura y escritura de la ruta relativa **Save Path**.

- En caso afirmativo, vaya a **Paso 9**.
- Si no, vaya a **Paso 8**.

Paso 7 Inicie sesión en el servidor en modo SFTP y compruebe si **FTP Username** tiene el permiso de lectura y escritura del **Save Path** de ruta absoluta.

- En caso afirmativo, vaya a **Paso 9**.
- Si no, vaya a **Paso 8**.

Paso 8 Agregue el permiso de lectura y escritura y compruebe si la alarma está borrada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 9**.

Comprobar si la ruta de guardado en el servidor tiene suficiente espacio en disco.

Paso 9 Inicie sesión en el servidor y compruebe si la ruta de guardado tiene suficiente espacio en disco.

- En caso afirmativo, vaya a **Paso 11**.
- Si no, vaya a **Paso 10**.

Paso 10 Elimine los archivos innecesarios o vaya a la página de configuración de volcado del indicador de supervisión para cambiar la ruta de guardado. A continuación, compruebe si la ruta de guardado tiene suficiente espacio en disco.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 11**.

Recopilar información de fallas.

Paso 11 En el portal del FusionInsight Manager, elija **O&M** > **Log > Download**.

Paso 12 Seleccione **OMS** en el **Service** y haga clic en **OK**.

Paso 13 Haga clic en  en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 1 hora antes y después del tiempo de generación de alarma, respectivamente. A continuación, haga clic en **Download**.

Paso 14 Póngase en contacto con el y envíe la información de registro recopilada.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.21 ALM-12039 Bases de datos de OMS activas/en espera no sincronizadas

Descripción

El sistema comprueba el estado de sincronización de datos entre las bases de datos de OMS activa y en espera cada 10 segundos. Esta alarma se genera cuando el estado de sincronización no puede consultarse durante 30 veces consecutivas o cuando el estado de sincronización es anormal.

Esta alarma se borra cuando el estado de sincronización de datos se vuelve normal.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
12039	Crítica	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster o sistema para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Local GaussDB HA IP	Especifica la dirección IP de HA de GaussDB local.
Peer GaussDB HA IP	Especifica la dirección IP de HA de GaussDB del mismo nivel.

Nombre	Significado
SYNC_PERCENT	Especifica el porcentaje de sincronización.

Impacto en el sistema

Cuando los datos no están sincronizados entre las bases de datos OMS activa y en espera, los datos pueden perderse o ser anormales si la instancia activa se vuelve anormal.

Causas posibles

- La red entre los nodos activos y en espera es inestable.
- La base de datos de OMS en espera es anormal.
- El espacio en disco del nodo en espera está lleno.

Procedimiento

Comprobar si la red entre los nodos activos y en espera es normal.

Paso 1 Inicie sesión en FusionInsight Manager, haga clic en **O&M > Alarm > Alarms**, haga clic en ⌄ en la fila donde se encuentra la alarma y consulte la dirección IP de la base de datos de OMS en espera.

Paso 2 Inicie sesión en el nodo de la base de datos OMS activa como **root**.

Paso 3 Ejecute el comando **ping** *Standby OMS Database heartbeat IP address* para comprobar si se puede acceder al nodo de la base de datos de OMS en espera.

- En caso afirmativo, vaya a **Paso 6**.
- Si no, vaya a **Paso 4**.

Paso 4 Póngase en contacto con el administrador de la red para comprobar si la red es defectuosa.

- En caso afirmativo, vaya a **Paso 5**.
- Si no, vaya a **Paso 6**.

Paso 5 Rectifique la falla de la red y compruebe si la alarma está borrada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 6**.

Comprobar si la base de datos OMS en espera es normal. (Omita esta comprobación para versiones posteriores a MRS 3.1.2.)

Paso 6 Inicie sesión en el nodo de la base de datos de OMS en espera como usuario **root**.

Paso 7 Ejecute el comando **su - omm** para cambiar a usuario **omm**.

Paso 8 Vaya al directorio **${BIGDATA_HOME}/om-server/om/sbin/** y ejecute el comando **./status-oms.sh** para comprobar si el estado de los recursos de la base de datos de OMS del DBService en espera es normal. En la salida del comando, compruebe si se muestra la siguiente información en la fila donde **ResName** es **gaussDB**:

Por ejemplo:

```
10_10_10_231 gaussDB Standby_normal Normal Active_standby
```


- En caso afirmativo, vaya a **Paso 9**.
- Si no, vaya a **Paso 16**.

Comprobar si el espacio en disco del nodo en espera está lleno.

Paso 9 Inicie sesión en el nodo de la base de datos de OMS en espera como usuario **root**.

Paso 10 Ejecute el comando **su - omm** para cambiar a usuario **omm**.

Paso 11 Ejecute el comando **echo ${BIGDATA_DATA_HOME}/dbdata_om** para obtener el directorio de datos de la base de datos de OMS.

Paso 12 Ejecute el comando **df -h** para ver la información de uso de la partición del disco del sistema.

Paso 13 Compruebe si el disco en el que está montado el directorio de datos de la base de datos de OMS está lleno.

- En caso afirmativo, vaya a **Paso 14**.
- Si no, vaya a **Paso 16**.

Paso 14 Amplíe la capacidad del disco.

Paso 15 Después de ampliar la capacidad del disco, espere 2 minutos y compruebe si la alarma está borrada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 16**.

Recopilar información de fallas.

Paso 16 En el portal del FusionInsight Manager, elija **O&M** > **Log > Download**.

Paso 17 Seleccione **OMMServer** en **Service** y haga clic en **OK**.

Paso 18 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 19 Póngase en contacto con el y envíe la información de registro recopilada.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.22 ALM-12040 Entropía del sistema insuficiente

Descripción

El sistema comprueba la entropía durante cinco veces consecutivas a las 00:00 todos los días. Específicamente, el sistema comprueba si rng-tools o haveged se ha habilitado y configurado

correctamente. Si ninguno de los dos está configurado, el sistema continúa comprobando la entropía. Si la entropía es menor que 100 durante cinco veces consecutivas, se informa de esta alarma.

Esta alarma se borra cuando el sistema detecta que se ha configurado el modo de número aleatorio verdadero, los parámetros de número aleatorio se han configurado en el modo de número pseudoaleatorio, o ninguno de los modos está configurado, pero la entropía del sistema operativo es mayor o igual a 100 en al menos una de las cinco comprobaciones de entropía.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
12040	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster o sistema para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

El sistema no está funcionando correctamente.

Causas posibles

- rng-tools o haveged no se ha instalado ni iniciado.
- La entropía del sistema operativo es menor que 100 por varias veces consecutivas.

Procedimiento

Compruebe si se ha instalado o iniciado haveged o rng-tools.

Paso 1 Inicie sesión en FusionInsight Manager y elija **O&M** > **Alarm** > **Alarms**.

Paso 2 Compruebe el valor de **HostName** en el área **Location** para obtener el nombre del host para el que se genera la alarma.

Paso 3 Inicie sesión en el nodo para el que se genera la alarma como usuario **root**.

Paso 4 Ejecute el comando **/bin/rpm -qa | grep -w "haveged"** para comprobar el estado de instalación haveged y comprobar si la salida del comando está vacía.

- En caso afirmativo, vaya a **Paso 6**.
- Si no, vaya a **Paso 5**.

Paso 5 Ejecute el comando **/sbin/service haveged status |grep "running"** y compruebe la salida del comando.

- Si el comando se ejecuta correctamente, haveged se ha instalado y configurado correctamente y se está ejecutando correctamente. Vaya a **Paso 8**.
- Si el comando no se ejecuta, haveged no se ejecuta correctamente. Ejecute el siguiente comando para reiniciar manualmente hasged y vaya a **Paso 9**:

  systemctl restart haveged.service

Paso 6 Ejecute el comando **/bin/rpm -qa | grep -w "rng-tools"** para comprobar la instalación de rng-tools y comprobar si la salida del comando está vacía.

- En caso afirmativo, póngase en contacto con el proveedor del sistema operativo para instalar e iniciar haveged o rng-tools. Entonces vaya a **Paso 9**.
- Si no, vaya a **Paso 7**.

Paso 7 Ejecute el comando **ps -ef | grep -v "grep" | grep rngd | tr -d " " | grep "\-r/dev/urandom"** y compruebe la salida del comando.

- Si el comando se ejecuta correctamente, rngd se ha instalado y configurado correctamente y se está ejecutando correctamente. Vaya a **Paso 8**.
- Si el comando no se ejecuta, rngd no se ejecuta correctamente. Ejecute el siguiente comando para reiniciar manualmente rngd y vaya a **Paso 9**:

  systemctl restart rngd.service

Compruebe la entropía del sistema operativo.

Paso 8 Verifique manualmente la entropía del sistema operativo.

Inicie sesión en el nodo de destino como usuario **root** y ejecute el comando **cat /proc/sys/kernel/random/entropy_avail** para comprobar si la entropía del sistema operativo cumple con los requisitos de instalación del clúster (no menos de 100).

- En caso afirmativo, la entropía del sistema operativo no es inferior a 100. Vaya a **Paso 9**.
- Si no, la entropía del sistema operativo es inferior a 100. Utilice cualquiera de los siguientes métodos y vaya a **Paso 9**.
  - Método 1: Usar haveged (modo de números aleatorios verdaderos). Póngase en contacto con el proveedor del sistema operativo para instalar e iniciar haveged.

    En Kylin, ejecute el siguiente comando:

    vi /usr/lib/systemd/system/haveged.service

    Configure **Type**, **ExecStar**, **SuccessExitStatus** y **Restart** en **[Service]** de la siguiente manera:

    ```
    Type=simple
    ExecStar=/usr/sbin/haveged -w 1024 -v 1 -Foreground
    SuccessExitStatus=137 143
    Restart=always
    ```

  - Método 2: Utilice rng-tools (modo de número pseudo-aleatorio). Póngase en contacto con el proveedor del sistema operativo para instalar e iniciar rng-tools y configurarlo según el tipo de sistema operativo.

- En Red Hat Linux o CentOS, ejecute los siguientes comandos:

  echo 'EXTRAOPTIONS="-r /dev/urandom -o /dev/random -t 1 -i"' >> /etc/sysconfig/rngd

  service rngd start

  chkconfig rngd on

- En SUSE, ejecute los siguientes comandos:

  rngd -r /dev/urandom -o /dev/random

  echo "rngd -r /dev/urandom -o /dev/random" >> /etc/rc.d/after.local

- En Kylin, ejecute el siguiente comando como usuario **root** en el nodo donde se reporta la alarma:

  vi /usr/lib/systemd/system/rngd.service

  Cambie el valor de **ExecStart** en **[Service]** de la siguiente manera:

  ```
  ExecStart=/sbin/rngd -f -r /dev/urandom -s 2048
  ```

Paso 9 Espere hasta que el sistema compruebe la entropía a las 00:00 del día siguiente y compruebe si la alarma está borrada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 10**.

Recopilar información de fallas.

Paso 10 En FusionInsight Manager, seleccione **O&M**. En el panel de navegación de la izquierda, elija **Log** > **Download**.

Paso 11 Seleccione **NodeAgent** para **Service** y haga clic en **OK**.

Paso 12 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 13 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

9.23 ALM-12041 Permiso incorrecto en archivos clave

Descripción

El sistema comprueba si la información de permisos, usuarios y grupos de usuarios sobre directorios o archivos críticos es normal cada 5 minutos. Esta alarma se genera cuando la información es anormal.

Esta alarma se borra cuando la información se vuelve normal.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
12041	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster o sistema para el que se genera la alarma.
ServiceName	Especifica el nombre del servicio para el que se genera la alarma.
RoleName	Especifica el nombre del rol para el que se genera la alarma.
HostName	Especifica el objeto (ID de host) para el que se genera la alarma.
PathName	Especifica la ruta de acceso o el nombre del archivo anormal.

Impacto en el sistema

Las funciones del sistema no están disponibles.

Causas posibles

El permiso de archivo es anormal o el archivo se pierde debido a una información modificada manualmente por el usuario, como el permiso de archivo, el usuario y el grupo de usuarios, o el sistema se apaga inesperadamente.

Procedimiento

Comprobar si existe el archivo anormal y si el permiso en el archivo anormal es correcto.

Paso 1 En el portal de FusionInsight Manager, seleccione **O&M > Alarm > Alarms**.

Paso 2 Compruebe el valor de **HostName** para obtener el nombre de host involucrado en esta alarma. Compruebe el valor de **PathName** para obtener la ruta o el nombre del archivo anormal.

Paso 3 Inicie sesión en el nodo para el que se genera la alarma como **root**.

Paso 4 Ejecute el comando **ll** *pathName*, donde *pathName* indica el nombre del archivo anormal para obtener la información de usuario, permiso y grupo de usuarios sobre el archivo o directorio.

Paso 5 Ir al directorio de **${BIGDATA_HOME}/om-agent/nodeagent/etc/agent/autocheck**. A continuación, ejecute el comando **vi keyfile** y busque el nombre del archivo anormal y compruebe el permiso debido del archivo.

NOTA

Para garantizar la sincronización adecuada de la configuración entre los servidores OMS activos y en espera, los archivos, directorios y archivos y subdirectorios de los directorios configurados en el **$OMS_RUN_PATH/workspace/ha/module/hasync/plugin/conf/filesync.xml** también se supervisarán, excepto los archivos y directorios de **keyfile**. El usuario **omm** debe tener permisos de lectura y escritura de archivos y permisos de lectura y ejecución de directorios.

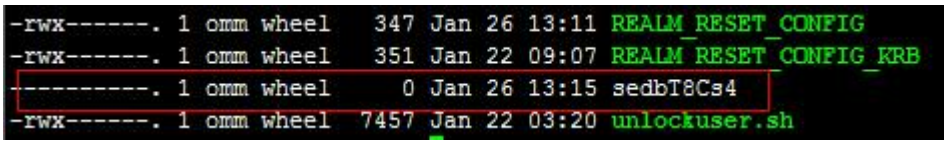
Paso 6 Compare el permiso real del archivo con el permiso debido obtenido en **Paso 5** y corrija la información de permiso, usuario y grupo de usuarios para el archivo.

Paso 7 Espere una hora y compruebe si la alarma está desactivada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 8**.

NOTA

Si se agota la partición de disco donde reside el directorio de instalación del clúster, se generarán algunos archivos temporales en el directorio de instalación del programa cuando la ejecución del comando **sed** falla. Los usuarios no tienen los permisos de lectura, escritura y ejecución de estos archivos temporales. El sistema informa de una alarma que indica que los permisos de los archivos temporales son anormales si estos archivos están dentro del rango de supervisión de la alarma. Realice los procesos de manejo de alarmas anteriores para borrar la alarma. Alternativamente, puede eliminar directamente los archivos temporales después de confirmar que los archivos con permisos anormales son temporales. El archivo temporal generado después de una falla en la ejecución del comando **sed** es similar al siguiente.



Recopilar información de fallas.

Paso 8 En el portal del FusionInsight Manager, elija **O&M** > **Log > Download**.

Paso 9 Seleccione **NodeAgent** en el **Service** y haga clic en **OK**.

Paso 10 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 11 Póngase en contacto con el y envíe la información de registro recopilada.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.24 ALM-12042 Configuración incorrecta de archivos clave

Descripción

El sistema comprueba si las configuraciones críticas son correctas cada 5 minutos. Esta alarma se genera cuando las configuraciones son anormales.

Esta alarma se borra cuando las configuraciones se vuelven normales.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
12042	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster o sistema para el que se genera la alarma.
ServiceName	Especifica el nombre del servicio para el que se genera la alarma.
RoleName	Especifica el nombre del rol para el que se genera la alarma.
HostName	Especifica el objeto (ID de host) para el que se genera la alarma.
PathName	Especifica la ruta de acceso o el nombre del archivo anormal.

Impacto en el sistema

Las funciones relacionadas con el archivo son anormales.

Causas posibles

La configuración del archivo se modifica manualmente o el sistema se apaga inesperadamente.

Procedimiento

Verificar la configuración de archivos anormales.

Paso 1 En el portal de FusionInsight Manager, seleccione **O&M > Alarm > Alarms**.

Paso 2 Compruebe el valor de **HostName** para obtener el nombre de host involucrado en esta alarma. Compruebe el valor de **PathName** para obtener la ruta o el nombre del archivo anormal.

Paso 3 Inicie sesión en el nodo para el que se genera la alarma como **root**.

Paso 4 Vea el archivo $BIGDATA_LOG_HOME/nodeagent/scriptlog/checkfileconfig.log y analice la causa basándose en el registro de errores. Localice los estándares de comprobación del archivo en el **Información relacionada** y compruebe y modifique manualmente el archivo en función de los estándares.

Ejecute el comando **vi** *file name* para entrar en el modo de edición y, a continuación, presione **Insert** para comenzar a editar.

Una vez completada la modificación, pulse **Esc** para salir del modo de edición e introduzca **:wq** para guardar la configuración y salir.

Por ejemplo:

vi /etc/ssh/sshd_config

Paso 5 Espere una hora y compruebe si la alarma está desactivada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 6**.

Recopilar información de fallas.

Paso 6 En el portal del FusionInsight Manager, elija **O&M** > **Log > Download**.

Paso 7 Seleccione **NodeAgent** en el **Service** y haga clic en **OK**.

Paso 8 Haga clic en  en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 9 Póngase en contacto con el y envíe la información de registro recopilada.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

- **Comprobar estándares de /etc/fstab**

  Compruebe si las particiones configuradas en el archivo **/etc/fstab** se encuentran en **/proc/mounts**.

  Compruebe si las particiones de swap configuradas en fstab corresponden a las de /proc/swaps.

- **Verificar el archivo de configuración /etc/hosts.**

  Ejecute **cat /ect/hosts**. Si se produce alguna de las siguientes situaciones, el archivo de configuración **/etc/hosts** es anormal:

  a. El archivo **/etc/hosts** no existe.

b. El nombre de host no está configurado en el archivo.

c. El nombre de host se asigna a varias direcciones IP del archivo.

d. La dirección IP correspondiente al nombre del host no existe en la salida del comando **ifconfig** .

e. Una dirección IP se asigna a varios nombres de host en el archivo.

- **Comprobar estándares de /etc/ssh/sshd_config**

  Ejecute el comando **vi /etc/ssh/sshd_config** para comprobar si los elementos de configuración están configurados de la siguiente manera:

  a. El valor de **UseDNS** debe establecerse en **no**.

  b. El valor de **MaxStartups** debe ser mayor o igual a 1000.

  c. Al menos uno de los parámetros **PasswordAuthentication** y **ChallengeResponseAuthentication** debe dejarse en blanco o al menos uno de los parámetros debe establecerse en **yes**.

9.25 ALM-12045 La tasa de pérdida de paquetes de lectura supera el umbral

Descripción

El sistema comprueba la tasa de pérdida del paquete de lectura cada 30 segundos. Esta alarma se genera cuando la tasa de pérdida del paquete de lectura excede el umbral (el umbral predeterminado es 0.5%) varias veces (el valor predeterminado es **5**).

Para cambiar el umbral, elija **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster* > **Host** > **Network Reading** > **Read Packet Dropped Rate**.

Esta alarma se borra cuando **Trigger Count** es 1 y la tasa de pérdida de paquetes de lectura es menor o igual que el umbral. Esta alarma se borra cuando **Trigger Count** es mayor que 1 y la tasa de pérdida del paquete de lectura es menor o igual al 90% del umbral.

La detección de alarma está deshabilitada de forma predeterminada. Si desea habilitar esta función, compruebe si esta función se puede habilitar en función de Comprobación de entornos del sistema.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
12045	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster o sistema para el que se genera la alarma.

Nombre	Significado
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
PortName	Especifica el puerto de red para el que se genera la alarma.
Trigger Condition	Especifica el umbral para activar la alarma.

Impacto en el sistema

El rendimiento del servicio se deteriora o el tiempo de espera de algunos servicios.

Advertencia de riesgos: En SUSE kernel 3.0 o posterior o Red Hat 7.2, el kernel del sistema modifica el mecanismo para contar el número de paquetes de lectura perdidos. En este caso, esta alarma puede generarse incluso si la red se está ejecutando correctamente, pero los servicios no se ven afectados. Se recomienda comprobar primero el entorno del sistema.

Causas posibles

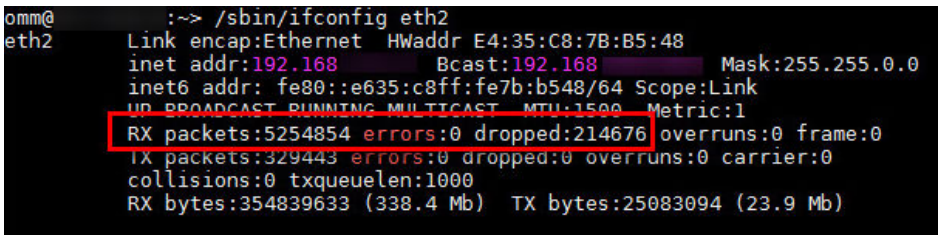
- Se produce una excepción del sistema operativo.
- Las NIC están unidas en modo activo/en espera.
- El umbral de alarma está configurado incorrectamente.
- La calidad de la red es mala.

Procedimiento

Ver la tasa de pérdida de paquetes de red.

Paso 1 En FusionInsight Manager, seleccione **O&M** > **Alarm** > **Alarms**. En la página que se muestra, haga clic en ⌄ en la fila que contiene la alarma y vea el nombre del host para el que se genera la alarma y el nombre de la NIC.

Paso 2 Inicie sesión en el nodo de alarma como usuario **omm** y ejecute el comando **/sbin/ifconfig** *NIC name* para comprobar si se produce pérdida de paquetes en la red.



NOTA

- *Dirección IP del nodo para el que se genera la alarma*: Consulta la dirección IP del nodo para el que se genera la alarma en la página **Hosts** del FusionInsight Manager basándose en el valor de **HostName** en la información de ubicación de la alarma. Compruebe tanto las direcciones IP del plano de gestión como del plano de servicio.
- Tasa de pérdida de paquetes = (Número de paquetes perdidos/Número total de paquetes recibidos) x 100%. Si la tasa de pérdida de paquetes es mayor que el umbral del sistema (0.5% por defecto), los paquetes de lectura se descartan.

- En caso afirmativo, vaya a **Paso 11**.
- Si no, vaya a **Paso 3**.

Comprobar el entorno de sistema.

Paso 3 Inicie sesión en el nodo OMS activo o en el nodo de alarma como usuario **omm**.

Paso 4 Ejecute el comando **cat /etc/*-release** para comprobar el tipo de sistema operativo.

- Para Red Hat Enterprise Linux, vaya a **Paso 5**.
```
# cat /etc/*-release
Red Hat Enterprise Linux Server release 7.2 (Santiago)
```
- Para SUSE Linux, vaya a **Paso 6**.
```
# cat /etc/*-release
SUSE Linux Enterprise Server 11 (x86_64)
VERSION = 11
PATCHLEVEL = 3
```
- Para otros tipos de sistema operativo, vaya a **Paso 11**.

Paso 5 Ejecute el comando **cat /etc/redhat-release** para comprobar si la versión del sistema operativo es de **Red Hat 7.2 (x86)** o de **Red Hat 7.4 (TaiShan)**.
```
# cat /etc/redhat-release
Red Hat Enterprise Linux Server release 7.2 (Santiago)
```
- En caso afirmativo, no se puede activar la función de envío de alarmas. Vaya a **Paso 7**.
- Si no, vaya a **Paso 11**.

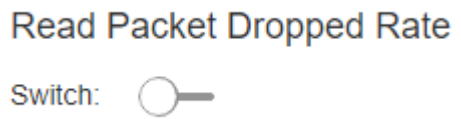
Paso 6 Ejecute el comando **cat /proc/version** para comprobar si la versión del kernel de SUSE es 3.0 o posterior.
```
# cat /proc/version
Linux version 3.0.101-63-default (geeko@buildhost) (gcc version 4.3.4 [gcc-4_3-
branch revision 152973] (SUSE Linux) ) #1 SMP Tue Jun 23 16:02:31 UTC 2015
(4b89d0c)
```
- En caso afirmativo, no se puede activar la función de envío de alarmas. Vaya a **Paso 7**.
- Si no, vaya a **Paso 11**.

Paso 7 Inicie sesión en el FusionInsight Manager y elija **O&M** > **Alarm** > **Threshold Configuration**.

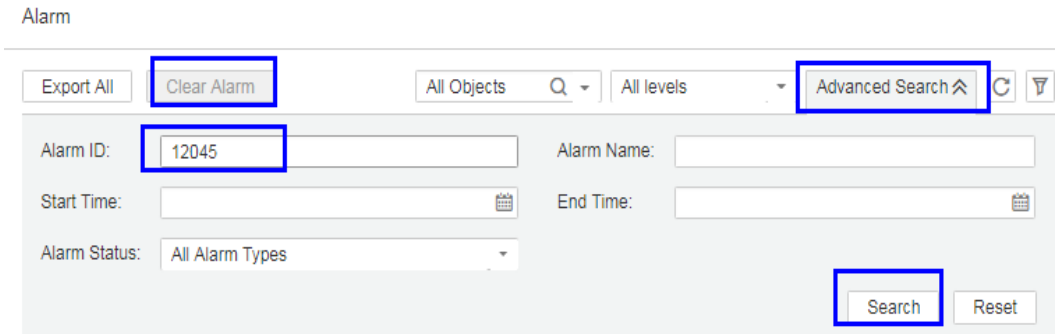
Paso 8 En el árbol de navegación de la página **Thresholds**, seleccione *Name of the desired cluster* > **Host** > **Network Reading** > **Read Packet Dropped Rate**. En el área de la derecha, comprueba si el **Switch** está activado.

- En caso afirmativo, la función de envío de alarmas está activada. Vaya a **Paso 9**.
- Si no, la función de envío de alarmas está desactivada. Vaya a **Paso 10**.

Paso 9 En el área de la derecha, desactive **Switch** para desactivar la comprobación de **La tasa de pérdida de paquetes de lectura de red supera el umbral**.



Paso 10 En la página **Alarm** del FusionInsight Manager, busque alarma **12045** y borre manualmente la alarma si no se borra automáticamente. No se requiere ninguna otra acción.



NOTA

El ID de la velocidad de pérdida de paquetes de lectura de red supera la alarma de umbral es **12045**.

Compruebe si las NIC están enlazadas en modo activo/en espera.

Paso 11 Inicie sesión en el nodo de alarma como usuario **omm** y ejecute el comando **ls -l /proc/net/bonding** para comprobar si el directorio **/proc/net/bonding** existe en el nodo.

- En caso afirmativo, el modo de enlace se configura para el nodo. Vaya a **Paso 12**.

```
# ls -l /proc/net/bonding/
total 0
-r--r--r-- 1 root root 0 Oct 11 17:35 bond0
```

- Si no, el modo de enlace no está configurado para el nodo. Vaya a **Paso 14**.

```
# ls -l /proc/net/bonding/
ls: cannot access /proc/net/bonding/: No such file or directory
```

Paso 12 Ejecute el comando **cat /proc/net/bonding/***bond0* para comprobar si el valor de **Bonding Mode** en el archivo de configuración es **fault-tolerance**.

NOTA

En el comando, **bond0** indica el nombre del archivo de configuración de enlace. Utilice el nombre de archivo obtenido en **Paso 11**.

```
# cat /proc/net/bonding/bond0
Ethernet Channel Bonding Driver: v3.7.1 (April 27, 2011)

Bonding Mode: fault-tolerance (active-backup)
Primary Slave: eth1 (primary_reselect always)
Currently Active Slave: eth1
MII Status: up
MII Polling Interval (ms): 100
Up Delay (ms): 0
Down Delay (ms): 0

Slave Interface: eth0
MII Status: up
Speed: 1000 Mbps
Duplex: full
Link Failure Count: 1
Slave queue ID: 0
```



```
Slave Interface: eth1
MII Status: up
Speed: 1000 Mbps
Duplex: full
Link Failure Count: 1
Slave queue ID: 0
```

- En caso afirmativo, las NIC se unen en modo activo/en espera. Vaya a **Paso 13**.
- Si no, vaya a **Paso 14**.

Paso 13 Compruebe si la NIC especificada por **NetworkCardName** en la alarma es la NIC en espera.

- En caso afirmativo, la alarma de la NIC en espera no se puede borrar automáticamente. Borre manualmente la alarma en la página de gestión de alarmas. No se requiere ninguna otra acción.
- Si no, vaya a **Paso 14**.

NOTA

Para determinar la NIC en espera, compruebe el archivo de configuración **/proc/net/bonding/bond0**. Si el nombre de NIC correspondiente a **NetworkCardName** es **Slave Interface** pero no **Currently Active Slave** (la NIC activa actual), la NIC es la en espera.

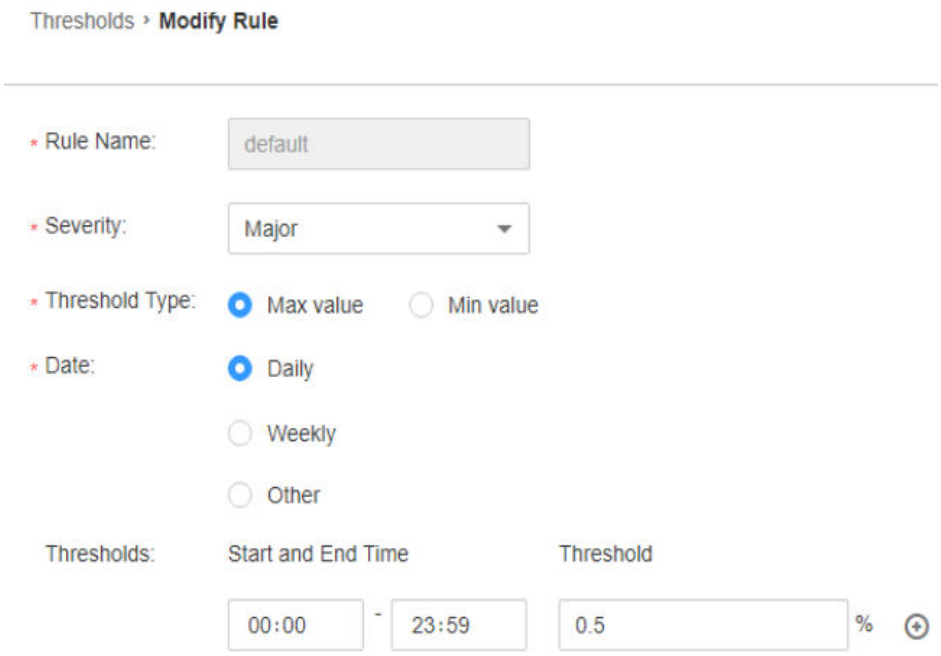
Comprobar si el umbral está configurado correctamente.

Paso 14 Inicie sesión en FusionInsight Manager, elija **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster* > **Host** > **Network Reading** > **Read Packet Dropped Rate** y compruebe si el umbral de alarma está configurado correctamente. El valor predeterminado es **0.5%**. Puede ajustar el umbral según sea necesario.

- En caso afirmativo, vaya a **Paso 17**.
- Si no, vaya a **Paso 15**.

Paso 15 Elija **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster* > **Host** > **Network Reading** > **Read Packet Dropped Rate**. Haga clic en **Modify** en la columna **Operation** para cambiar el umbral. Consulte **Figura 9-5**.

Figura 9-5 Configuración del umbral de alarma



Paso 16 Después de 5 minutos, compruebe si la alarma está borrada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 17**.

Comprobar si la conexión de red es normal.

Paso 17 Póngase en contacto con el administrador de la red para comprobar si la red es normal.

- En caso afirmativo, rectifique la falla y diríjase a **Paso 18**.
- Si no, vaya a **Paso 19**.

Paso 18 Después de 5 minutos, compruebe si la alarma está borrada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 19**.

Recopilar información de fallas.

Paso 19 En el FusionInsight Manager del clúster activo, seleccione **O&M**. En el panel de navegación de la izquierda, elija **Log** > **Download**.

Paso 20 Seleccione **OMS** para **Service** y haga clic en **OK**.

Paso 21 Expanda el cuadro de diálogo **Hosts** y seleccione el nodo de alarma y el nodo OMS activo.

Paso 22 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 30 minutos antes y después del tiempo de generación de alarmas respectivamente. A continuación, haga clic en **Download**.

Paso 23 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

Información relacionada

Ninguna

9.26 ALM-12046 La tasa de pérdidas de paquetes de escritura supera el umbral

Descripción

El sistema comprueba la tasa de pérdida del paquete de escritura cada 30 segundos. Esta alarma se genera cuando la tasa de pérdida de paquetes de escritura supera el umbral (el umbral predeterminado es 0.5%) varias veces (el valor predeterminado es **5**).

Para cambiar el umbral, elija **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster* > **Host** > **Network Writing** > **Write Packet Dropped Rate**.

Si **Trigger Count** es de **1**, esta alarma se borra cuando la tasa de pérdida de paquetes de escritura en red es menor o igual que el umbral. Si **Trigger Count** es mayor que **1**, esta

alarma se borra cuando la tasa de pérdida de paquetes de escritura en red es menor o igual al 90% del umbral.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
12046	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster o sistema para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Port Name	Especifica el puerto de red para el que se genera la alarma.
Trigger Condition	Especifica el umbral para activar la alarma.

Impacto en el sistema

El rendimiento del servicio se deteriora o el tiempo de espera de algunos servicios.

Causas posibles

- El umbral de alarma está configurado incorrectamente.
- La calidad de la red es mala.

Procedimiento

Comprobar si el umbral está configurado correctamente.

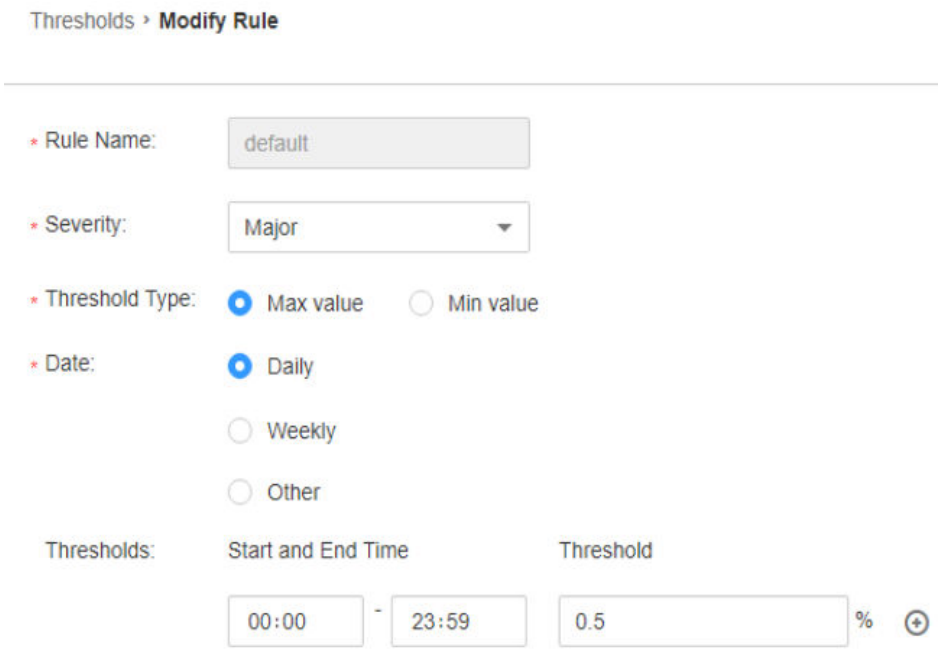
Paso 1 Inicie sesión en el FusionInsight Manager,, elija **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster* > **Host** > **Network Writing** > **Write Packet Dropped Rate** y compruebe si el umbral de alarma está configurado correctamente. El valor predeterminado es **0.5%**. Puede ajustar el umbral según sea necesario.

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 2**.

Paso 2 Elija **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster* > **Host** > **Network Writing** > **Write Packet Dropped Rate**. Haga clic en **Modify** en la columna **Operation** para cambiar el umbral.

Consulte **Figura 9-6**.

Figura 9-6 Configuración del umbral de alarma



Paso 3 Después de 5 minutos, compruebe si la alarma está borrada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 4**.

Comprobar si la conexión de red es normal.

Paso 4 Póngase en contacto con el administrador de la red para comprobar si la red es normal.

- En caso afirmativo, rectifique la falla y diríjase a **Paso 5**.
- Si no, vaya a **Paso 6**.

Paso 5 Después de 5 minutos, compruebe si la alarma está borrada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 6**.

Recopilar información de fallas.

Paso 6 En el FusionInsight Manager del clúster activo, seleccione **O&M**. En el panel de navegación de la izquierda, elija **Log** > **Download**.

Paso 7 Seleccione **OMS** para **Service** y haga clic en **OK**.

Paso 8 Expanda el cuadro de diálogo **Hosts** y seleccione el nodo de alarma y el nodo OMS activo.

Paso 9 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 30 minutos antes y después del tiempo de generación de alarmas respectivamente. A continuación, haga clic en **Download**.

Paso 10 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

Información relacionada

Ninguna

9.27 ALM-12047 La tasa de error de paquete de lectura supera el umbral

Descripción

El sistema comprueba la tasa de errores del paquete leído cada 30 segundos. Esta alarma se genera cuando la tasa de error del paquete leído excede el umbral (el umbral predeterminado es de **0.5%**) varias veces (el valor predeterminado es de **5**).

Para cambiar el umbral, elija **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster* > **Host** > **Network Reading** > **Read Packet Error Rate**.

Si **Trigger Count** es de **1**, esta alarma se borra cuando la tasa de error del paquete leído es menor o igual que el umbral. Si **Trigger Count** es mayor que **1**, esta alarma se borra cuando la tasa de error del paquete leído es menor o igual al 90% del umbral.

Atributo

ID de alarma	Gravedad de la alarma	Borrado automático
12047	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster o sistema para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Nombre	Significado
Port Name	Especifica el puerto de red para el que se genera la alarma.
Trigger Condition	Especifica el umbral para activar la alarma.

Impacto en el sistema

La comunicación se interrumpe intermitentemente y los servicios expiran.

Causas posibles

- El umbral de alarma está configurado incorrectamente.
- La calidad de la red es mala.

Procedimiento

Comprobar si el umbral está configurado correctamente.

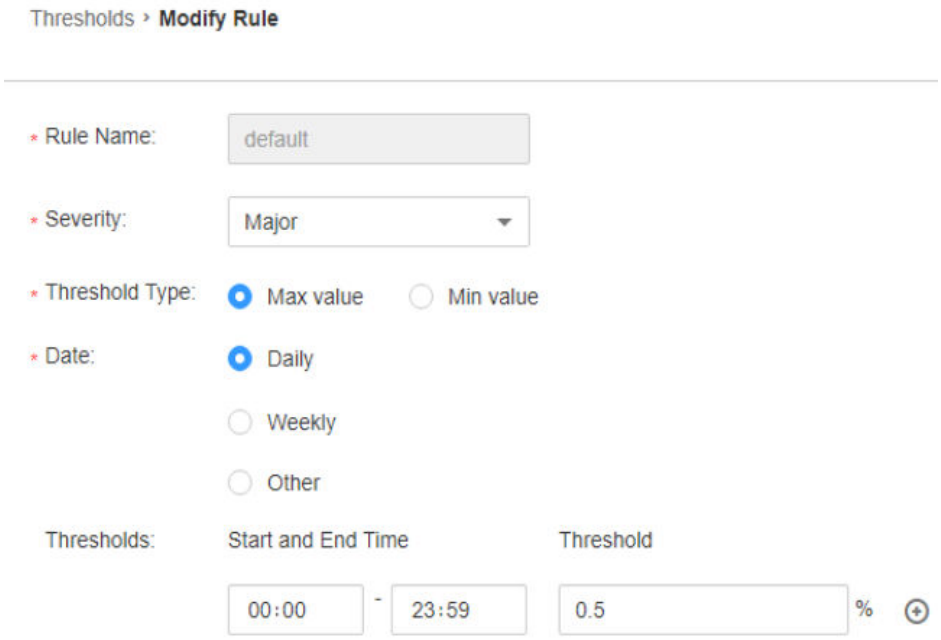
Paso 1 Inicie sesión en el Administrador de FusionInsight, elija **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster* > **Host** > **Network Reading** > **Read Packet Error Rate** y compruebe si el umbral de alarma está configurado correctamente. El valor predeterminado es **0.5%**. Puede ajustar el umbral según sea necesario.

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 2**.

Paso 2 Elija **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster* > **Host** > **Network Reading** > **Read Packet Error Rate**. Haga clic en **Modify** en la columna **Operation** para cambiar el umbral.

Consulte **Figura 9-7**.

Figura 9-7 Configuración del umbral de alarma



Paso 3 Después de 5 minutos, compruebe si la alarma está borrada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 4**.

Comprobar si la conexión de red es normal.

Paso 4 Póngase en contacto con el administrador de la red para comprobar si la red es normal.

- En caso afirmativo, rectifique la falla y diríjase a **Paso 5**.
- Si no, vaya a **Paso 6**.

Paso 5 Después de 5 minutos, compruebe si la alarma está borrada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 6**.

Recopilar información de fallas.

Paso 6 En el FusionInsight Manager del clúster activo, seleccione **O&M**. En el panel de navegación de la izquierda, elija **Log** > **Download**.

Paso 7 Seleccione **OMS** para **Service** y haga clic en **OK**.

Paso 8 Expanda el cuadro de diálogo **Hosts** y seleccione el nodo de alarma y el nodo OMS activo.

Paso 9 Haga clic en  en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 30 minutos antes y después del tiempo de generación de alarmas respectivamente. A continuación, haga clic en **Download**.

Paso 10 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

Información relacionada

Ninguna

9.28 ALM-12048 La tasa de errores de escritura de paquetes supera el umbral

Descripción

El sistema comprueba la tasa de errores de escritura de paquetes cada 30 segundos. Esta alarma se genera cuando la tasa de errores de paquete de escritura supera el umbral (el umbral predeterminado es de **0.5%**) varias veces (el valor predeterminado es de **5**).

Para cambiar el umbral, elija **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster* > **Host** > **Network Writing** > **Write Packet Error Rate**.

Si **Trigger Count** es de **1**, esta alarma se borra cuando la tasa de errores de paquete de escritura es menor o igual que el umbral. Si **Trigger Count** es mayor que **1**, esta alarma se borra cuando la tasa de error de paquete de escritura es menor o igual al 90% del umbral.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
12048	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster o sistema para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Port Name	Especifica el puerto de red para el que se genera la alarma.
Trigger Condition	Especifica el umbral para activar la alarma.

Impacto en el sistema

La comunicación se interrumpe intermitentemente y los servicios expiran.

Causas posibles

- El umbral de alarma está configurado incorrectamente.
- La calidad de la red es mala.

Procedimiento

Comprobar si el umbral está configurado correctamente.

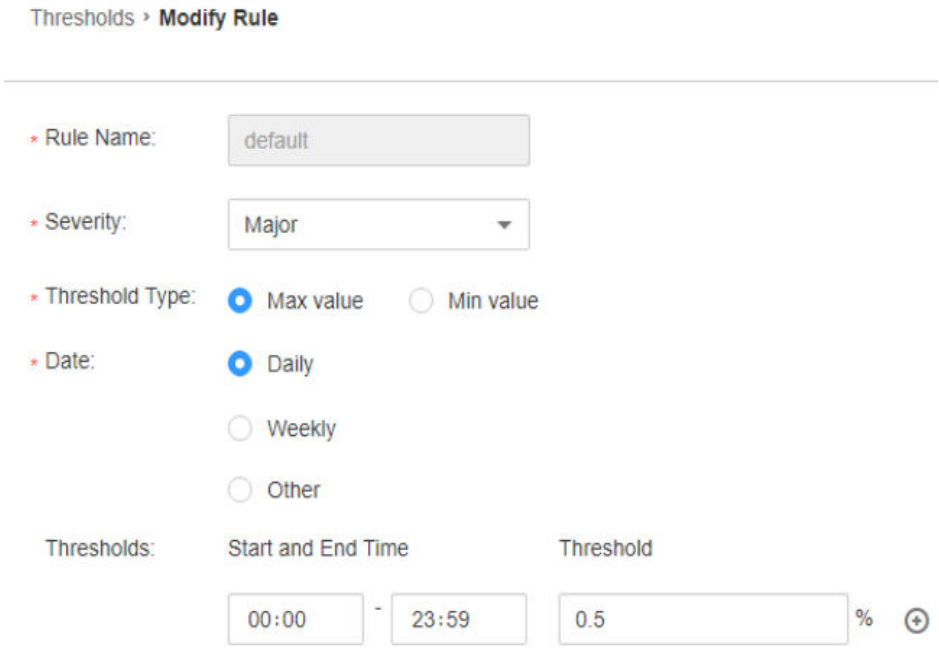
Paso 1 Inicie sesión en FusionInsight Manager, elija **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster* > **Host** > **Network Writing** > **Write Packet Error Rate** y compruebe si el umbral de alarma está configurado correctamente. El valor predeterminado es **0.5%**. Puede ajustar el umbral según sea necesario.

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 2**.

Paso 2 Elija **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster* > **Host** > **Network Writing** > **Write Packet Error Rate**. Haga clic en **Modify** en la columna **Operation** para cambiar el umbral.

Consulte **Figura 9-8**.

Figura 9-8 Configuración del umbral de alarma



Paso 3 Después de 5 minutos, compruebe si la alarma está borrada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 4**.

Comprobar si la conexión de red es normal.

Paso 4 Póngase en contacto con el administrador de la red para comprobar si la red es normal.

- En caso afirmativo, rectifique la falla y diríjase a **Paso 5**.
- Si no, vaya a **Paso 6**.

Paso 5 Después de 5 minutos, compruebe si la alarma está borrada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 6**.

Recopilar información de fallas.

Paso 6 En el FusionInsight Manager del clúster activo, seleccione **O&M** > **Log** > **Download**.

Paso 7 Seleccione **OMS** para **Service** y haga clic en **OK**.

Paso 8 Expanda el cuadro de diálogo **Hosts** y seleccione el nodo de alarma y el nodo OMS activo.

Paso 9 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 30 minutos antes y después del tiempo de generación de alarmas respectivamente. A continuación, haga clic en **Download**.

Paso 10 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

Información relacionada

Ninguna

9.29 ALM-12049 La tasa de rendimiento de lectura de red supera el umbral

Descripción

El sistema comprueba la tasa de rendimiento de lectura de la red cada 30 segundos y compara la tasa de rendimiento real con el umbral (el umbral predeterminado es 80%). Esta alarma se genera cuando el sistema detecta que la tasa de rendimiento de lectura de la red excede el umbral varias veces (5 veces por defecto) consecutivamente.

Para cambiar el umbral, elija **O&M > Alarm** > **Thresholds** > *Name of the desired cluster* > **Host** > **Network Reading** > **Read Throughput Rate**.

Cuando el **Trigger Count** es 1, esta alarma se borra cuando la tasa de rendimiento de lectura de red es menor o igual que el umbral. Cuando el **Trigger Count** es mayor que 1, esta alarma se borra cuando la tasa de rendimiento de lectura de red es menor o igual al 90% del umbral.

Atributo

ID de alarma	Gravedad de la alarma	Borrado automático
12049	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster o sistema para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Nombre	Significado
NetworkCardName	Especifica el puerto de red para el que se genera la alarma.
Trigger Condition	Especifica el umbral que activa la alarma. Si el valor del indicador actual excede este umbral, se genera la alarma.

Impacto en el sistema

El sistema de servicio se ejecuta incorrectamente o no está disponible.

Causas posibles

- El umbral de alarma se establece incorrectamente.
- La velocidad de puerto de red no puede cumplir los requisitos de servicio actuales.

Procedimiento

Compruebe si el umbral está configurado correctamente.

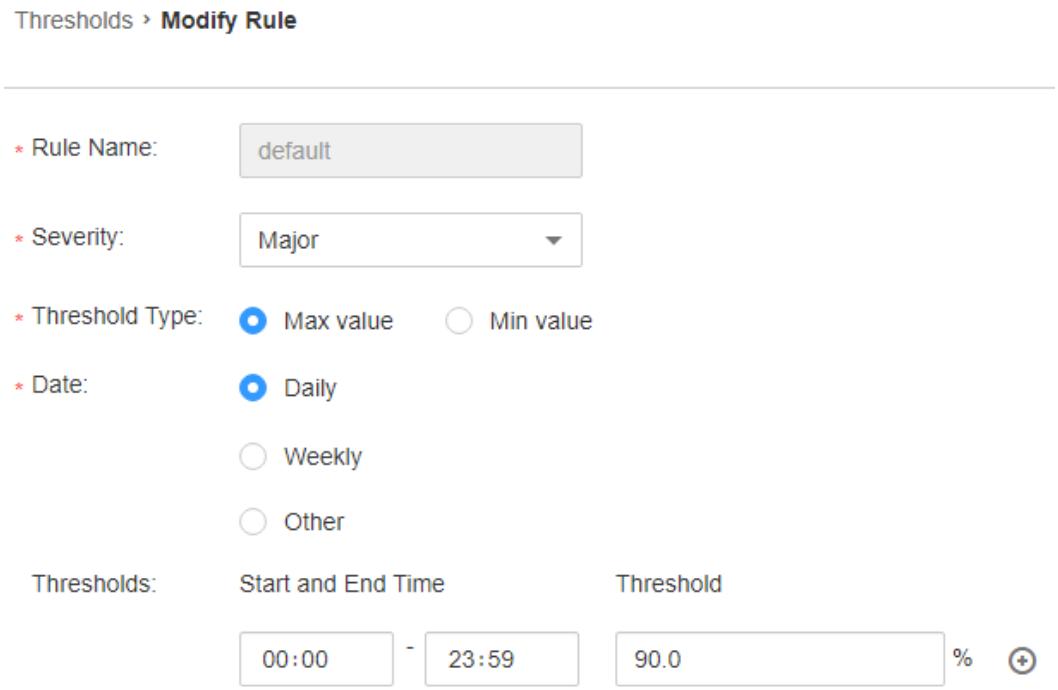
Paso 1 En el Administrador de FusionInsight, seleccione **O&M > Alarm** > **Thresholds** > *Name of the desired cluster* > **Host** > **Network Reading** > **Read Throughput Rate** y compruebe si el umbral de alarma está ajustado correctamente. (Por defecto, 80% es un valor apropiado. Sin embargo, los usuarios pueden configurar el valor según sea necesario.)

- En caso afirmativo, vaya a **Paso 2**.
- Si no, vaya a **Paso 4**.

Paso 2 En función de la condición de uso real, elija **O&M > Alarm** > **Thresholds** > *Name of the desired cluster* > **Host** > **Network Reading** > **Read Throughput Rate** y haga clic en **Modify** en la columna **Operation** para modificar el umbral de alarma.

Para obtener más información, consulte **Figura 9-9**.

Figura 9-9 Establecer umbrales de alarma



Paso 3 Espere 5 minutos y compruebe si la alarma está desactivada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 4**.

Compruebe si la velocidad del puerto de red puede cumplir con los requisitos del servicio.

Paso 4 En el Administrador de FusionInsight, haga clic en ⌄ en la fila donde se encuentra la alarma en la lista de alarmas en tiempo real y obtenga la dirección IP del host y el nombre del puerto de red para el que se genera la alarma.

Paso 5 Inicie sesión en el host para el que se genera la alarma como usuario **root**.

Paso 6 Ejecute el comando **ethtool** *network port name* para comprobar la velocidad máxima del puerto de red actual.

NOTA

En el entorno de VM, no puede ejecutar un comando para consultar la velocidad de puerto de red. Se recomienda que se ponga en contacto con el administrador del sistema para confirmar si la velocidad de puerto de red cumple los requisitos.

Paso 7 Si la tasa de rendimiento de lectura de red excede el umbral, póngase en contacto con el administrador del sistema para aumentar la tasa de puerto de red.

Paso 8 Verifique si la alarma se ha borrado.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 9**.

Recopilar información de fallas.

Paso 9 En la página principal del FusionInsight Manager del clúster activo, elija **O&M** > **Log** > **Download**.

Paso 10 Seleccione **OMS** en el **Service** y haga clic en **OK**.

Paso 11 Establezca **Host** en el nodo para el que se genera la alarma y en el nodo OMS activo.

Paso 12 Haga clic en  en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 30 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 13 Póngase en contacto con el y envíe la información de registro recopilada.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.30 ALM-12050 La tasa de rendimiento de escritura en red supera el umbral

Descripción

El sistema comprueba la tasa de rendimiento de escritura de red cada 30 segundos y compara la tasa de rendimiento real con el umbral (el umbral predeterminado es 80%). Esta alarma se genera cuando el sistema detecta que la tasa de rendimiento de escritura de red excede el umbral varias veces (5 veces por defecto) consecutivamente.

Para cambiar el umbral, elija **O&M > Alarm** > **Thresholds** > *Name of the desired cluster* > **Host** > **Network Writing** > **Write Throughput Rate**.

Cuando el **Trigger Count** es 1, esta alarma se borra cuando la tasa de rendimiento de escritura de red es menor o igual que el umbral. Cuando el **Trigger Count** es mayor que 1, esta alarma se borra cuando la tasa de rendimiento de escritura de red es menor o igual al 90% del umbral.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
12050	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster o sistema para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
NetworkCardName	Especifica el puerto de red para el que se genera la alarma.
Trigger Condition	Especifica el umbral que activa la alarma. Si el valor del indicador actual excede este umbral, se genera la alarma.

Impacto en el sistema

El sistema de servicio se ejecuta incorrectamente o no está disponible.

Causas posibles

- El umbral de alarma se establece incorrectamente.
- La velocidad de puerto de red no puede cumplir los requisitos de servicio actuales.

Procedimiento

Comprobar si el umbral está configurado correctamente.

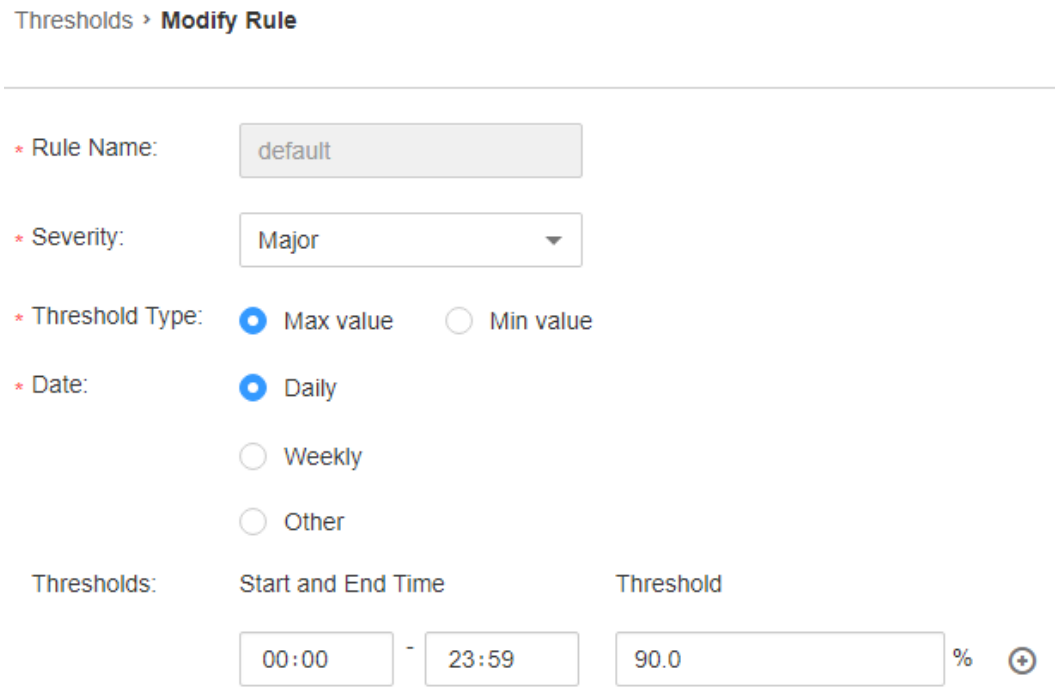
Paso 1 En el FusionInsight Manager, seleccione **O&M > Alarm** > **Thresholds** > *Name of the desired cluster* > **Host** > **Network Writing** > **Write Throughput Rate** y compruebe si el umbral de alarma está ajustado correctamente. (Por defecto, 80% es un valor apropiado. Sin embargo, los usuarios pueden configurar el valor según sea necesario.)

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 2**.

Paso 2 En función de la condición de uso real, elija **O&M > Alarm** > **Thresholds** > *Name of the desired cluster* > **Host** > **Network Writing** > **Write Throughput Rate** y haga clic en **Modify** en la columna **Operation** para modificar el umbral de alarma.

Para obtener más información, consulte **Figura 9-10**.

Figura 9-10 Establecer umbrales de alarma



Paso 3 Espere 5 minutos y compruebe si la alarma está desactivada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 4**.

Compruebe si la velocidad del puerto de red puede cumplir con los requisitos del servicio.

Paso 4 En el Administrador de FusionInsight, haga clic en ⌄ en la fila donde se encuentra la alarma en la lista de alarmas en tiempo real y obtenga la dirección IP del host y el nombre del puerto de red para el que se genera la alarma.

Paso 5 Inicie sesión en el host para el que se genera la alarma como usuario **root**.

Paso 6 Ejecute el comando **ethtool***network port name* para comprobar la velocidad máxima del puerto de red actual.

NOTA

En el entorno de VM, no puede ejecutar un comando para consultar la velocidad de puerto de red. Se recomienda que se ponga en contacto con el administrador del sistema para confirmar si la velocidad de puerto de red cumple los requisitos.

Paso 7 Si la tasa de rendimiento de escritura en red excede el umbral, póngase en contacto con el administrador del sistema para aumentar la tasa de puerto de red.

Paso 8 Verifique si la alarma se ha borrado.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 9**.

Recopilar información de fallas.

Paso 9 En la página principal del FusionInsight Manager del clúster activo, elija **O&M** > **Log** > **Download**.

Paso 10 Seleccione **OMS** en el **Service** y haga clic en **OK**.

Paso 11 Establezca **Host** en el nodo para el que se genera la alarma y en el nodo OMS activo.

Paso 12 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 30 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 13 Póngase en contacto con el y envíe la información de registro recopilada.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.31 ALM-12051 El uso de Inode de disco supera el umbral

Descripción

El sistema comprueba el uso del Inode del disco cada 30 segundos y compara el uso real del Inode con el umbral (el umbral predeterminado es 80%). Esta alarma se genera cuando el uso de Inode excede el umbral varias veces (5 veces por defecto) consecutivamente.

Para cambiar el umbral, elija **O&M > Alarm** > **Thresholds** > *Name of the desired cluster* > **Host** > **Disk** > **Disk Inode Usage**.

Cuando el **Trigger Count** es 1, esta alarma se borra cuando el uso del Inode del disco es menor o igual al umbral. Cuando el **Trigger Count** es mayor que 1, esta alarma se borra cuando el uso del Inode del disco es menor o igual al 90% del umbral.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
12051	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster o sistema para el que se genera la alarma.

Nombre	Significado
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
PartitionName	Especifica la partición de disco para la que se genera la alarma.
Trigger Condition	Especifica el umbral que activa la alarma. Si el valor del indicador actual excede este umbral, se genera la alarma.

Impacto en el sistema

Los datos no se pueden escribir correctamente en el sistema de archivos.

Causas posibles

En el disco se almacenan archivos masivos de pequeño tamaño.

Procedimiento

En el disco se almacenan archivos masivos de pequeño tamaño.

Paso 1 En FusionInsight Manager, elija **O&M > Alarm > Alarms** y haga clic en ⌄ en la fila donde se encuentra la alarma en la lista de alarmas en tiempo real y obtenga la dirección IP del host y la partición de disco para la que se genera la alarma.

Paso 2 Inicie sesión en el host para el que se genera la alarma como usuario **root**.

Paso 3 Ejecute el comando **df -i | grep -iE "***partition name*|Filesystem" para comprobar el uso actual del Inode del disco.

```
# df -i | grep -iE "xvda2|Filesystem"
Filesystem            Inodes   IUsed   IFree IUse% Mounted on
/dev/xvda2           2359296  207420 2151876    9% /
```

Paso 4 Si el uso de Inode supera el umbral, compruebe manualmente los archivos pequeños almacenados en la partición del disco y confirme si estos archivos pequeños se pueden eliminar.

NOTA

Ejecute el comando **for i in /*; do echo $i; find $i|wc -l; done** para consultar el número de archivos de una partición. Reemplace **/*** con la partición especificada.

```
# for i in /srv/*; do echo $i; find $i|wc -l; done
/srv/BigData
4284
/srv/ftp
1
/srv/www
13
```


- En caso afirmativo, ejecute el comando **rm -rf** *Path of the file or folder* para eliminar el archivo o la carpeta y vaya a **Paso 5**.

  NOTA

  Eliminar un archivo o carpeta es una operación de alto riesgo. Asegúrese de que el archivo o la carpeta ya no es necesario antes de realizar esta operación.

- Si no es así, expanda la capacidad. A continuación, realice **Paso 5**.

Paso 5 Espere 5 minutos y compruebe si la alarma está desactivada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 6**.

Recopilar información de fallas.

Paso 6 En la página principal del FusionInsight Manager del clúster activo, elija **O&M** > **Log** > **Download**.

Paso 7 Seleccione **OMS** en el **Service** y haga clic en **OK**.

Paso 8 Establezca **Host** en el nodo para el que se genera la alarma y en el nodo OMS activo.

Paso 9 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 30 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 10 Póngase en contacto con el y envíe la información de registro recopilada.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.32 ALM-12052 El uso de puerto temporal de TCP supera el umbral

Descripción

El sistema comprueba el uso temporal del puerto TCP cada 30 segundos y compara el uso real con el umbral (el umbral predeterminado es 80%). Esta alarma se genera cuando el uso del puerto temporal TCP excede el umbral varias veces (5 veces por defecto) consecutivamente.

Para cambiar el umbral, elija **O&M > Alarm** > **Thresholds** > *Name of the desired cluster* > **Host** > **Network Status** > **TCP Ephemeral Port Usage**.

Cuando el **Trigger Count** es 1, esta alarma se borra cuando el uso temporal del puerto TCP es menor o igual al umbral. Cuando el **Trigger Count** es mayor que 1, esta alarma se borra cuando el uso temporal del puerto TCP es menor o igual al 90% del umbral.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
12052	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster o sistema para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger Condition	Especifica el umbral que activa la alarma. Si el valor del indicador actual excede este umbral, se genera la alarma.

Impacto en el sistema

Los servicios en el host no pueden establecer conexiones externas y, por lo tanto, se interrumpen.

Causas posibles

- El puerto temporal no puede cumplir con los requisitos de servicio actuales.
- El sistema no funciona normalmente.

Procedimiento

Expandir el rango de número de puerto temporal.

Paso 1 En FusionInsight Manager, haga clic en ⌄ en la fila donde se encuentra la alarma en la lista de alarmas en tiempo real y obtenga la dirección IP del host para el que se genera la alarma.

Paso 2 Inicie sesión en el host para el que se genera la alarma como usuario **omm**.

Paso 3 Ejecute el comando **cat /proc/sys/net/ipv4/ip_local_port_range |cut -f 1** para obtener el valor del puerto de inicio y ejecute el comando **cat /proc/sys/net/ipv4/ip_local_port_range | cut -f 2** para obtener el valor del puerto final. El número total de puertos temporales es el valor del puerto final menos el valor del puerto inicial. Si el número total de puertos temporales es menor de 28,232, el rango de puertos aleatorios del sistema operativo es estrecho. Póngase en contacto con el administrador del sistema para aumentar el rango de puertos.

Paso 4 Ejecute el comando **ss -ant 2>/dev/null | grep -v LISTEN | awk 'NR > 2 {print $4}'|cut -d ':' -f 2 | awk '$1 >"***Value of the start port***" {print $1}' | sort -u | wc -l** para calcular el número de puertos temporales usados.

Paso 5 La fórmula para calcular el uso de los puertos temporales es: Uso de los puertos temporales = (Número de puertos temporales usados/Número total de puertos temporales) x 100%. Compruebe si el uso temporal del puerto excede el umbral.

- En caso afirmativo, vaya a **Paso 7**.
- Si no, vaya a **Paso 6**.

Paso 6 Espere 5 minutos y compruebe si la alarma está desactivada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 7**.

Comprobar si el entorno del sistema es anormal.

Paso 7 Ejecute el siguiente comando para importar el archivo temporal y ver los puertos más utilizados en **port_result.txt file**:

netstat -tnp|sort > $BIGDATA_HOME/tmp/port_result.txt

```
netstat -tnp|sort

Active Internet connections (w/o servers)

Proto Recv Send LocalAddress ForeignAddress State PID/ProgramName tcp   0   0
10-120-85-154:45433  10-120-85-154:9866 CLOSE_WAIT 94237/java
tcp   0   0 10-120-85-154:45434  10-120-85-154:9866 CLOSE_WAIT 94237/java
tcp   0   0 10-120-85-154:45435  10-120-85-154:9866 CLOSE_WAIT 94237/java
...
```

Paso 8 Ejecute el siguiente comando para ver los procesos que ocupan un gran número de puertos:

ps -ef |grep *PID*

NOTA

- PID es el ID de procesos consultados en **Paso 7**.
- Ejecute el siguiente comando para recopilar información sobre todos los procesos y comprobar los procesos que ocupan un gran número de puertos:

  ps -ef > $BIGDATA_HOME/tmp/ps_result.txt

Paso 9 Después de obtener la aprobación del administrador, borre los procesos que ocupan un gran número de puertos. Espere 5 minutos y compruebe si la alarma está desactivada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 10**.

Recopilar información de fallas.

Paso 10 En la página principal del FusionInsight Manager del clúster activo, elija **O&M** > **Log** > **Download**.

Paso 11 Seleccione **OMS** en el **Service** y haga clic en **OK**.

Paso 12 Establezca **Host** en el nodo para el que se genera la alarma y en el nodo OMS activo.

Paso 13 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 30 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 14 Póngase en contacto con el y envíe la información de registro recopilada y archivos **port_result.txt** y **ps_result.txt**. A continuación, elimine los dos archivos temporales residuales del entorno.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.33 ALM-12053 El uso del handle de archivos del host supera el umbral

Descripción

El sistema comprueba el uso del handle de archivos cada 30 segundos y compara el uso real con el umbral (el umbral predeterminado es 80%). Esta alarma se genera cuando el uso del handle de archivo del host excede el umbral varias veces (5 veces por defecto) consecutivamente.

Para cambiar el umbral, elija **O&M > Alarm** > **Thresholds** > *Name of the desired cluster* > **Host** > **Host Status** > **Host File Handle Usage**.

Cuando el **Trigger Count** es 1, esta alarma se borra cuando el uso del handle del archivo de host es menor o igual que el umbral. Cuando el **Trigger Count** es mayor que 1, esta alarma se borra cuando el uso del handle del archivo de host es menor o igual al 90% del umbral.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
12053	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster o sistema para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.

Nombre	Significado
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger Condition	Especifica el umbral que activa la alarma. Si el valor del indicador actual excede este umbral, se genera la alarma.

Impacto en el sistema

Las operaciones de E/S, como abrir un archivo o conectarse a la red, no se pueden realizar y los programas son anormales.

Causas posibles

- El proceso de solicitud es anormal. Por ejemplo, el archivo abierto o el socket no está cerrado.
- El número de handles de archivo no puede cumplir los requisitos de servicio actuales.
- El sistema no funciona normalmente.

Procedimiento

Verificar información sobre archivos abiertos en procesos.

Paso 1 En FusionInsight Manager, haga clic en ⌄ en la fila donde se encuentra la alarma en la lista de alarmas en tiempo real y obtenga la dirección IP del host para el que se genera la alarma.

Paso 2 Inicie sesión en el host para el que se genera la alarma como usuario **root**.

Paso 3 Ejecute el comando **lsof -n|awk '{print $2}'|sort|uniq -c|sort -nr|more** para comprobar el proceso que ocupa demasiados handles de archivo.

Paso 4 Compruebe si los procesos en los que se abren un gran número de archivos son normales. Por ejemplo, compruebe si hay archivos o sockets no cerrados.

- En caso afirmativo, vaya a **Paso 5**.
- Si no, vaya a **Paso 7**.

Paso 5 Libere los procesos anormales que ocupan demasiados handles de archivo.

Paso 6 Cinco minutos más tarde, compruebe si la alarma está borrada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 7**.

Aumentar el número de handles de archivo.

Paso 7 En FusionInsight Manager, haga clic en ⌄ en la fila donde se encuentra la alarma en la lista de alarmas en tiempo real y obtenga la dirección IP del host para el que se genera la alarma.

Paso 8 Inicie sesión en el host para el que se genera la alarma como usuario **root**.

Paso 9 Póngase en contacto con el administrador del sistema para aumentar el número de handles de archivo del sistema.

Paso 10 Ejecute el comando **cat /proc/sys/fs/file-nr** para ver los handles usados y el número máximo de handles de archivo. El primer valor es el número de handles usados, el tercer valor es el número máximo. Compruebe si el uso excede el umbral.

- En caso afirmativo, vaya a **Paso 9**.
- Si no, vaya a **Paso 11**.

```
# cat /proc/sys/fs/file-nr
12704 0 640000
```

Paso 11 Espere 5 minutos y compruebe si la alarma está desactivada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 12**.

Comprobar si el entorno del sistema es anormal.

Paso 12 Póngase en contacto con el administrador del sistema para comprobar si el sistema operativo es anormal.

- En caso afirmativo, vaya a **Paso 13** para rectificar la falla.
- Si no, vaya a **Paso 14**.

Paso 13 Espere 5 minutos y compruebe si la alarma está desactivada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 14**.

Recopilar información de fallas.

Paso 14 En la página principal del FusionInsight Manager del clúster activo, elija **O&M** > **Log** > **Download**.

Paso 15 Seleccione **OMS** en el **Service** y haga clic en **OK**.

Paso 16 Establezca **Host** en el nodo para el que se genera la alarma y en el nodo OMS activo.

Paso 17 Haga clic en  en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 30 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 18 Póngase en contacto con el y envíe la información de registro recopilada.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.34 ALM-12054 Archivo de certificado no válido

Descripción

El sistema comprueba si el archivo de certificado no es válido (ha caducado o aún no es válido) 23:00 cada día. Esta alarma se genera cuando el archivo de certificado no es válido.

Esta alarma se borra cuando se importa un certificado válido.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
12054	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster o sistema para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger Condition	Especifica el umbral para activar la alarma.

Impacto en el sistema

Algunas funciones no están disponibles.

Causas posibles

Sin certificado (certificado CA, certificado raíz HA, certificado de usuario HA, certificado raíz Gaussdb o certificado de usuario Gaussdb) se importa al sistema, el certificado no se importa o el archivo de certificado no es válido.

Procedimiento

Comprobar la causa de la alarma.

Paso 1 En FusionInsight Manager, localice la alarma de destino en la lista de alarmas en tiempo real y haga clic en .

Vea **Información adicional** para obtener información adicional sobre la alarma.

- Si se muestra **CA Certificate** en la información de alarma adicional, inicie sesión en el nodo de gestión de OMS activo como usuario **omm** y vaya a **Paso 2**.
- Si aparece **HA root Certificate** en la información adicional, vea **Location** para obtener el nombre del host involucrado en esta alarma. Luego, inicie sesión en el host como usuario **omm** y vaya a **Paso 3**.
- Si aparece **HA server Certificate** en la información adicional, vea **Location** para obtener el nombre del host involucrado en esta alarma. Luego, inicie sesión en el host como usuario **omm** y vaya a **Paso 4**.
- Si aparece **Certificate has expired** en la información adicional, vea **Location** para obtener el nombre del host para el que se genera la alarma. A continuación, inicie sesión en el host como usuario **omm** y realizar **Paso 2** a **Paso 4** en secuencia para comprobar si los certificados han caducado. Si estos certificados no han caducado, compruebe si se han importado otros certificados. Si es así, vuelva a importar los archivos de certificado.

Verificar el período de validez de los archivos del certificado en el sistema.

Paso 2 Compruebe si la hora actual del sistema está en el período de validez del certificado de CA.

Ejecute el comando **bash ${CONTROLLER_HOME}/security/cert/conf/querycertvalidity.sh** para comprobar el tiempo efectivo y el tiempo de vencimiento del certificado raíz de CA.

- En caso afirmativo, vaya a **Paso 7**.
- Si no, vaya a **Paso 5**.

Paso 3 Compruebe si la hora actual del sistema está en el período de validez del certificado raíz de HA.

Ejecute el comando **openssl x509 -noout -text -in ${CONTROLLER_HOME}/security/certHA/root-ca.crt** para comprobar el tiempo efectivo y el tiempo de vencimiento del certificado raíz HA.

- En caso afirmativo, vaya a **Paso 7**.
- Si no, vaya a **Paso 6**.

Paso 4 Compruebe si la hora actual del sistema está en el período de validez del certificado de usuario de HA.

Ejecute el comando **openssl x509 -noout -text -in ${CONTROLLER_HOME}/security/certHA/server.crt** para comprobar el tiempo efectivo y el tiempo de vencimiento del certificado de usuario HA.

- En caso afirmativo, vaya a **Paso 7**.
- Si no, vaya a **Paso 6**.

A continuación se muestra un ejemplo del tiempo efectivo y el tiempo de vencimiento de un certificado de CA o HA:

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            97:d5:0e:84:af:ec:34:d8
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=CN, ST=xxx, L=yyy, O=zzz, OU=IT, CN=HADOOP.COM
        Validity
```



```
            Not Before: Dec 13 06:38:26 2016 GMT            // Effective time
            Not After : Dec 11 06:38:26 2026 GMT            // Due time
```

Importar archivos de certificado.

Paso 5 Importar un nuevo archivo de certificado de CA.

Solicite o genere un nuevo archivo de certificado de CA e impórtelo al sistema. Para obtener más información, consulte **Sustitución del certificado de CA**. La alarma se borra automáticamente después de importar el certificado de CA. Compruebe si esta alarma se notifica de nuevo durante la comprobación periódica.

- En caso afirmativo, vaya a **Paso 7**.
- En caso negativo, no se requiere ninguna otra acción.

Paso 6 Importe un nuevo archivo de certificado HA.

Solicite o genere un nuevo archivo de certificado HA e impórtelo al sistema. Para obtener más información, consulte **Sustitución de certificados de HA**. La alarma se borra automáticamente después de importar el certificado de CA. Compruebe si esta alarma se notifica de nuevo durante la comprobación periódica.

- En caso afirmativo, vaya a **Paso 7**.
- En caso negativo, no se requiere ninguna otra acción.

Recopilar información de fallas.

Paso 7 En FusionInsight Manager, seleccione **O&M**. En el panel de navegación de la izquierda, elija **Log** > **Download**.

Paso 8 En el área **Services**, seleccione **Controller**, **OmmServer**, **OmmCore** y **Tomcat** y haga clic en **OK**.

Paso 9 Haga clic en  en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 10 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

Información relacionada

Para obtener más información sobre cómo gestionar un certificado OBS caducado, consulte **Certificado OBS en un clúster caducado**.

9.35 ALM-12055 El archivo de certificado está a punto de caducar

Descripción

El sistema comprueba el archivo de certificado el 23:00 todos los días. Esta alarma se genera si el archivo de certificado está a punto de caducar en un plazo de 30 días.

Esta alarma se borra cuando un certificado que no está a punto de caducar se importa.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
12055	Leves	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster o sistema para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger Condition	Especifica el umbral para activar la alarma.

Impacto en el sistema

Algunas funciones no están disponibles.

Causas posibles

El período de validez restante de un certificado del sistema (Certificado CA, certificado raíz HA, certificado de usuario HA, certificado raíz Gaussdb o certificado de usuario Gaussdb) es menos de 30 días.

Procedimiento

Comprobar la causa de la alarma.

Paso 1 En FusionInsight Manager, localice la alarma de destino en la lista de alarmas en tiempo real y haga clic en ⌄.

Vea **Información adicional** para obtener información adicional sobre la alarma.

- Si se muestra **CA Certificate** en la información de alarma adicional, inicie sesión en el nodo de gestión de OMS activo como usuario **omm** y vaya a **Paso 2**.
- Si aparece **HA root Certificate** en la información adicional, vea **Location** para obtener el nombre del host involucrado en esta alarma. Luego, inicie sesión en el host como usuario **omm** y vaya a **Paso 3**.
- Si aparece **HA server Certificate** en la información adicional, vea **Location** para obtener el nombre del host involucrado en esta alarma. Luego, inicie sesión en el host como usuario **omm** y vaya a **Paso 4**.

Verificar el período de validez de los archivos del certificado en el sistema.

Paso 2 Compruebe si el período de validez restante del certificado de CA es menor que el umbral de alarma.

Ejecute el comando **bash ${CONTROLLER_HOME}/security/cert/conf/querycertvalidity.sh** para comprobar el tiempo efectivo y el tiempo de vencimiento del certificado raíz de CA.

- En caso afirmativo, vaya a **Paso 5**.
- Si no, vaya a **Paso 7**.

Paso 3 Compruebe si el período de validez restante del certificado raíz de HA es menor que el umbral de alarma.

Ejecute el comando **openssl x509 -noout -text -in ${CONTROLLER_HOME}/security/certHA/root-ca.crt** para comprobar el tiempo efectivo y el tiempo de vencimiento del certificado raíz HA.

- En caso afirmativo, vaya a **Paso 6**.
- Si no, vaya a **Paso 7**.

Paso 4 Compruebe si el período de validez restante del certificado de usuario de HA es menor que el umbral de alarma.

Ejecute el comando **openssl x509 -noout -text -in ${CONTROLLER_HOME}/security/certHA/server.crt** para comprobar el tiempo efectivo y el tiempo de vencimiento del certificado de usuario HA.

- En caso afirmativo, vaya a **Paso 6**.
- Si no, vaya a **Paso 7**.

A continuación se muestra un ejemplo del tiempo efectivo y el tiempo de vencimiento de un certificado de CA o HA:

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            97:d5:0e:84:af:ec:34:d8
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=CN, ST=xxx, L=yyy, O=zzz, OU=IT, CN=HADOOP.COM
        Validity
            Not Before: Dec 13 06:38:26 2016 GMT            // Effective time
            Not After : Dec 11 06:38:26 2026 GMT            // Due time
```


Importar archivos de certificado.

Paso 5 Importar un nuevo archivo de certificado de CA.

Solicite o genere un nuevo archivo de certificado de CA e impórtelo al sistema. Para obtener más información, consulte **Sustitución del certificado de CA**. Borre manualmente la alarma y compruebe si esta alarma se genera de nuevo durante la comprobación periódica.

- En caso afirmativo, vaya a **Paso 7**.
- En caso negativo, no se requiere ninguna otra acción.

Paso 6 Importe un nuevo archivo de certificado HA.

Solicite o genere un nuevo archivo de certificado HA e impórtelo al sistema. Para obtener más información, consulte **Sustitución de certificados de HA**. Borre manualmente la alarma y compruebe si esta alarma se genera de nuevo durante la comprobación periódica.

- En caso afirmativo, vaya a **Paso 7**.
- En caso negativo, no se requiere ninguna otra acción.

Recopilar información de fallas.

Paso 7 En FusionInsight Manager, seleccione **O&M**. En el panel de navegación de la izquierda, elija **Log** > **Download**.

Paso 8 En el área **Services**, seleccione **Controller**, **OmmServer**, **OmmCore** y **Tomcat** y haga clic en **OK**.

Paso 9 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 10 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

Información relacionada

Ninguna

9.36 ALM-12057 Metadatos no configurados con la tarea de realizar una copia de respaldo periódica de datos en un servidor de terceros

Descripción

Después de instalar el sistema, comprueba si la tarea para realizar copias de respaldo de metadatos periódicamente en el servidor de terceros y, a continuación, realiza la comprobación cada hora. Si no se configura la tarea para realizar copias de respaldo de metadatos periódicamente en un servidor de terceros, se genera una alarma crítica.

Esta alarma se borra cuando un usuario crea tal tarea de copia de respaldo.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
12057	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster o sistema para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

Si no se realiza una copia de respaldo de los metadatos en un servidor de terceros, los metadatos no se pueden restaurar si los nodos de gestión activo y en espera del clúster son defectuosos y se pierden los datos de copia de respaldo locales.

Causas posibles

Los metadatos no se configuran con la tarea de realizar periódicamente copias de respaldo de los datos en un servidor de terceros.

Procedimiento

Paso 1 En el portal del FusionInsight Manager, seleccione **O&M > Alarm > Alarms**.

Paso 2 En la lista de alarmas, haga clic en ⌄ en la fila donde se encuentra la alarma e identifique el módulo de datos a partir del cual se genera la alarma basándose en el archivo **Additional Information**.

Paso 3 Elija **O&M** >**Backup and Restoration > Backup Management** >**Create**.

Paso 4 Configurar una tarea de copia de respaldo. Los datos de copia de respaldo que se van a configurar son consistentes con los datos de Información Adicional de la alarma.

Realice copias de respaldo de los datos en un servidor de terceros, por ejemplo, HDFS remotos (RemoteHDFS), NAS (NFS/CIFS), Object Storage Service (OBS) y servidor SFTP (SFTP). Para obtener más información, consulte **Copia de respaldo de datos**.

Paso 5 Después de que la tarea de copia de respaldo se haya creado correctamente, espere dos minutos y compruebe si la alarma está borrada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 6**.

Recopilar información de fallas

Paso 6 En FusionInsight Manager, elija **O&M** > **Log > Download**.

Paso 7 En el área **Service**, seleccione **Controller** y haga clic en **OK**.

Paso 8 Haga clic en  en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 9 Póngase en contacto con el y envíe la información de registro recopilada.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.37 ALM-12061 El uso del proceso supera el umbral

Descripción

El sistema comprueba el uso del proceso omm cada 30 segundos. Los usuarios pueden ejecutar el comando **ps -o nlwp, pid, args, -u omm | awk '{sum+=$1} END {print "", sum}'** para obtener el número de procesos simultáneos de **omm** de usuario. Ejecute el comando **ulimit -u** para obtener el máximo número de procesos que puede abrir simultáneamente el **omm** de usuario. Dividir el número de procesos simultáneos por el número máximo para obtener el uso de procesos de **omm** de usuario. El uso del proceso tiene un umbral predeterminado. Esta alarma se genera cuando el uso del proceso excede el umbral.

Si **Trigger Count** es **3** y el uso del proceso es menor o igual que el umbral, esta alarma se borra. Si **Trigger Count** es mayor que **1** y el uso del proceso es menor o igual al 90% del umbral, esta alarma se borra.

Atributo

ID de alarma	Gravedad de la alarma	Borrado automático
12061	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster o sistema para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger Condition	Especifica el umbral para activar la alarma.

Impacto en el sistema

- El cambio al **omm** de usuario falla.
- No se puede crear un nuevo proceso de omm.

Causas posibles

- El umbral de alarma está configurado incorrectamente.
- El número máximo de procesos (incluidos los subprocesos) que puede abrir simultáneamente el usuario **omm** es inapropiado.
- Un número excesivo de subprocesos se abren al mismo tiempo.

Procedimiento

Compruebe si el umbral de alarma o el número de aciertos de alarma están configurados correctamente.

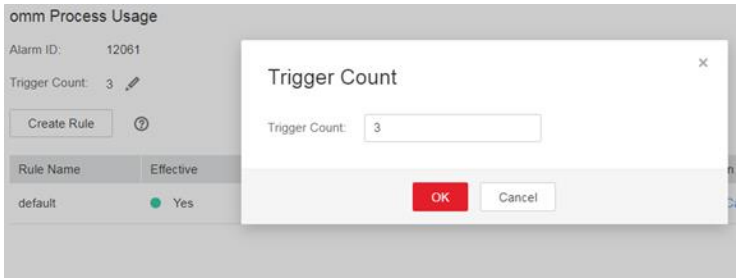
Paso 1 En el FusionInsight Manager, cambie el umbral de alarma y **Trigger Count** según el uso real de la CPU.

Específicamente, elija **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster* > **Host**> **Process** > **omm Process Usage** para cambiar Trigger Count, como se muestra en **Figura 9-11**.

NOTA

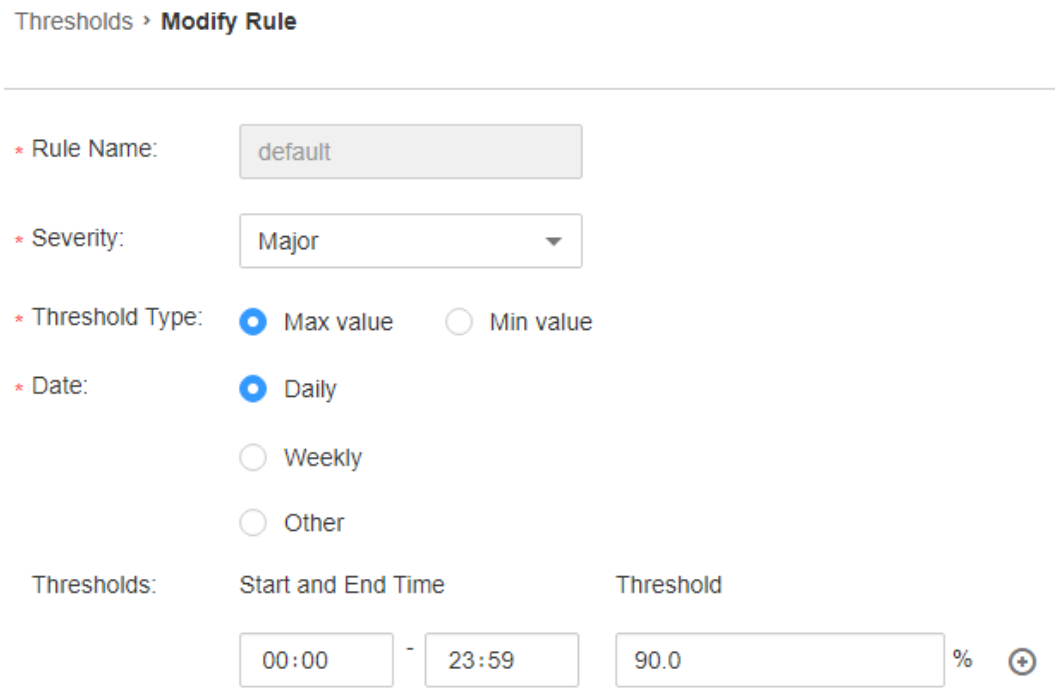
La alarma se genera cuando el uso del proceso excede el umbral para los tiempos especificados por **Trigger Count**.

Figura 9-11 Configuración de Trigger Count



Establezca el umbral de alarma basado en el uso real del proceso. Para comprobar el uso del proceso, elija **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster* > **Host**> **Process** > **omm Process Usage**, como se muestra en **Figura 9-12**.

Figura 9-12 Establecer un umbral de alarma



Paso 2 2 minutos más tarde, compruebe si la alarma está desactivada.

- Si lo es, no se requiere ninguna otra acción.
- Si no es así, vaya a **Paso 3**.

Compruebe si el número máximo de procesos (incluidos los subprocesos) abiertos por el usuario omm es adecuado.

Paso 3 En la lista de alarmas del FusionInsight Manager, localice la fila que contiene la alarma y vea la dirección IP del host para el que se genera la alarma.

Paso 4 Inicie sesión en el host donde se genera la alarma como usuario **root**.

Paso 5 Ejecute el comando **su - omm** para cambiar a usuario **omm**.

Paso 6 Ejecute el comando **ulimit -u** para obtener el número máximo de subprocesos que puede abrir el usuario **omm** y compruebe si el número es mayor o igual a 60000.

- Si lo es, vaya a **Paso 8**.
- Si no es así, vaya a **Paso 7**.

Paso 7 Ejecute el comando **ulimit -u 60000** para cambiar el número máximo a 60000. Dos minutos más tarde, compruebe si la alarma está desactivada.

- Si lo es, no se requiere ninguna otra acción.
- Si no es así, vaya a **Paso 12**.

Compruebe si se abre un número excesivo de procesos al mismo tiempo.

Paso 8 En la lista de alarmas del FusionInsight Manager, localice la fila que contiene la alarma y vea la dirección IP del host para el que se genera la alarma.

Paso 9 Inicie sesión en el host donde se genera la alarma como usuario **root**.

Paso 10 Ejecute el comando **ps -o nlwp, pid, lwp, args, -u omm|sort -n** para comprobar el número de subprocesos utilizados por el sistema. El resultado se ordena en función del número de subproceso. Analice los 5 números principales de subprocesos y verifique si los subprocesos se utilizan incorrectamente. Si lo son, póngase en contacto con el personal de mantenimiento para rectificar la falla. Si no lo son, ejecute el comando **ulimit -u** para cambiar el número máximo para que sea mayor de 60000.

Paso 11 Cinco minutos más tarde, compruebe si la alarma está borrada.

- Si lo es, no se requiere ninguna otra acción.
- Si no es así, vaya a **Paso 12**.

Recopilar información de fallas.

Paso 12 En la página de inicio del Administrador FusionInsight de los clústeres activos, seleccione **O&M** > **Log** > **Download**.

Paso 13 Seleccione **OmmServer** y **NodeAgent** en el **Service** y haga clic en **OK**.

Paso 14 Haga clic en  en la esquina superior derecha. En el cuadro de diálogo que se muestra, establezca **Start Date** y **End Date** en 10 minutos antes y después del tiempo de generación de alarmas respectivamente y haga clic en **OK**. A continuación, haga clic en **Download**.

Paso 15 Póngase en contacto con el y envíe la información de registro recopilada.

----Fin

Eliminación de alarmas

Esta alarma se borrará automáticamente después de que se corrija la falla.

Información relacionada

Ninguna

9.38 ALM-12062 Las configuraciones del parámetro OMS no coinciden con la escala del clúster

Descripción

El sistema comprueba si las configuraciones de los parámetros de OMS coinciden con la escala del clúster en cada hora superior. Si las configuraciones de parámetros de OMS no cumplen los requisitos de escala de clúster, el sistema genera esta alarma. Esta alarma se borra automáticamente cuando se modifican las configuraciones del parámetro OMS.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
12062	Importante	Sí

Parámetros

Parámetro	Descripción
Source	Especifica el clúster o sistema para el que se genera la alarma.
ServiceName	Especifica el nombre del servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

La configuración de OMS no se modifica cuando se instala el clúster o se expande la capacidad del sistema.

Causas posibles

Las configuraciones de los parámetros de OMS no coinciden con la escala del clúster.

Procedimiento

Comprobar si las configuraciones de los parámetros de OMS coinciden con la escala del clúster.

Paso 1 En la lista de alarmas del FusionInsight Manager, localice la fila que contiene la alarma y vea la dirección IP del host para el que se genera la alarma.

Paso 2 Inicie sesión en el host donde se genera la alarma como usuario **root**.

Paso 3 Ejecute el comando **su - omm** para cambiar a usuario **omm**.

Paso 4 Ejecute el comando **vi $BIGDATA_LOG_HOME/controller/scriptlog/modify_manager_param.log** para abrir el archivo de registro y buscar el archivo de registro que contiene la siguiente información: Las configuraciones actuales de oms no pueden admitir nodos de *xx*. En la información, *xx* indica el número de nodos en el clúster.

Paso 5 Optimice la configuración de clúster actual siguiendo las instrucciones en **Optimización de configuraciones de Manager basadas en el número de nodos de clúster**.

Paso 6 Una hora más tarde, compruebe si la alarma está desactivada.

- Si lo es, no se requiere ninguna otra acción.
- Si no es así, vaya a **Paso 7**.

Recopilar información de fallas.

Paso 7 En FusionInsight Manager, elija **O&M** > **Log** > **Download**.

Paso 8 Seleccione **Controller** en el **Service** y haga clic en **OK**.

Paso 9 Haga clic en  en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 10 Póngase en contacto con el y envíe la información de registro recopilada.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Optimización de las configuraciones del administrador en función del número de nodos del clúster

Paso 1 Inicie sesión en el nodo de administrador activo como usuario **omm**.

Paso 2 Ejecute el siguiente comando para cambiar el directorio:

cd ${BIGDATA_HOME}/om-server/om/sbin

Paso 3 Ejecute el siguiente comando para ver las configuraciones actuales de Manager.

sh oms_config_info.sh -q

Paso 4 Ejecute el siguiente comando para especificar el número de nodos en el clúster actual.

Formato de comando: **sh oms_config_info.sh -s** *number of nodes*

Ejemplo:

sh oms_config_info.sh -s 1000

Escriba **y** como se le solicite.

```
The following configurations will be modified:
     Module       Parameter         Current          Target
     Controller   controller.Xmx    4096m        =>  16384m
     Controller   controller.Xms    1024m        =>  8192m
     Controller   controller.node.heartbeat.error.threshold
30000                       =>   60000
     Pms          pms.mem           8192m        =>  10240m
Do you really want to do this operation? (y/n):
```

Las configuraciones se actualizan correctamente si se muestra la siguiente información:

```
...
Operation has been completed. Now restarting OMS server.                  [done]
Restarted oms server successfully.
```


NOTA

- OMS se reinicia automáticamente durante el proceso de actualización de la configuración.
- Los clústeres con cantidades similares de nodos tienen las mismas configuraciones de Manager. Por ejemplo, cuando el número de nodos se cambia de 100 a 101, no es necesario actualizar ningún elemento de configuración.

----Fin

9.39 ALM-12063 Disco no disponible

Descripción

El sistema comprueba si el disco de datos del host actual está disponible en la parte superior de cada hora. El sistema crea archivos, escribe archivos y elimina archivos en el directorio de montaje del disco. Si las operaciones fallan, se genera la alarma. Si las operaciones tienen éxito, el disco está disponible y la alarma se borra.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
12063	Importante	Sí

Parámetros

Parámetro	Descripción
Source	Especifica el clúster o sistema para el que se genera la alarma.
ServiceName	Especifica el nombre del servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
DiskName	Especifica el disco para el que se genera la alarma.

Impacto en el sistema

La lectura o escritura de datos en el disco de datos falla y los servicios son anormales.

Causas posibles

- El permiso del directorio de montaje en disco es anormal.
- Hay sectores defectuosos de disco.

Procedimiento

Comprobar si el permiso del directorio de montaje del disco es normal.

Paso 1 En la lista de alarmas del FusionInsight Manager, localice la fila que contiene la alarma y vea la dirección IP del host y **DiskName** del disco para el que se genera la alarma.

Paso 2 Inicie sesión en el host donde se genera la alarma como usuario **root**.

Paso 3 Ejecute el comando **df -h |grep DiskName** para obtener el punto de montaje y compruebe si el permiso del directorio de montaje es inescribible o ilegible.

- Si lo es, vaya a **Paso 4**.
- Si no es así, vaya a **Paso 8**.

NOTA

Si el permiso del directorio de montaje es 000 o el propietario es **root**, el directorio de montaje es ilegible e inescribible.

Paso 4 Modifique el permiso de directorio.

Paso 5 Una hora más tarde, compruebe si esta alarma está desactivada.

- Si lo es, no se requiere ninguna otra acción.
- Si no es así, vaya a **Paso 6**.

Paso 6 Póngase en contacto con los ingenieros de hardware para rectificar el disco.

Paso 7 Una hora más tarde, compruebe si esta alarma está desactivada.

- Si lo es, no se requiere ninguna otra acción.
- Si no es así, vaya a **Paso 8**.

Recopilar información de fallas.

Paso 8 En FusionInsight Manager, elija **O&M** > **Log** > **Download**.

Paso 9 Seleccione **NodeAgent** en el **Service** y haga clic en **OK**.

Paso 10 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 11 Póngase en contacto con el y envíe la información de registro recopilada.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.40 ALM-12064 Conflictos de rango de puertos aleatorios del host con el puerto utilizado del clúster

Descripción de la alarma

El sistema comprueba si el rango de puertos aleatorios del host entra en conflicto con el rango de puertos utilizado por el sistema de clúster cada hora. La alarma se genera si entran en conflicto. La alarma se borra automáticamente cuando el rango de puertos aleatorios del host se cambia al rango normal.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
12064	Importante	Sí

Parámetros

Parámetro	Descripción
Source	Especifica el sistema o clúster para el que se ha generado el mismo.
ServiceName	Especifica el nombre del servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

El puerto predeterminado del sistema de clúster está ocupado. Como resultado, algunos procesos no pueden iniciarse.

Causas posibles

Se modifica la configuración de rango de puertos aleatorios.

Procedimiento

Verifique el rango de puertos aleatorios del sistema.

Paso 1 En la lista de alarmas del FusionInsight Manager, localice la fila que contiene la alarma y vea la dirección IP del host para el que se genera la alarma.

Paso 2 Inicie sesión en el host donde se genera la alarma como usuario **root**.

Paso 3 Ejecute el comando **cat /proc/sys/net/ipv4/ip_local_port_range** para obtener el rango de puertos aleatorios del host y verifique si el valor mínimo es menor que 32768.

- Si lo es, vaya a **Paso 4**.
- Si no lo es, vaya a **Paso 7**.

Paso 4 Ejecute el comando **vim /etc/sysctl.conf** para cambiar el valor de **net.ipv4.ip_local_port_range** a **32768 61000**. Si este parámetro no existe, agregue la siguiente configuración **net.ipv4.ip_local_port_range = 32768 61000**.

Paso 5 Ejecute el comando **sysctl -p /etc/sysctl.conf** para que la modificación surta efecto.

Paso 6 Una hora más tarde, compruebe si la alarma está desactivada.

- Si lo es, no se requiere ninguna otra acción.
- Si no es así, vaya a **Paso 7**.

Recopilar información de fallas.

Paso 7 En FusionInsight Manager, elija **O&M** > **Log** > **Download**.

Paso 8 Seleccione **NodeAgent** para **Service** y haga clic en **OK**.

Paso 9 Haga clic en  en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 10 Póngase en contacto con el y envíe la información de registro recopilada.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.41 ALM-12066 Las relaciones de confianza entre nodos se vuelven inválidas

Descripción

El sistema comprueba si la relación de confianza entre el nodo OMS activo y otros nodos de Agente es normal cada hora. La alarma se genera si falla la confianza mutua. Esta alarma se borra automáticamente si se resuelve este problema.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
12066	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster o sistema para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

Algunas operaciones en el plano de gestión pueden ser anormales.

Causas posibles

- El archivo de configuración **/etc/ssh/sshd_config** está dañado.
- La contraseña del usuario **omm** ha caducado.

Procedimiento

Comprobar el estado del archivo de configuración /etc/ssh/sshd_config.

Paso 1 En la lista de alarmas del FusionInsight Manager, localice la fila que contiene la alarma y haga clic en ⌄ para ver la lista de hosts en los detalles de la alarma.

Paso 2 Inicie sesión en el nodo OMS activo como usuario **omm**.

Paso 3 Ejecute el comando **ssh**, por ejemplo, **ssh *host2*** en cada nodo de los detalles de la alarma para comprobar si la conexión falla. (***host2*** es un nodo distinto del nodo OMS en los detalles de la alarma.)

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 6**.

Paso 4 Abra el archivo de configuración **/etc/ssh/sshd_config** en host2 y compruebe si **AllowUsers** o **DenyUsers** están configurados para otros nodos.

- En caso afirmativo, vaya a **Paso 5**.
- Si no, póngase en contacto con expertos en sistemas operativos.

Paso 5 Modifique la lista blanca o la lista negra para asegurarse de que el usuario **omm** esté en la lista blanca o no en la lista negra. Verifique si la alarma se ha borrado.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 6**.

Verificar el estado de la contraseña del usuario omm.

Paso 6 Compruebe la información de interacción del comando **ssh**.

- Si se requiere la contraseña del **omm** de usuario, vaya a **Paso 7**.
- Si aparece el mensaje "Enter passphrase for key '/home/omm/.ssh/id_rsa':", vaya a **Paso 9**.

Paso 7 Compruebe la lista de confianza (**/home/omm/.ssh/authorized_keys**) del usuario **omm** en el nodo OMS y el nodo host2. Compruebe si la lista de confianza contiene el archivo de clave pública (**/home/omm/.ssh/id_rsa.pub**) del usuario **omm** en el host del mismo nivel.

- En caso afirmativo, póngase en contacto con expertos en sistemas operativos.
- Si no, agregue la clave pública del usuario **omm** del host del mismo nivel a la lista de confianza del host local.

Paso 8 Agregue la clave pública del usuario **omm** del host del mismo nivel a la lista de confianza del host local. Ejecute el comando **ssh**, por ejemplo, **ssh host2** en cada nodo de los detalles de la alarma para comprobar si la conexión falla. (***host2*** es un nodo distinto del nodo OMS en los detalles de la alarma.)

- En caso afirmativo, vaya a **Paso 9**.
- Si no, compruebe si la alarma está desactivada. Si la alarma está desactivada, no se requiere ninguna otra acción; de lo contrario, vaya a **Paso 9**.

Recopilar información de fallas.

Paso 9 En FusionInsight Manager, seleccione **O&M**. En el panel de navegación de la izquierda, elija **Log** > **Download**.

Paso 10 Seleccione **Controller** para **Service** y haga clic en **OK**.

Paso 11 Haga clic en  en la esquina superior derecha para establecer el intervalo de tiempo de recopilación de registros. Generalmente, el intervalo de tiempo es de 10 minutos antes y después del tiempo de generación de alarma. Haga clic en **Download**.

Paso 12 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

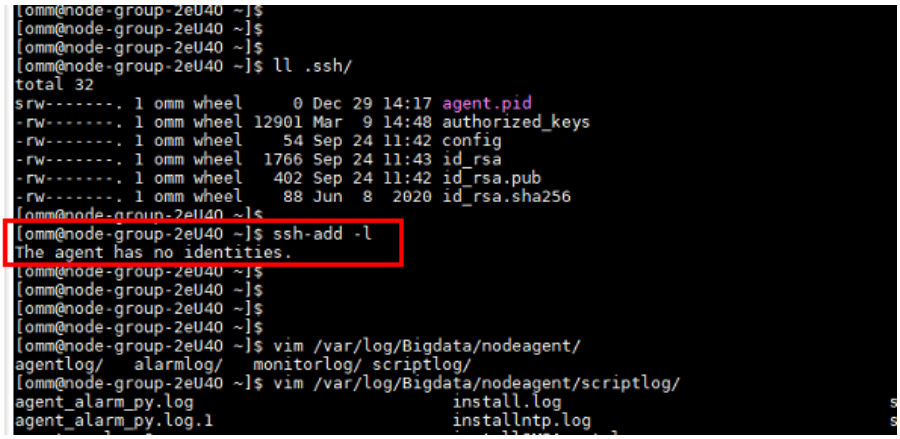
Información relacionada

Realice los siguientes pasos para controlar las relaciones de confianza anormales entre nodos:

AVISO

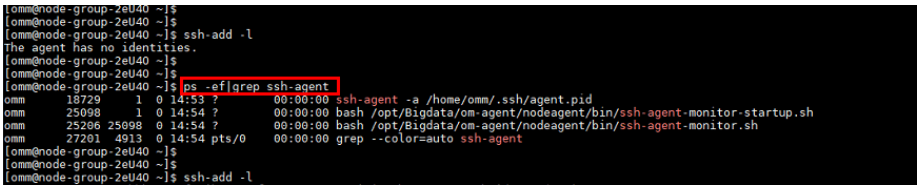
- Realice esta operación como usuario **omm**.
- Si la red entre nodos está desconectada, rectifique primero la falla de red. Compruebe si los dos nodos están conectados al mismo grupo de seguridad y si **hosts.deny** y **hosts.allow** están configurados.

1. Ejecute el comando **ssh-add -l** en ambos nodos para comprobar si existen identidades.

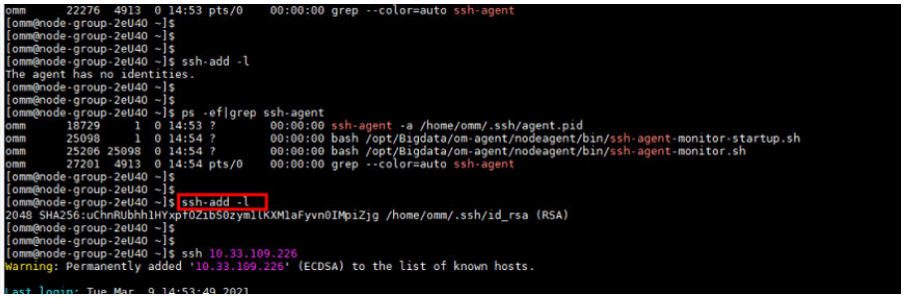


   – En caso afirmativo, vaya a **4**.
   – Si no, vaya a **2**.

2. Si no se muestra ninguna identidad, ejecute el comando **ps -ef|grep ssh-agent** para encontrar el proceso **ssh-agent** y esperar a que el proceso se reinicie automáticamente.



3. Ejecute el comando **ssh-add -l** para comprobar si se han agregado las identidades. En caso afirmativo, ejecute manualmente el comando **ssh** para comprobar si la relación de confianza es normal.



4. Si existen identidades, compruebe si el archivo **/home/omm/.ssh/authorized_keys** contiene la información en el archivo **/home/omm/.ssh/id_rsa.pub** del nodo par. Si no es así, agregue manualmente la información.
5. Compruebe si se modifican los permisos de los archivos del directorio **/home/omm/.ssh**.
6. Compruebe el archivo **/var/log/Bigdata/nodeagent/scriptlog/ssh-agent-monitor.log**.

7. Si se elimina el directorio **/home** del usuario **omm**, póngase en contacto con el personal de soporte de MRS para obtener ayuda.

9.42 ALM-12067 Tomcat Resource es anormal

Descripción

HA comprueba los recursos de Tomcat de Manager cada 85 segundos. Esta alarma se genera cuando HA detecta que los recursos de Tomcat son anormales durante dos veces consecutivas.

Esta alarma se borra cuando HA detecta que los recursos Tomcat se vuelven normales.

Resource Type de Tomcat es **Single-active**. Activo/en espera se activará en caso de excepciones de recursos. Cuando se genera esta alarma, se completa la conmutación activa/en espera y se han habilitado nuevos recursos de Tomcat en el nuevo Manager activo. En este caso, esta alarma se borra. Esta alarma se utiliza para notificar a los usuarios de la causa de la conmutación del Manager activo/en espera.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
12067	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster o sistema para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

- Se produce el cambio de Manager activo/en espera.
- El proceso Tomcat se reinicia repetidamente.

Causas posibles

- El permiso del directorio de Tomcat es anormal, y el proceso de Tomcat es anormal.

Procedimiento

Comprobar si el permiso en el directorio de Tomcat es normal.

Paso 1 En la lista de alarmas del FusionInsight Manager, busque la fila que contiene la alarma y haga clic en para ver la dirección IP del host para el que se genera la alarma.

Paso 2 Inicie sesión en el host de alarma como usuario **root**.

Paso 3 Ejecute el comando **su - omm** para cambiar a usuario **omm**.

Paso 4 Ejecute el comando **vi $BIGDATA_LOG_HOME/omm/oms/ha/scriptlog/tomcat.log** para comprobar si el registro de recursos de Tomcat contiene la palabra clave **Cannot find *XXX*** y rectifique el permiso del archivo basado en la palabra clave.

Paso 5 Después de 5 minutos, compruebe si la alarma se borra automáticamente.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 6**.

Recopilar información de fallas.

Paso 6 En FusionInsight Manager, seleccione **O&M**. En el panel de navegación de la izquierda, elija **Log** > **Download**.

Paso 7 En el área **Services**, seleccione **OmmServer** y **Tomcat** y haga clic en **OK**.

Paso 8 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 9 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

Información relacionada

Ninguna

9.43 ALM-12068 Excepción de recursos de ACS

Descripción

HA comprueba los recursos de ACS de Manager cada 80 segundos. Esta alarma se genera cuando HA detecta que los recursos de ACS son anormales durante dos veces consecutivas.

Esta alarma se borra cuando HA detecta que los recursos de ACS son normales.

Resource Type de ACS es de **Single-active**. Activo/en espera se activará en caso de excepciones de recursos. Cuando se genera esta alarma, se completa la conmutación activa/en espera y se han habilitado nuevos recursos de ACS en el nuevo Manager activo. En este caso, esta alarma se borra. Esta alarma se utiliza para notificar a los usuarios de la causa de la conmutación del Manager activo/en espera.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
12068	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster o sistema para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

- Se produce el cambio de Manager activo/en espera.
- El proceso ACS se reinicia repetidamente, lo que puede causar el error de inicio de sesión del FusionInsight Manager.

Causas posibles

El proceso de ACS es anormal.

Procedimiento

Comprobar si el proceso de ACS es normal.

Paso 1 En la lista de alarmas del Administrador de FusionInsight, busque la fila que contiene la alarma y haga clic en para ver el nombre del host para el que se genera la alarma.

Paso 2 Inicie sesión en el host de alarma como usuario **root**.

Paso 3 Ejecute el comando **su - omm** y luego **sh ${BIGDATA_HOME}/om-server/OMS/workspace0/ha/module/hacom/script/status_ha.sh** para comprobar si el estado de los recursos ACS gestionados por el HA es normal. En el sistema de nodo único, el recurso ACS está en el estado normal. En el sistema de doble nodo, el recurso ACS está en el estado normal en el nodo activo y en el estado detenido en el nodo de espera.

- En caso afirmativo, vaya a **Paso 6**.
- Si no, vaya a **Paso 4**.

Paso 4 Ejecute el comando **vi $BIGDATA_LOG_HOME/omm/oms/ha/scriptlog/acs.log** para comprobar si el registro de recursos ACS de HA contiene la palabra clave **ERROR**. En caso

afirmativo, analice los registros para localizar la causa de la excepción de recurso y corrija la excepción.

Paso 5 Después de 5 minutos, compruebe si la alarma está borrada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 6**.

Recopilar información de fallas.

Paso 6 En FusionInsight Manager, seleccione **O&M**. En el panel de navegación de la izquierda, elija **Log** > **Download**.

Paso 7 En el área **Services**, seleccione **Controller** y **OmmServer** y haga clic en **OK**.

Paso 8 Haga clic en  en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 1 hora antes y después del tiempo de generación de alarma, respectivamente. A continuación, haga clic en **Download**.

Paso 9 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

Información relacionada

Ninguna

9.44 ALM-12069 Excepción de recursos de AOS

Descripción

HA comprueba los recursos de AOS de Manager cada 81 segundos. Esta alarma se genera cuando HA detecta que los recursos de AOS son anormales durante dos veces consecutivas.

Esta alarma se borra cuando HA detecta que los recursos de AOS se vuelven normales.

Resource Type de AOS es **Single-active**. Activo/en espera se activará en caso de excepciones de recursos. Cuando se genera esta alarma, se completa la conmutación activa/en espera y se han habilitado nuevos recursos de AOS en el nuevo Manager activo. En este caso, esta alarma se borra. Esta alarma se utiliza para notificar a los usuarios de la causa de la conmutación del Manager activo/en espera.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
12069	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster o sistema para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

- Se produce el cambio de Manager activo/en espera.
- El proceso AOS se reinicia repetidamente, lo que puede causar un error de inicio de sesión del FusionInsight Manager.

Causas posibles

El proceso de AOS es anormal.

Procedimiento

Comprobar si el proceso AOS es normal.

Paso 1 En la lista de alarmas del Administrador de FusionInsight, busque la fila que contiene la alarma y haga clic en para ver el nombre del host para el que se genera la alarma.

Paso 2 Inicie sesión en el host de alarma como usuario **root**.

Paso 3 Ejecute el comando **sh ${BIGDATA_HOME}/om-server/OMS/workspace0/ha/module/hacom/script/status_ha.sh** para comprobar si el estado de los recursos AOS gestionados por el HA es normal. En el sistema de nodo único, el recurso AOS está en el estado normal. En el sistema de nodo doble, el recurso AOS está en el estado normal en el nodo activo y en el estado detenido en el nodo de espera.

- En caso afirmativo, vaya a **Paso 6**.
- Si no, vaya a **Paso 4**.

Paso 4 Ejecute el comando **vi $BIGDATA_LOG_HOME/omm/oms/ha/scriptlog/aos.log** para comprobar si el registro de recursos AOS de HA contiene la palabra clave **ERROR**. En caso afirmativo, analice los registros para localizar la causa de la excepción de recurso y corrija la excepción.

Paso 5 Después de 5 minutos, compruebe si la alarma está borrada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 6**.

Recopilar información de fallas.

Paso 6 En FusionInsight Manager, seleccione **O&M**. En el panel de navegación de la izquierda, elija **Log** > **Download**.

Paso 7 En el área **Services**, seleccione **Controller** y **OmmServer** y haga clic en **OK**.

Paso 8 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 1 hora antes y después del tiempo de generación de alarma, respectivamente. A continuación, haga clic en **Download**.

Paso 9 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

Información relacionada

Ninguna

9.45 ALM-12070 El recurso del controller es anormal

Descripción de la alarma

HA comprueba los recursos del controller de Manager cada 80 segundos. Esta alarma se genera cuando HA detecta que los recursos del controller son anormales durante 2 veces consecutivas.

Esta alarma se borra cuando el recurso Controller es normal.

Resource Type del Controller es **Single-active**. Activo/en espera se activará en caso de excepciones de recursos. Cuando se genera esta alarma, se completa la conmutación activa/en espera y se han habilitado nuevos recursos del Controller en el nuevo FusionInsight Manager activo. En este caso, esta alarma se borra. Esta alarma se utiliza para notificar a los usuarios de la causa de la conmutación activa/en espera.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
12070	Importante	Sí

Parámetros

Parámetro	Descripción
Source	Especifica el clúster o sistema para el que se genera la alarma.

Parámetro	Descripción
ServiceName	Especifica el nombre del servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

- Se produce la conmutación del FusionInsight Manager activo/en espera.
- El proceso del Controller se reinicia repetidamente, lo que puede provocar un error de inicio de sesión del FusionInsight Manager.

Causas posibles

El proceso del Controller es anormal.

Procedimiento

Comprobar si el proceso del controller es normal.

Paso 1 En la lista de alarmas del FusionInsight Manager, busque la fila que contiene la alarma y vea el nombre del host para el que se genera la alarma.

Paso 2 Inicie sesión en el host para el que se genera la alarma como usuario **root**.

Paso 3 Ejecute el comando **su - omm** para cambiar al **omm** del usuario.Ejecute el comando **sh ${BIGDATA_HOME}/om-server/OMS/workspace0/ha/module/hacom/script/status_ha.sh** para comprobar si el estado de los recursos del Controller gestionados por el HA es normal. En el sistema de nodo único, el recurso Controller está en el estado normal. En el sistema de nodo doble, el recurso del controller está en el estado normal en el nodo activo y en el estado detenido en el nodo de espera.

- Si lo es, vaya a **Paso 6**.
- Si no es así, vaya a **Paso 4**.

Paso 4 Ejecute el comando **vi $BIGDATA_LOG_HOME/omm/oms/ha/scriptlog/controller.log** para ver los registros de recursos del controller y ejecute el comando **vi $BIGDATA_LOG_HOME/controller/controller.log** para ver los registros de ejecución del controller, compruebe si existe la palabra clave **ERROR**. Analice los registros para localizar y rectificar la falla.

Paso 5 Cinco minutos más tarde, compruebe si esta alarma está desactivada.

- Si lo es, no se requiere ninguna otra acción.
- Si no es así, vaya a **Paso 6**.

Recopilar información de fallas.

Paso 6 En FusionInsight Manager, elija **O&M** > **Log** > **Download**.

Paso 7 Seleccione **Controller** y **OmmServe** para **Service** y haga clic en **OK**.

Paso 8 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 1 hora antes y después del tiempo de generación de alarma, respectivamente. A continuación, haga clic en **Download**.

Paso 9 Póngase en contacto con el y envíe la información de registro recopilada.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.46 ALM-12071 El recurso Httpd es anormal

Descripción

HA comprueba los recursos httpd de Manager cada 120 segundos. Esta alarma se genera cuando HA detecta que los recursos httpd son anormales durante 10 veces consecutivas.

Esta alarma se borra cuando el recurso httpd es normal.

Resource Type de httpd es de **Single-active**. Activo/en espera se activará en caso de excepciones de recursos. Cuando se genera esta alarma, se completa la conmutación activa/en espera y se han habilitado nuevos recursos httpd en el nuevo FusionInsight Manager activo. En este caso, esta alarma se borra. Esta alarma se utiliza para notificar a los usuarios de la causa de la conmutación activa/en espera.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
12071	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster o sistema para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.

Nombre	Significado
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

- Se produce la conmutación del FusionInsight Manager activo/en espera.
- El proceso httpd se reinicia repetidamente, lo que puede provocar que no se visite la interfaz de usuario de servicio nativa.

Causas posibles

El proceso httpd es anormal.

Procedimiento

Comprobar si el proceso httpd es anormal.

Paso 1 En la lista de alarmas del FusionInsight Manager, busque la fila que contiene la alarma y vea el nombre del host para el que se genera la alarma.

Paso 2 Inicie sesión en el host para el que se genera la alarma como usuario **root**.

Paso 3 Ejecute el comando **su - omm** para cambiar a usuario **omm**.

Paso 4 Ejecute el comando **sh ${BIGDATA_HOME}/om-server/OMS/workspace0/ha/module/hacom/script/status_ha.sh** para comprobar si el estado de los recursos httpd gestionados por el HA es normal. En el sistema de nodo único, el recurso httpd está en el estado normal. En el sistema de nodo dual, el recurso httpd está en el estado normal en el nodo activo y en el estado detenido en el nodo de espera.

- Si lo es, vaya a **Paso 7**.
- Si no es así, vaya a **Paso 5**.

Paso 5 Ejecute el comando **vi $BIGDATA_LOG_HOME/omm/oms/ha/scriptlog/httpd.log** para ver los registros de recursos httpd y compruebe si existe la palabra clave **ERROR**. Analice los registros para localizar y rectificar la falla.

Paso 6 Cinco minutos más tarde, compruebe si esta alarma está desactivada.

- Si lo es, no se requiere ninguna otra acción.
- Si no es así, vaya a **Paso 7**.

Recopilar información de fallas.

Paso 7 En FusionInsight Manager, elija **O&M** > **Log** > **Download**.

Paso 8 Seleccione **Controller** y **OmmServer** para **Service** y haga clic en **OK**.

Paso 9 Haga clic en  en la esquina superior derecha. En el cuadro de diálogo que aparece, establezca **Start Date** y **End Date** en 1 hora antes y después del tiempo de generación de alarmas, respectivamente, y haga clic en **OK**. A continuación, haga clic en **Download**.

Paso 10 Póngase en contacto con el y envíe la información de registro recopilada.

----Fin

Eliminación de alarmas

Esta alarma se borrará automáticamente después de que se corrija la falla.

Información relacionada

Ninguna

9.47 ALM-12072 El recurso FloatIP es anormal

Descripción

HA comprueba los recursos flotantes de Manager cada 9 segundos. Esta alarma se genera cuando HA detecta que los recursos flotantes son anormales durante 3 veces consecutivas.

Esta alarma se borra cuando el recurso FloatIP es normal.

Resource Type de FloatIP es **Single-active**. Activo/en espera se activará en caso de excepciones de recursos. Cuando se genera esta alarma, la conmutación activa/en espera se completa y se han habilitado nuevos recursos de FloatIP en el nuevo FusionInsight Manager activo. En este caso, esta alarma se borra. Esta alarma se utiliza para notificar a los usuarios de la causa de la conmutación activa/en espera.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
12072	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster o sistema para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

- Se produce la conmutación del FusionInsight Manager activo/en espera.
- El proceso FloatIP se reinicia repetidamente, lo que puede llevar a que no se visite la interfaz de usuario de servicio nativa.

Causas posibles

- La dirección IP flotante es anormal.

Procedimiento

Verificar el estado de la dirección IP flotante del nodo de gestión activo.

Paso 1 En la lista de alarmas del FusionInsight Manager, busque la fila que contiene la alarma y vea la dirección del host para el que se genera la alarma y el nombre del recurso.

Paso 2 Inicie sesión en el nodo de gestión activo como **root**.

Paso 3 Ejecute el siguiente comando, vaya al directorio **${BIGDATA_HOME}/om-server/om/sbin/**.

su - omm

cd ${BIGDATA_HOME}/om-server/om/sbin/

Paso 4 Ejecute el comando **sh status-oms.sh** y ejecute el script **status-oms.sh** para comprobar si la dirección IP flotante del FusionInsight Manager activo es normal. Vea la salida del comando, localice la fila donde **ResName** es **floatip** y compruebe si se muestra la siguiente información.

Por ejemplo:

```
10-10-10-160 floatip Normal Normal Single_active
```

- Si lo es, vaya a **Paso 8**.
- Si no es así, vaya a **Paso 5**.

Paso 5 Ejecute el comando **ifconfig** para comprobar si existe la NIC con la dirección IP flotante.

- Si es así, vaya a **Paso 8**.
- Si no es así, vaya a **Paso 6**.

Paso 6 Ejecute el comando **ifconfig** *NIC name Floating IPaddress* netmask *Subnet mask* para volver a configurar la NIC con la dirección IP flotante. (Por ejemplo, **ifconfig eth0 10.10.10.102 netmask 255.255.255.0**).

Paso 7 Cinco minutos más tarde, compruebe si la alarma está borrada.

- Si lo es, no se requiere ninguna otra acción.
- Si no es así, vaya a **Paso 8**.

Recopilar información de fallas.

Paso 8 En FusionInsight Manager, elija **O&M** > **Log** > **Download**.

Paso 9 Seleccione **Controller** y **OmmServer** para **Service** y haga clic en **OK**.

Paso 10 Haga clic en  en la esquina superior derecha. En el cuadro de diálogo que aparece, establezca **Start Date** y **End Date** en 1 hora antes y después del tiempo de generación de alarmas, respectivamente, y haga clic en **OK**. A continuación, haga clic en **Download**.

Paso 11 Póngase en contacto con el y envíe la información de registro recopilada.

----Fin

Eliminación de alarmas

Esta alarma se borrará automáticamente después de que se corrija la falla.

Información relacionada

Ninguna

9.48 ALM-12073 El recurso de CEP es anormal

Descripción

HA comprueba los recursos cep de Manager cada 60 segundos. Esta alarma se genera cuando HA detecta que los recursos cep son anormales durante 2 veces consecutivas.

Esta alarma se borra cuando el recurso CEP es normal.

Resource Type de CEP es de **Single-active**. Activo/en espera se activará en caso de excepciones de recursos. Cuando se genera esta alarma, se completa la conmutación activa/en espera y se han habilitado nuevos recursos CEP en el nuevo activo FusionInsight Manager. En este caso, esta alarma se borra. Esta alarma se utiliza para notificar a los usuarios de la causa de la conmutación activa/en espera.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
12073	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster o sistema para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

- Se produce la conmutación del FusionInsight Manager activo/en espera.
- El proceso CEP se reinicia repetidamente, haciendo que los datos de monitorización sean anormales.

Causas posibles

El proceso CEP es anormal.

Procedimiento

Comprobar si el proceso CEP es anormal.

Paso 1 En la lista de alarmas del FusionInsight Manager, busque la fila que contiene la alarma y vea el nombre del host para el que se genera la alarma.

Paso 2 Inicie sesión en el host para el que se genera la alarma como usuario **root**.

Paso 3 Ejecute el comando **su -omm** y luego el comando **sh ${BIGDATA_HOME}/om-server/OMS/workspace0/ha/module/hacom/script/status_ha.sh** para comprobar si el estado de los recursos CEP gestionados por el HA es normal. En el sistema de nodo único, el recurso CEP está en el estado normal. En el sistema de nodo doble, el recurso CEP está en el estado normal en el nodo activo y en el estado detenido en el nodo de espera.

- Si lo es, vaya a **Paso 6**.
- Si no es así, vaya a **Paso 4**.

Paso 4 Ejecute los comandos **vi $BIGDATA_LOG_HOME/omm/oms/cep/cep.log** y **vi $BIGDATA_LOG_HOME/omm/oms/cep/scriptlog/cep_ha.log** para ver los registros de recursos CEP, compruebe si existe la palabra clave **ERROR**. Analice los registros para localizar y rectificar la falla.

Paso 5 Cinco minutos más tarde, compruebe si esta alarma está desactivada.

- Si lo es, no se requiere ninguna otra acción.
- Si no es así, vaya a **Paso 6**.

Recopilar información de fallas.

Paso 6 En FusionInsight Manager, elija **O&M** > **Log** > **Download**.

Paso 7 Seleccione **Controller** y **OmmServer** para **Service** y haga clic en **OK**.

Paso 8 Haga clic en  en la esquina superior derecha. En el cuadro de diálogo que aparece, establezca **Start Date** y **End Date** en 1 hora antes y después del tiempo de generación de alarmas, respectivamente, y haga clic en **OK**. A continuación, haga clic en **Download**.

Paso 9 Póngase en contacto con el y envíe la información de registro recopilada.

----Fin

Eliminación de alarmas

Esta alarma se borrará automáticamente después de que se corrija la falla.

Información relacionada

Ninguna

9.49 ALM-12074 El recurso de FMS es anormal

Descripción

HA comprueba los recursos fms de Manager cada 60 segundos. Esta alarma se genera cuando HA detecta que los recursos fms son anormales durante 2 veces consecutivas.

Esta alarma se borra cuando el recurso FMS es normal.

Tipo de recurso de FMS es **Single-active**. Activo/en espera se activará en caso de excepciones de recursos. Cuando se genera esta alarma, se completa la conmutación activa/en espera y se han habilitado nuevos recursos FMS en el nuevo FusionInsight Manager activo. En este caso, esta alarma se borra. Esta alarma se utiliza para notificar a los usuarios de la causa de la conmutación activa/en espera.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
12074	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster o sistema para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

- Se produce la conmutación del FusionInsight Manager activo/en espera.
- El proceso FMS se reinicia repetidamente. Como resultado, la información de alarma puede no ser notificada.

Causas posibles

El proceso FMS es anormal.

Procedimiento

Comprobar si el proceso FMS es anormal.

Paso 1 En la lista de alarmas del FusionInsight Manager, busque la fila que contiene la alarma y vea el nombre del host para el que se genera la alarma.

Paso 2 Inicie sesión en el host para el que se genera la alarma como usuario **root**.

Paso 3 Ejecute el comando **su -omm** y, a continuación, el comando **sh ${BIGDATA_HOME}/om-server/OMS/workspace0/ha/module/hacom/script/status_ha.sh** para comprobar si el estado de los recursos FMS gestionados por el HA es normal. En el sistema de nodo único, el recurso FMS está en el estado normal. En el sistema de doble nodo, el recurso FMS está en el estado normal en el nodo activo y en el estado detenido en el nodo de espera.

- Si lo es, vaya a **Paso 6**.
- Si no es así, vaya a **Paso 4**.

Paso 4 Ejecute los comandos **vi $BIGDATA_LOG_HOME/omm/oms/fms/fms.log** y **vi $BIGDATA_LOG_HOME/omm/oms/fms/scriptlog/fms_ha.log** para ver los registros de recursos de FMS, compruebe si existe la palabra clave **ERROR**. Analice los registros para localizar y rectificar la falla.

Paso 5 5 minutos más tarde, compruebe si esta alarma está desactivada.

- Si lo es, no se requiere ninguna otra acción.
- Si no es así, vaya a **Paso 6**.

Recopilar información de fallas.

Paso 6 En FusionInsight Manager, seleccione **O&M**> **Log** > **Download**.

Paso 7 Seleccione **Controller** y **OmmServer** para **Service** y haga clic en **OK**.

Paso 8 Haga clic en en la esquina superior derecha. En el cuadro de diálogo que aparece, establezca **Start Date** y **End Date** en 1 hora antes y después del tiempo de generación de alarmas, respectivamente, y haga clic en **OK**. A continuación, haga clic en **Download**.

Paso 9 Póngase en contacto con el y envíe la información de registro recopilada.

----Fin

Eliminación de alarmas

Esta alarma se borrará automáticamente después de que se corrija la falla.

Información relacionada

Ninguna

9.50 ALM-12075 El recurso de PMS es anormal

Descripción

HA comprueba los recursos pms de Manager cada 55 segundos. Esta alarma se genera cuando HA detecta que los recursos pms son anormales durante tres veces consecutivas.

Esta alarma se borra cuando el recurso PMS es normal.

Resource Type de PMS es de **Single-active**. Activo/en espera se activará en caso de excepciones de recursos. Cuando se genera esta alarma, se completa la conmutación activa/en espera y se han habilitado nuevos recursos de PMS en el nuevo FusionInsight Manager. En este caso, esta alarma se borra. Esta alarma se utiliza para notificar a los usuarios de la causa de la conmutación activa/en espera.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
12075	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster o sistema para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

- Se produce la conmutación del FusionInsight Manager activo/en espera.
- El proceso PMS se reinicia repetidamente, haciendo que la información de monitorización sea anormal.

Causas posibles

El proceso de PMS es anormal.

Procedimiento

Comprobar si el proceso PMS es anormal.

Paso 1 En la lista de alarmas del FusionInsight Manager, busque la fila que contiene la alarma y vea el nombre del host para el que se genera la alarma.

Paso 2 Inicie sesión en el host para el que se genera la alarma como usuario **root**.

Paso 3 Ejecute el comando **su -omm** y, a continuación, el comando **sh ${BIGDATA_HOME}/om-server/OMS/workspace0/ha/module/hacom/script/status_ha.sh** para comprobar si el estado de los recursos PMS gestionados por el HA es normal. En el sistema de nodo único, el

recurso PMS está en el estado normal. En el sistema de nodo doble, el recurso PMS está en el estado normal en el nodo activo y en el estado detenido en el nodo de espera.

- Si lo es, vaya a **Paso 6**.
- Si no es así, vaya a **Paso 4**.

Paso 4 Ejecute los comandos **vi $BIGDATA_LOG_HOME/omm/oms/pms/pms.log** y **vi $BIGDATA_LOG_HOME/omm/oms/pms/scriptlog/pms_ha.log** para ver los registros de recursos de PMS, compruebe si existe la palabra clave **ERROR**. Analice los registros para localizar y rectificar la falla.

Paso 5 Cinco minutos más tarde, compruebe si esta alarma está desactivada.

- Si lo es, no se requiere ninguna otra acción.
- Si no es así, vaya a **Paso 6**.

Recopilar información de fallas.

Paso 6 En FusionInsight Manager, seleccione **O&M**> **Log** > **Download**.

Paso 7 Seleccione **Controller** y **OmmServer** para **Service** y haga clic en **OK**.

Paso 8 Haga clic en en la esquina superior derecha. En el cuadro de diálogo que aparece, establezca **Start Date** y **End Date** en 1 hora antes y después del tiempo de generación de alarmas, respectivamente, y haga clic en **OK**. A continuación, haga clic en **Download**.

Paso 9 Póngase en contacto con el y envíe la información de registro recopilada.

----Fin

Eliminación de alarmas

Esta alarma se borrará automáticamente después de que se corrija la falla.

Información relacionada

Ninguna

9.51 ALM-12076 El recurso GaussDB es anormal

Descripción

HA comprueba la base de datos del Manager cada 10 segundos. Esta alarma se genera cuando HA detecta que la base de datos es anormal durante 3 veces consecutivas.

Esta alarma se borra cuando la base de datos es normal.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
12076	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster o sistema para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

Si las bases de datos son anormales, todos los servicios básicos y procesos de servicio relacionados, tales como alarmas y funciones de supervisión, se ven afectados.

Causas posibles

Se produce una excepción en la base de datos.

Procedimiento

Verificar el estado de la base de datos de los nodos de gestión activos y en espera.

Paso 1 Inicie sesión en los nodos de gestión activo y en espera respectivamente como usuario **root**. Ejecute el comando **su - ommdba** para cambiar a usuario **ommdba**, a continuación, ejecute el comando **gs_ctl query** para comprobar si se muestra la siguiente información en la salida del comando.

Salida del comando del nodo de gestión activo:

```
Ha state:
       LOCAL_ROLE: Primary
       STATIC_CONNECTIONS            : 1
       DB_STATE                      : Normal
       DETAIL_INFORMATION            : user/password invalid
Senders info:
       No information
Receiver info:
       No information
```

Salida del comando del nodo de gestión en espera:

```
Ha state:
       LOCAL_ROLE: Standby
       STATIC_CONNECTIONS            : 1
       DB_STATE                      : Normal
       DETAIL_INFORMATION            : user/password invalid
Senders info:
       No information
Receiver info:
       No information
```

- Si lo es, vaya a **Paso 3**.

- Si no es así, vaya a **Paso 2**.

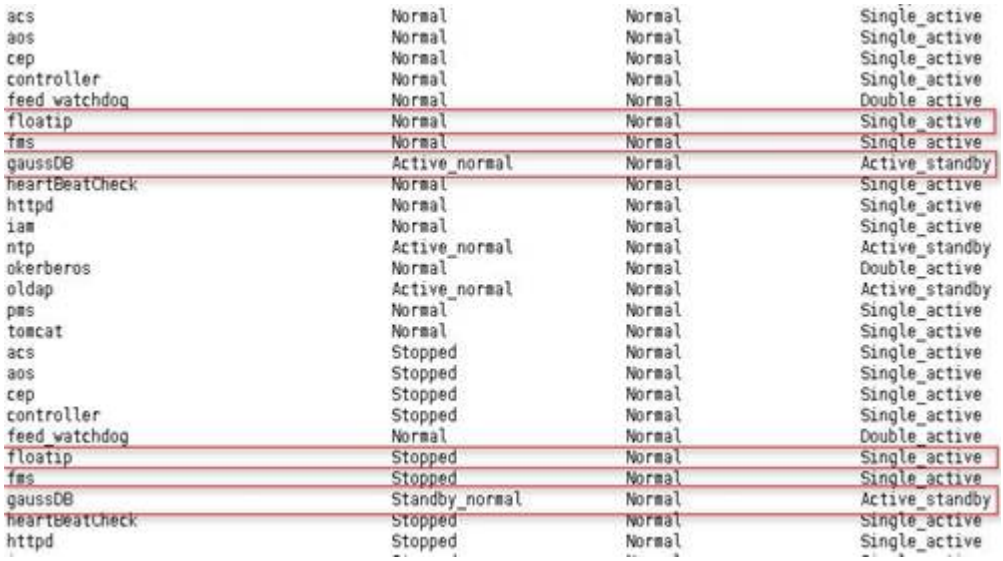
Paso 2 Póngase en contacto con el administrador de la red para comprobar si la red es defectuosa.

- Si lo es, vaya a **Paso 3**.
- Si no es así, vaya a **Paso 5**.

Paso 3 Cinco minutos más tarde, compruebe si la alarma está borrada.

- Si lo es, no se requiere ninguna otra acción.
- Si no es así, vaya a **Paso 4**.

Paso 4 Inicie sesión en los nodos de gestión activo y en espera, ejecute el comando **su -omm** para cambiar a usuario **omm**, vaya al directorio **${BIGDATA_HOME} /om-server/om/sbin/** y ejecute el script **status-oms.sh** para comprobar si las direcciones IP flotantes y los recursos de GaussDB de FusionInsight Managers activos y en espera están en el estado que se muestra en la siguiente figura.



- Si lo están, busque la alarma en la lista de alarmas y borre la alarma manualmente.
- Si no lo son, vaya a **Paso 5**.

Recopilar información de fallas.

Paso 5 En FusionInsight Manager, elija **O&M** > **Log** > **Download**.

Paso 6 Seleccione **OmmServer** para **Service** y haga clic en **OK**.

Paso 7 Haga clic en en la esquina superior derecha. En el cuadro de diálogo que se muestra, establezca **Start Date** y **End Date** en 10 minutos antes y después del tiempo de generación de alarmas respectivamente y haga clic en **OK**. A continuación, haga clic en **Download**.

Paso 8 Póngase en contacto con el y envíe la información de registro recopilada.

----Fin

Eliminación de alarmas

Esta alarma se borrará automáticamente después de que se corrija la falla.

Información relacionada

Ninguna

9.52 ALM-12077 Usuario omm caducado

Descripción

El sistema comienza a las 00:00 todos los días para comprobar si el usuario **omm** ha caducado cada ocho horas. Esta alarma se genera si la cuenta de usuario ha caducado.

Esta alarma se borra cuando se cambia el tiempo de expiración del **omm** de usuario y el estado de la cuenta de usuario se vuelve normal.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
12077	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster o sistema para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

El usuario **omm** ha expirado. La relación de confianza de nodo no está disponible y FusionInsight Manager no puede gestionar los servicios.

Causas posibles

El usuario **omm** ha expirado.

Procedimiento

Comprobar si el usuario omm en el sistema ha caducado.

Paso 1 Inicie sesión en el nodo defectuoso como usuario **root**.

Ejecute el comando **chage -l omm** para ver la información sobre la contraseña del usuario **omm**.

Paso 2 Vea el valor de **Account expires** para comprobar si las configuraciones de usuario han caducado.

NOTA

Si el valor del parámetro es **never**, las configuraciones de usuario nunca caducan.

- Si han caducado, vaya a **Paso 3**.
- Si no han caducado, vaya a **Paso 4**.

Paso 3 Ejecute el comando **chage -E 'yyyy-MM-dd' omm** para establecer el tiempo de caducidad del usuario **omm**. Ocho horas más tarde, compruebe si la alarma se borra automáticamente.

- Si lo es, no se requiere ninguna otra acción.
- Si no es así, vaya a **Paso 4**.

Recopilar información de fallas.

Paso 4 En FusionInsight Manager, elija **O&M** > **Log** > **Download**.

Paso 5 Seleccione **NodeAgent** para **Service** y haga clic en **OK**.

Paso 6 Haga clic en  en la esquina superior derecha. En el cuadro de diálogo que se muestra, establezca **Start Date** y **End Date** en 10 minutos antes y después del tiempo de generación de alarmas respectivamente y haga clic en **OK**. A continuación, haga clic en **Download**.

Paso 7 Póngase en contacto con el y envíe la información de registro recopilada.

----Fin

Eliminación de alarmas

Esta alarma se borrará automáticamente después de que se corrija la falla.

Información relacionada

Ninguna

9.53 ALM-12078 Contraseña del usuario omm caducado

Descripción

El sistema comienza a las 00:00 todos los días para comprobar si la contraseña del usuario **omm** ha caducado cada 8 horas. Esta alarma se genera si la contraseña ha caducado.

Esta alarma se borra cuando se cambia el tiempo de expiración de la contraseña de usuario **omm** y el estado de la contraseña de usuario se vuelve normal.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
12078	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster o sistema para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

La contraseña del usuario **omm** ha caducado. La relación de confianza de nodo no está disponible y FusionInsight Manager no puede gestionar los servicios.

Causas posibles

La contraseña del usuario **omm** ha caducado.

Procedimiento

Comprobar si la contraseña de usuario omm en el sistema se ha caducado.

Paso 1 Inicie sesión en el nodo defectuoso como usuario **root**.

Ejecute el comando **chage -l omm** para ver la información sobre la contraseña del usuario **omm**.

Paso 2 Vea el valor de **Password expires** para comprobar si las configuraciones de usuario han caducado.

NOTA

Si el valor del parámetro es **never**, las configuraciones de usuario nunca caducan.

- Si han caducado, vaya a **Paso 3**.
- Si no han caducado, vaya a **Paso 4**.

Paso 3 Ejecute el comando **chage -M '***days***' omm** para establecer el período de validez de la contraseña para el usuario **omm**. Ocho horas más tarde, compruebe si la alarma se borra automáticamente.

- Si lo es, no se requiere ninguna otra acción.
- Si no es así, vaya a **Paso 4**.

Recopilar información de fallas.

Paso 4 En FusionInsight Manager, seleccione **O&M**> **Log** > **Download**.

Paso 5 Seleccione **NodeAgent** para **Service** y haga clic en **OK**.

Paso 6 Haga clic en  en la esquina superior derecha. En el cuadro de diálogo que se muestra, establezca **Start Date** y **End Date** en 10 minutos antes y después del tiempo de generación de alarmas respectivamente y haga clic en **OK**. A continuación, haga clic en **Download**.

Paso 7 Póngase en contacto con el y envíe la información de registro recopilada.

----Fin

Eliminación de alarmas

Esta alarma se borrará automáticamente después de que se corrija la falla.

Información relacionada

Ninguna

9.54 ALM-12079 El usuario omm está a punto de caducar

Descripción

El sistema comienza a las 00:00 todos los días para comprobar si el usuario **omm** está a punto de caducar cada 8 horas. Esta alarma se genera si la cuenta de usuario caducará no menos de 15 días después.

Esta alarma se borra cuando se cambia el tiempo de expiración del **omm** de usuario y el estado de la cuenta de usuario se vuelve normal.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
12079	Leves	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster o sistema para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.

Nombre	Significado
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

El usuario **omm** ha expirado. La relación de confianza de nodo no está disponible y FusionInsight Manager no puede gestionar los servicios.

Causas posibles

La cuenta del usuario **omm** está a punto de caducar.

Procedimiento

Compruebe si el usuario omm está a punto de expirar.

Paso 1 Inicie sesión en el nodo defectuoso como usuario **root**.

Ejecute el comando **chage -l omm** para ver la información sobre la contraseña del usuario **omm**.

Paso 2 Vea el valor de **Account expires** para comprobar si las configuraciones de usuario están a punto de caducar.

NOTA

Si el valor del parámetro es de **never**, el usuario y la contraseña son válidos permanentemente; si el valor es una fecha, compruebe si el usuario y la contraseña están a punto de caducar en un plazo de 15 días.

- Si lo son, vaya a **Paso 3**.
- Si no lo son, vaya a **Paso 4**.

Paso 3 Ejecute el comando **chage -E** *'yyyy-MM-dd'* **omm** para establecer el período de validez del usuario **omm**. Ocho horas más tarde, compruebe si la alarma se borra automáticamente.

- Si lo es, no se requiere ninguna otra acción.
- Si no es así, vaya a **Paso 4**.

Recopilar información de fallas.

Paso 4 En FusionInsight Manager, elija **O&M** > **Log** > **Download**.

Paso 5 Seleccione **NodeAgent** para **Service** y haga clic en **OK**.

Paso 6 Haga clic en en la esquina superior derecha. En el cuadro de diálogo que se muestra, establezca **Start Date** y **End Date** en 10 minutos antes y después del tiempo de generación de alarmas respectivamente y haga clic en **OK**. A continuación, haga clic en **Download**.

Paso 7 Póngase en contacto con el y envíe la información de registro recopilada.

----Fin

Eliminación de alarmas

Esta alarma se borrará automáticamente después de que se corrija la falla.

Información relacionada

Ninguna

9.55 ALM-12080 La contraseña del usuario omm está a punto de caducar

Descripción

El sistema comienza a las 00:00 todos los días para comprobar si la contraseña del usuario **omm** está a punto de caducar cada 8 horas. Esta alarma se genera si la contraseña caducará no menos de 15 días después.

Esta alarma se borra cuando se restablece el tiempo de expiración de la contraseña de usuario **omm** y el estado de la contraseña de usuario se vuelve normal.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
12080	Leves	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster o sistema para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

La contraseña del usuario **omm** ha caducado. La relación de confianza de nodo no está disponible y FusionInsight Manager no puede gestionar los servicios.

Causas posibles

La contraseña del usuario **omm** está a punto de caducar.

Procedimiento

Comprobar si la contraseña del usuario omm en el sistema está a punto de caducar.

Paso 1 Inicie sesión en el nodo defectuoso como usuario **root**.

Ejecute el comando **chage -l omm** para ver la información sobre la contraseña del usuario **omm**.

Paso 2 Vea el valor de **Password expires** para comprobar si las configuraciones de usuario están a punto de caducar.

NOTA

Si el valor del parámetro es de **never**, el usuario y la contraseña son válidos permanentemente; si el valor es una fecha, compruebe si el usuario y la contraseña están a punto de caducar en un plazo de 15 días.

- Si lo son, vaya a **Paso 3**.
- Si no lo son, vaya a **Paso 4**.

Paso 3 Ejecute el comando **chage -M '***days***' omm** para establecer el período de validez de la contraseña para el usuario **omm**. Ocho horas más tarde, compruebe si la alarma se borra automáticamente.

- Si lo es, no se requiere ninguna otra acción.
- Si no es así, vaya a **Paso 4**.

Recopilar información de fallas.

Paso 4 En FusionInsight Manager, seleccione **O&M**> **Log** > **Download**.

Paso 5 Seleccione **NodeAgent** para **Service** y haga clic en **OK**.

Paso 6 Haga clic en  en la esquina superior derecha. En el cuadro de diálogo que se muestra, establezca **Start Date** y **End Date** en 10 minutos antes y después del tiempo de generación de alarmas respectivamente y haga clic en **OK**. A continuación, haga clic en **Download**.

Paso 7 Póngase en contacto con el y envíe la información de registro recopilada.

----Fin

Eliminación de alarmas

Esta alarma se borrará automáticamente después de que se corrija la falla.

Información relacionada

Ninguna

9.56 ALM-12081 Usuario ommdba caducado

Descripción

El sistema comienza a las 00:00 todos los días para comprobar si el usuario **ommdba** ha caducado cada 8 horas. Esta alarma se genera si la cuenta de usuario ha caducado.

Esta alarma se borra cuando se restablece el tiempo de expiración del usuario **ommdba** y el estado de la cuenta de usuario se vuelve normal.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
12081	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster o sistema para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

No se puede gestionar la base de datos de OMS y no se puede acceder a los datos.

Causas posibles

La cuenta de usuario **ommdba** para el host ha caducado.

Procedimiento

Compruebe si el usuario ommdba ha expirado.

Paso 1 Inicie sesión en el nodo defectuoso como usuario **root**.

Ejecute el comando **chage -l ommdba** para ver la información sobre la contraseña del usuario **ommdba**.

Paso 2 Vea el valor de **Account expires** para comprobar si las configuraciones de usuario han caducado.

NOTA

Si el valor del parámetro es **never** , el usuario y la contraseña son válidos permanentemente; si el valor es una fecha, compruebe si el usuario y la contraseña han caducado.

- Si han caducado, vaya a **Paso 3**.
- Si no han caducado, vaya a **Paso 4**.

Paso 3 Ejecute el comando **chage -E** *'yyyy-MM-dd'* **omm** para establecer el período de validez del usuario **ommdba**. Ocho horas más tarde, compruebe si la alarma se borra automáticamente.

- Si lo es, no se requiere ninguna otra acción.
- Si no es así, vaya a **Paso 4**.

Recopilar información de fallas.

Paso 4 En FusionInsight Manager, elija **O&M** > **Log** > **Download**.

Paso 5 Seleccione **NodeAgent** para **Service** y haga clic en **OK**.

Paso 6 Haga clic en  en la esquina superior derecha. En el cuadro de diálogo que se muestra, establezca **Start Date** y **End Date** en 10 minutos antes y después del tiempo de generación de alarmas respectivamente y haga clic en **OK**. A continuación, haga clic en **Download**.

Paso 7 Póngase en contacto con el y envíe la información de registro recopilada.

----Fin

Eliminación de alarmas

Esta alarma se borrará automáticamente después de que se corrija la falla.

Información relacionada

Ninguna

9.57 ALM-12082 El usuario ommdba está a punto de caducar

Descripción

El sistema comienza a las 00:00 todos los días para comprobar si el usuario **ommdba** está a punto de caducar cada 8 horas. Esta alarma se genera si la cuenta de usuario caducará no menos de 15 días después.

Esta alarma se borra cuando se restablece el tiempo de expiración del usuario **ommdba** y el estado de la cuenta de usuario se vuelve normal.

Atributo

ID de alarma	Gravedad de la alarma	Borrado automático
12082	Leves	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster o sistema para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

No se puede gestionar la base de datos de OMS y no se puede acceder a los datos.

Causas posibles

La cuenta de usuario **ommdba** para el host está a punto de caducar.

Procedimiento

Comprobar si el usuario ommdba está a punto de expirar.

Paso 1 Inicie sesión en el nodo defectuoso como usuario **root**.

Ejecute el comando **chage -l ommdba** para ver la información sobre usuario **ommdba**.

Paso 2 Vea el valor de **Account expires** para comprobar si las configuraciones de usuario están a punto de caducar.

NOTA

Si el valor del parámetro es de **never**, el usuario y la contraseña son válidos permanentemente; si el valor es una fecha, compruebe si el usuario y la contraseña están a punto de caducar en un plazo de 15 días.

- Si lo son, vaya a **Paso 3**.
- Si no lo son, vaya a **Paso 4**.

Paso 3 Ejecute el comando **chage -E** *'yyyy-MM-dd'* **ommdba** para establecer el período de validez de usuario **ommdba**. Ocho horas más tarde, compruebe si la alarma se borra automáticamente.

- Si lo es, no se requiere ninguna otra acción.
- Si no es así, vaya a **Paso 4**.

Recopilar información de fallas.

Paso 4 En FusionInsight Manager, elija **O&M** > **Log** > **Download**.

Paso 5 Seleccione **NodeAgent** para **Service** y haga clic en **OK**.

Paso 6 Haga clic en  en la esquina superior derecha. En el cuadro de diálogo que se muestra, establezca **Start Date** y **End Date** en 10 minutos antes y después del tiempo de generación de alarmas respectivamente y haga clic en **OK**. A continuación, haga clic en **Download**.

Paso 7 Póngase en contacto con el y envíe la información de registro recopilada.

----Fin

Eliminación de alarmas

Esta alarma se borrará automáticamente después de que se corrija la falla.

Información relacionada

Ninguna

9.58 ALM-12083 La contraseña del usuario ommdba está a punto de caducar

Descripción

El sistema comienza a las 00:00 todos los días para comprobar si la contraseña del usuario **ommdba** está a punto de caducar cada 8 horas. Esta alarma se genera si la contraseña está a punto de caducar no menos de 15 días después.

Esta alarma se borra cuando se restablece el tiempo de expiración de la contraseña de **ommdba** de usuario y el estado de la contraseña de usuario se vuelve normal.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
12083	Leves	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster o sistema para el que se genera la alarma.

Nombre	Significado
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

No se puede gestionar la base de datos de OMS y no se puede acceder a los datos.

Causas posibles

La contraseña del usuario **ommdba** está a punto de caducar.

Procedimiento

Comprobar si la contraseña del usuario ommdba en el sistema está a punto de caducar.

Paso 1 Inicie sesión en el nodo defectuoso como usuario **root**.

Ejecute el comando **chage -l ommdba** para ver la información sobre la contraseña del usuario **ommdba**.

Paso 2 Vea el valor de **Password expires** para comprobar si las configuraciones de usuario están a punto de caducar.

NOTA

Si el valor del parámetro es de **never**, el usuario y la contraseña son válidos permanentemente; si el valor es una fecha, compruebe si el usuario y la contraseña están a punto de caducar en un plazo de 15 días.

- Si lo son, vaya a **Paso 3**.
- Si no lo son, vaya a **Paso 4**.

Paso 3 Ejecute el comando **chage -M** *'days'* **ommdba** para establecer el período de validez de la contraseña para el usuario **ommdba**. Ocho horas más tarde, compruebe si la alarma se borra automáticamente.

- Si lo es, no se requiere ninguna otra acción.
- Si no es así, vaya a **Paso 4**.

Recopilar información de fallas.

Paso 4 En FusionInsight Manager, elija **O&M** > **Log** > **Download**.

Paso 5 Seleccione **NodeAgent** para **Service** y haga clic en **OK**.

Paso 6 Haga clic en  en la esquina superior derecha. En el cuadro de diálogo que se muestra, establezca **Start Date** y **End Date** en 10 minutos antes y después del tiempo de generación de alarmas respectivamente y haga clic en **OK**. A continuación, haga clic en **Download**.

Paso 7 Póngase en contacto con el y envíe la información de registro recopilada.

----Fin

Eliminación de alarmas

Esta alarma se borrará automáticamente después de que se corrija la falla.

Información relacionada

Ninguna

9.59 ALM-12084 Contraseña del usuario ommdba caducada

Descripción

El sistema comienza a las 00:00 todos los días para comprobar si la contraseña del usuario **ommdba** ha caducado cada 8 horas. Esta alarma se genera si la contraseña ha caducado.

Esta alarma se borra cuando se restablece el tiempo de expiración de la contraseña de **ommdba** de usuario y el estado de la contraseña de usuario se vuelve normal.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
12084	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster o sistema para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

La contraseña del usuario **ommdba** ha caducado. La relación de confianza de nodo no está disponible y FusionInsight Manager no puede gestionar los servicios.

Causas posibles

La contraseña del usuario **ommdba** para el host ha caducado.

Procedimiento

Comprobar si la contraseña del usuario ommdba en el sistema ha caducado.

Paso 1 Inicie sesión en el nodo defectuoso como usuario **root**.

Ejecute el comando **chage -l ommdba** para ver la información sobre la contraseña del usuario **ommdba**.

Paso 2 Vea el valor de **Password expires** para comprobar si las configuraciones de usuario han caducado.

NOTA

Si el valor del parámetro es **never**, el usuario y la contraseña son válidos permanentemente; si el valor es una fecha, compruebe si el usuario y la contraseña han caducado.

- Si han caducado, vaya a **Paso 3**.
- Si no han caducado, vaya a **Paso 4**.

Paso 3 Ejecute el comando **chage -M** *'days'* **ommdba** para establecer el período de validez de la contraseña para el usuario **ommdba**. Ocho horas más tarde, compruebe si la alarma se borra automáticamente.

- Si lo es, no se requiere ninguna otra acción.
- Si no es así, vaya a **Paso 4**.

Recopilar información de fallas.

Paso 4 En FusionInsight Manager, elija **O&M** > **Log** > **Download**.

Paso 5 Seleccione **NodeAgent** para **Service** y haga clic en **OK**.

Paso 6 Haga clic en  en la esquina superior derecha. En el cuadro de diálogo que se muestra, establezca **Start Date** y **End Date** en 10 minutos antes y después del tiempo de generación de alarmas respectivamente y haga clic en **OK**. A continuación, haga clic en **Download**.

Paso 7 Póngase en contacto con el y envíe la información de registro recopilada.

----Fin

Eliminación de alarmas

Esta alarma se borrará automáticamente después de que se corrija la falla.

Información relacionada

Ninguna

9.60 ALM-12085 Error de volcado del registro de auditoría de servicio

Descripción

El sistema volca los registros de auditoría de servicio a las 03:00 todos los días y los almacena en el nodo OMS. Esta alarma se genera cuando el volcado falla. Esta alarma se borra cuando el próximo volcado tiene éxito.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
12085	Leves	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster o sistema para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

Es posible que se pierdan los registros de auditoría del servicio.

Causas posibles

- Los registros de auditoría del servicio están sobredimensionados.
- El espacio de almacenamiento de la copia de respaldo de OMS es insuficiente.
- El espacio de almacenamiento de un host donde se encuentra el servicio es insuficiente.

Procedimiento

Comprobar si los registros de auditoría del servicio están sobredimensionados.

Paso 1 En la lista de alarmas del FusionInsight Manager, localice la fila que contiene la alarma y vea la dirección IP del host y la información adicional para la que se genera la alarma.

Paso 2 Inicie sesión en el host donde se genera la alarma como usuario **root**.

Paso 3 Ejecute el comando **vi ${BIGDATA_LOG_HOME}/controller/scriptlog/getLogs.log** para comprobar si se puede buscar la palabra clave "LOG SIZE is more than 5000MB".

- Si puede, vaya a **Paso 4**.
- Si no puede, vaya a **Paso 5**.

Paso 4 Compruebe si los registros de auditoría de servicio de gran tamaño son causados por excepciones.

El espacio de almacenamiento de la copia de respaldo de OMS es insuficiente.

Paso 5 Ejecute el comando **vi ${BIGDATA_LOG_HOME}/controller/scriptlog/getLogs.log** para comprobar si se puede buscar la palabra clave "Collect log failed, too many logs on".

- Si puede, obtenga la dirección IP del host siguiendo la palabra clave "Collect log failed, too many logs on", y vaya a **Paso 6**.
- Si no puede, vaya a **Paso 11**.

Paso 6 Inicie sesión en el host con la dirección IP obtenida en **Paso 5** como usuario **root**.

Paso 7 Ejecute el comando **vi {BIGDATA_LOG_HOME}/nodeagent/scriptlog/collectLog.log** para comprobar si se puede buscar la palabra clave "log size overs".

- Si puede, vaya a **Paso 9**.
- Si no puede, vaya a **Paso 8**.

Paso 8 Compruebe si la información adicional de la alarma contiene la palabra clave "no enough space".

- En caso afirmativo, vaya a **Paso 9**.
- Si no, vaya a **Paso 11**.

Paso 9 Realice las siguientes operaciones para ampliar la capacidad del disco (solo para MRS 3.1.2 y versiones anteriores) o reducir el número máximo de copias de seguridad de registros de auditoría:

- Amplíe la capacidad del nodo OMS.
- Ejecute el siguiente comando para editar el archivo y reducir el valor de **MAX_NUM_BK_AUDITLOG**.

  vi ${CONTROLLER_HOME}/etc/om/componentsauditlog.properties

Paso 10 En el siguiente periodo de ejecución, 03:00, compruebe si la alarma está borrada.

- Si lo es, no se requiere ninguna otra acción.
- Si no es así, vaya a **Paso 11**.

Comprobar si el espacio del host donde se encuentra el servicio es insuficiente.

Paso 11 Ejecute el comando **vi ${BIGDATA_LOG_HOME}/controller/scriptlog/getLogs.log** para comprobar si se puede buscar la palabra clave "Collect log failed, no enough space on *hostIp*".

- Si puede, obtenga la dirección IP del host anormal y diríjase a **Paso 12**.
- Si no puede, vaya a **Paso 15**.

Paso 12 Inicie sesión en el host con la dirección IP obtenida como usuario **root** y ejecute el comando **df "$BIGDATA_HOME/tmp" -lP | tail -1 | awk '{print ($4/1024)}'** para obtener el espacio restante del directorio log del host. Compruebe si el valor es inferior a 1000 MB.

- Si lo es, vaya a **Paso 13**.
- Si no es así, vaya a **Paso 15**.

Paso 13 Amplíe la capacidad del nodo

Paso 14 En el siguiente periodo de ejecución, 03:00, compruebe si la alarma está borrada.

- Si lo es, no se requiere ninguna otra acción.
- Si no es así, vaya a **Paso 15**.

Recopilar información de fallas.

Paso 15 En FusionInsight Manager, seleccione **O&M**> **Log** > **Download**.

Paso 16 Seleccione **Controller** para **Service** y haga clic en **OK**.

Paso 17 Haga clic en  en la esquina superior derecha. En el cuadro de diálogo que se muestra, establezca **Start Date** y **End Date** en 10 minutos antes y después del tiempo de generación de alarmas respectivamente y haga clic en **OK**. A continuación, haga clic en **Download**.

Paso 18 Póngase en contacto con el y envíe la información de registro recopilada.

----Fin

Eliminación de alarmas

Esta alarma se borrará automáticamente después de que se corrija la falla.

Información relacionada

Ninguna

9.61 ALM-12087 El sistema está en el período de observación de actualización

Descripción

El sistema comprueba si está en el período de observación de actualización a las 00:00 todos los días y comprueba si la duración que ha estado en el estado de observación de actualización excede el período de observación de actualización preestablecido, 10 días por defecto. Esta alarma se genera cuando el sistema está en el período de observación de actualización y la duración en que el sistema ha estado en el estado de observación de actualización excede el período preestablecido (10 días por defecto). Esta alarma se borra automáticamente si el sistema sale del período de observación de actualización después de que el usuario realiza una reversión o envío.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
12087	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster o sistema para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Upgrade Observation Period (Days)	Especifica los días que el sistema está en el período de observación de actualización.

Impacto en el sistema

La próxima actualización o instalación de parches fallará.

Causas posibles

La tarea de actualización no se envía un período de tiempo especificado (10 días de forma predeterminada) después de la actualización del sistema.

Procedimiento

Compruebe si el sistema se encuentra en el período de observación de actualización.

Paso 1 Inicie sesión en el nodo de gestión activo como usuario **root**.

Paso 2 Ejecute los siguientes comandos para cambiar a usuario **omm** e inicie sesión en la base de datos de **omm**:

su - omm

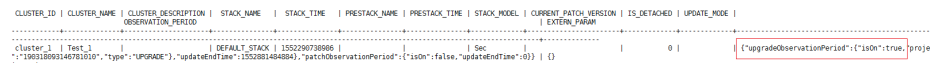
gsql -U omm -W *omm database password* **-p 20015**

Paso 3 Ejecute el comando **select * from OM_CLUSTERS** para ver la información del clúster.

Paso 4 Comprobar si el valor de **upgradObservationPeriod isON** es de **true** como se muestra en la **Figura 9-13**.

- Si es así, el sistema se encuentra en el período de observación de actualización. Utilice el UpdateTool para enviar la tarea de actualización. Para obtener más información, consulte la guía de actualización de la versión correspondiente.
- Si no es así, vaya a **Paso 6**.

Figura 9-13 Información del clúster



Paso 5 A primera hora de la mañana del día siguiente, compruebe si esta alarma está borrada.

- Si lo es, no se requiere ninguna otra acción.
- Si no es así, vaya a **Paso 6**.

Recopilar información de fallas.

Paso 6 En el portal del FusionInsight Manager, elija **O&M** > **Log > Download**.

Paso 7 Seleccione **Controller** en el **Service** y haga clic en **OK**.

Paso 8 Haga clic en  en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 9 Póngase en contacto con el y envíe la información de registro recopilada.

----Fin

Eliminación de alarmas

Esta alarma se borrará automáticamente después de que se corrija la falla.

Información relacionada

Ninguna

9.62 ALM-12089 La red entre nodos es anormal

Descripción

El módulo de alarma comprueba el estado de la red de los nodos del clúster cada 10 segundos. Esta alarma se genera cuando la red entre dos nodos es inalcanzable o el estado de la red es inestable.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
12089	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster o sistema para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.

Nombre	Significado
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

Las funciones de algunos componentes, como HDFS y ZooKeeper se ven afectadas.

Causas posibles

- El nodo se rompe.
- La red está defectuosa.

Procedimiento

Comprobar el estado de salud de red.

Paso 1 En la lista de alarmas en el FusionInsight Manager, haga clic en el botón desplegable de la alarma y vea **Additional Information**. Registre la dirección IP de origen y la dirección IP de destino del nodo para el que se notifica la alarma.

Paso 2 Inicie sesión en el nodo para el que se notifica la alarma. En el nodo, haga ping al nodo de destino para comprobar si la red entre los dos nodos es normal.

- En caso afirmativo, vaya a **6**.
- Si no, vaya a **3**.

Comprobar el estado de nodo.

Paso 3 En FusionInsight Manager, haga clic en **Host** y compruebe si la lista de hosts contiene el nodo defectuoso para determinar si el nodo defectuoso se ha eliminado del clúster.

- En caso afirmativo, vaya a **5**.
- Si no, vaya a **4**.

Paso 4 Compruebe si el nodo defectuoso está apagado.

- En caso afirmativo, inicie el nodo defectuoso y vaya a **Paso 2**.
- Si no, póngase en contacto con el personal relacionado para encontrar la causa raíz, si es necesario quitar los nodos defectuosos del clúster y vaya a **5**, de lo contrario vaya a **6**.

Paso 5 Quite el archivo **$NODE_AGENT_HOME/etc/agent/hosts.ini** de todos los nodos del clúster, limpie el archivo **/var/log/Bigdata/unreachable/unreachable_ip_info.log** y, a continuación, borre manualmente la alarma.

Paso 6 Espere 30 segundos y compruebe si la alarma se ha despejado.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **7**.

Recopilar información de fallas.

Paso 7 En el portal del FusionInsight Manager, elija **O&M** > **Log > Download**.

Paso 8 Seleccione **OmmAgent** en el **Service** y haga clic en **OK**.

Paso 9 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 10 Póngase en contacto con el y envíe la información de registro recopilada.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.63 ALM-12101 AZ de mal funcionamiento

Descripción

Después de activar la función AZ DR, el sistema comprueba el estado de salud de zona de disponibilidad cada 5 minutos. Esta alarma se genera cuando el sistema detecta que la zona de disponibilidad está subhealthy o en mal funcionamiento. Esta alarma se borra cuando la zona de disponibilidad se vuelve en buen funcionamiento.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
12101	Crítica	Sí

Parámetros

Parámetro	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
AZName	Especifica la zona de disponibilidad para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

El estado de funcionamiento de una zona de disponibilidad se determina por si el estado de funcionamiento de los recursos de almacenamiento (HDFS), los recursos de computación (Yarn) y los roles clave en la zona de disponibilidad exceden el umbral configurado.

Una zona de disponibilidad es subsana cuando:

- Los recursos informáticos (Yarn) no están en buen estado, pero los recursos de almacenamiento (HDFS) están en buen estado. Las tareas no se pueden enviar a la zona de disponibilidad local, pero los datos aún se pueden leer y escribir en la zona de disponibilidad local.
- Los recursos informáticos (Yarn) están en buen estado, pero algunos recursos de almacenamiento (HDFS) no están en buen estado. Las tareas se pueden enviar a la zona de disponibilidad local, y algunos datos se pueden leer y escribir en la zona de disponibilidad local. Esto depende de la localidad de los datos detectados por la programación de Spark/Hive.

Una zona de disponibilidad no es sana cuando:

- Los recursos informáticos (Yarn) están en buen estado, pero los recursos de almacenamiento (HDFS) no están en buen estado. Aunque las tareas se pueden enviar a la zona de disponibilidad local, los datos no se pueden leer o escribir en la zona de disponibilidad local. Como resultado, las tareas enviadas a la zona de disponibilidad local no son válidas.
- Los recursos informáticos (Yarn) y los recursos de almacenamiento (HDFS) están en mal estado. Las tareas no se pueden enviar a la zona de disponibilidad local, y los datos no se pueden leer o escribir en la zona de disponibilidad local.
- El estado de salud de los roles clave, excepto Yarn y HDFS, es inferior al umbral configurado.

Causas posibles

- Los recursos informáticos (Yarn) no están en buen estado.
- Los recursos de almacenamiento (HDFS) no están en buen estado.
- Algunos recursos de almacenamiento (HDFS) no están en buen estado.
- Los roles clave, excepto Yarn y HDFS, no están en buen estado.

Procedimiento

Deshabilitar el simulacro de recuperación ante desastres.

Paso 1 En FusionInsight Manager, elija **Cluster** > *Name of the desired cluster* > **Cross-AZ HA**. Se muestra la página Cross-AZ HA.

Paso 2 En la lista de AZ DR, compruebe si **Perform DR Drill** en la columna **Operation** de la AZ cuyo estado de salud es **Unhealthy** es gris.

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 3**.

Paso 3 Haga clic en **Restore** en la columna **Operation** de la zona de disponibilidad de destino. Espere 2 minutos y actualice la página para ver el estado de salud de la zona de disponibilidad. Compruebe si el estado de salud es normal.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 4**.

Recopilar información de fallas.

Paso 4 Inicie sesión en el nodo de gestión activo como usuario **root**.

Paso 5 Vea los registros de servicios en mal estado.

- Los archivos de registro de HDFS se almacenan en **/var/log/Bigdata/hdfs/nn/hdfs-az-state.log**.
- Los archivos de registro de Yarn se almacenan en **/var/log/Bigdata/yarn/rm/yarn-az-state.log**.
- Para otros servicios, vea los registros de comprobación de estado del servicio en el directorio de registro de servicio correspondiente.

Paso 6 Póngase en contacto con y proporcione información detallada del archivo de registro.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.64 ALM-12102 El componente AZ HA no se despliega según los requisitos de DR.

Descripción

El módulo de alarma comprueba el estado de despliegue de los componentes de zona de disponibilidad HA cada 5 minutos. Esta alarma se genera cuando los componentes que admiten DR no se despliegan en función de los requisitos de DR después de habilitar AZ. Esta alarma se borra cuando los componentes se despliegan en función de los requisitos de DR.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
12102	Grave	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.

Impacto en el sistema

La capacidad de HA entre AZ de un solo clúster se ve afectada.

Causas posibles

Los roles de los componentes que admiten DR no se despliegan en función de los requisitos de DR.

Procedimiento

Obtener información de alarma.

Paso 1 En FusionInsight Manager, seleccione **O&M** > **Alarm** > **Alarms**.

Paso 2 En la lista de alarmas, haga clic en ⌄ en la fila que contiene la alarma y vea los roles que no se implementan según los requisitos de DR de **Additional Information**.

Volver a desplegar la instancia de rol.

Paso 3 Elija **Cluster** > **Services** > *Name of the desired service* > **Instance**. En la página de instancia, vuelva a desplegar o ajuste la instancia de rol.

Paso 4 Compruebe si la alarma se borra 10 minutos después.

- En caso afirmativo, no es necesario hacer nada más.
- En caso negativo, contacte a .

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

Información relacionada

Ninguna

9.65 ALM-12103 Excepción de recursos del executor

Descripción

HA comprueba los recursos del Executor de Manager cada 30 segundos. Esta alarma se genera cuando HA detecta que los recursos del Executor son anormales durante dos veces consecutivas.

Esta alarma se borra cuando los recursos del Executor son normales.

Resource Type de Executor es **Single-active**. Activo/en espera se activará en caso de excepciones de recursos. Cuando se genera esta alarma, se completa la conmutación activa/en espera y se han habilitado nuevos recursos de Executor en el nuevo Manager activo. En este caso, esta alarma se borra. Esta alarma se utiliza para notificar a los usuarios de la causa de la conmutación del Manager activo/en espera.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
12103	Grave	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster o sistema para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

- Se produce el cambio de Manager activo/en espera.
- El proceso Executor sigue reiniciando. Como resultado, es posible que no se acceda a la página del clúster.

Causas posibles

El proceso del Executor es anormal.

Procedimiento

Comprobar si el proceso de Executor es anormal.

Paso 1 En la lista de alarmas del FusionInsight Manager, busque la fila que contiene la alarma y haga clic en para ver el nombre del host para el que se genera la alarma.

Paso 2 Inicie sesión en el host para el que se genera la alarma como usuario **root**.

Paso 3 Ejecute el comando **su - omm** para cambiar a usuario **omm**.

Paso 4 Ejecute el comando **sh ${BIGDATA_HOME}/om-server/OMS/workspace0/ha/module/hacom/script/status_ha.sh** para comprobar si el estado de los recursos del Executor gestionados por el HA es normal. En el sistema de nodo único, el recurso Executor está en el estado normal. En el sistema de nodo doble, el recurso Executor está en el estado normal en el nodo activo y en el estado detenido en el nodo de espera.

- En caso afirmativo, vaya a **Paso 7**.
- Si no, vaya a **Paso 5**.

Paso 5 Ejecute el comando **vi $BIGDATA_LOG_HOME/omm/oms/ha/scriptlog/executor.log** para comprobar si el registro de recursos del Executor de HA contiene la palabra clave **ERROR**. En caso afirmativo, analice el registro para localizar la causa de la excepción del recurso y corrija la excepción.

Paso 6 Después de 5 minutos, compruebe si esta alarma está desactivada.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 7**.

Recopilar información de fallas.

Paso 7 En FusionInsight Manager, seleccione **O&M**. En el panel de navegación de la izquierda, elija **Log** > **Download**.

Paso 8 En el área **Services**, seleccione **Controller** y **OmmServer** y haga clic en **OK**.

Paso 9 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 1 hora antes y después del tiempo de generación de alarma, respectivamente. A continuación, haga clic en **Download**.

Paso 10 Póngase en contacto con y proporcione los registros recopilados.

----Fin

9.66 ALM-12104 Recursos Knox anormales

Descripción

HA comprueba los recursos de Knox de Manager cada 70 segundos. Esta alarma se genera cuando HA detecta que los recursos de Knox son anormales durante tres veces consecutivas.

Esta alarma se borra cuando HA detecta que los recursos de Knox son normales.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
12104	Grave	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster o sistema para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

Las solicitudes enviadas por los servicios de nivel superior mediante el uso de Knox no se pueden procesar correctamente.

Causas posibles

El proceso de Knox es anormal.

Procedimiento

Compruebe si el proceso Knox es normal.

Paso 1 Inicie sesión en FusionInsight Manager. En la lista de alarmas, busque la fila que contiene la alarma y vea el nombre del host para el que se genera la alarma.

Paso 2 Utilice PuTTY para iniciar sesión en el host para el que se genera la alarma como usuario **root**.

Paso 3 Ejecute el comando **su - omm** para cambiar a usuario **omm**.

Paso 4 Ejecute el comando **sh ${BIGDATA_HOME}/om-server/om/sbin/status-oms.sh** para comprobar si el estado de los recursos Knox gestionados por HA es normal. Si el estado es normal, los recursos de Knox son normales. De lo contrario, los recursos de Knox son anormales.

- En caso afirmativo, vaya a **Paso 7**.
- Si no, vaya a **Paso 5**.

Paso 5 Ejecute el comando **vi $BIGDATA_LOG_HOME/omm/oms/ha/scriptlog/knox.log** para comprobar si el registro de recursos de Knox de HA contiene la palabra clave **ERROR**. En

caso afirmativo, analice el registro para localizar la causa de la excepción del recurso y corrija la excepción.

Paso 6 Después de 5 minutos, compruebe si esta alarma está desactivada.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 7**.

Recopilar información de fallas.

Paso 7 En FusionInsight Manager, seleccione **O&M**. En el panel de navegación de la izquierda, elija **Log** > **Download**.

Paso 8 En el área **Services**, seleccione **Controller** y **OmmServer** y haga clic en **OK**.

Paso 9 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 1 hora antes y después del tiempo de generación de alarma, respectivamente. A continuación, haga clic en **Download**.

Paso 10 Póngase en contacto con y proporcione los registros recopilados.

----Fin

9.67 ALM-12110 Error al obtener ECS AK/SK temporal

Descripción

El metaservicio obtiene periódicamente el AK/SK temporal del ECS. Esta alarma se genera cuando el servicio de metadatos no obtiene el AK/SK temporal.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
12110	Grave	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

En escenarios de desacoplamiento de almacenamiento-cómputo, el clúster no puede obtener el último AK/SK temporal, lo que puede conducir a un acceso fallido a OBS.

Causas posibles

- El meta rol del clúster de MRS es anormal.
- El grupo ha estado vinculado a una delegación y ha accedido a OBS, pero ha estado desvinculado de la delegación. En consecuencia, el clúster no ha estado vinculado a ninguna delegación.

Procedimiento

Comprobar el estado de meta rol.

Paso 1 En FusionInsight Manager del clúster, seleccione **O&M** > **Alarm** > **Alarms**. En la página que se muestra, haga clic en ⌄ en la fila que contiene la alarma y determine la dirección IP del host para el que se genera la alarma.

Paso 2 En FusionInsight Manager del clúster, seleccione **Cluster** > **Services** > **Meta**. En la página que se muestra, haga clic en la pestaña **Instance** y compruebe si el rol meta correspondiente al host para el que se genera la alarma es normal.

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 3**.

Paso 3 Seleccione el rol anormal y elija **More** > **Restart Instance** para reiniciar el rol meta anormal. Una vez finalizado el reinicio, compruebe si la alarma se borra varios minutos más tarde.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 4**.

Volver a vincular el clúster a una delegación.

Paso 4 Inicie sesión en la consola de gestión de MRS.

Paso 5 En el panel de navegación de la izquierda, elija **Clusters** >**Active Clusters**. En la página que se muestra, haga clic en el nombre del clúster para ir a su página de descripción general. A continuación, compruebe si el clúster está vinculado a una delegación en el área de gestión de O&M.

- En caso afirmativo, vaya a **Paso 7**.
- Si no, vaya a **Paso 6**.

Paso 6 Haga clic en **Manage Agency**. En la página que se muestra, vuelva a vincular el clúster a una delegación. A continuación, compruebe si la alarma se borra unos minutos más tarde.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 7**.

Paso 7 Póngase en contacto con .

----Fin

9.68 ALM-12172 Error al notificar métricas a Cloud Eye

Descripción

Después de habilitar el uso compartido de métricas para un clúster, el Controller recopila periódicamente métricas del clúster y las informa a Cloud Eye.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
12172	Grave	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster o sistema para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

Las métricas de monitoreo de MRS no están disponibles en Cloud Eye.

Causas posibles

- Error al invocar a las API de Cloud Eye debido a los permisos insuficientes.
- No se pudo informar de datos a Cloud Eye debido a problemas de red.
- Error al informar datos a Cloud Eye debido a errores internos.

Procedimiento

Paso 1 En FusionInsight Manager, seleccione **O&M** > **Alarm** > **Alarms**. En la página que se muestra, haga clic en ⌄ en la fila que contiene la alarma y vea la información adicional de la alarma.

Paso 2 Rectifique el fallo en base a los siguientes escenarios:

- Si "Call CES to send metrics fail. Permission exception" se muestra en la información adicional, el token del tenant del recurso no es válido. Reinicie el Controller y obtenga el token de nuevo.
- Si "Call CES to send metrics fail. Request CES error code xxx" se muestra en la información adicional, se produce un error en la solicitud a Cloud Eye. Compruebe la conectividad de red y la información de autenticación.
- Si "Call CES to send metrics fail. CES internal error code xxx" se muestra en la información adicional, el servicio de Cloud Eye encuentra un error interno y no está disponible. Póngase en contacto con y envíe los registros de fallas recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

Información relacionada

Ninguna

9.69 ALM-12180 E/S de disco suspendido

Descripción

- En el caso de HDDs, la alarma se activa cuando se cumple alguna de las siguientes condiciones:
  - El sistema recopila datos cada 3 segundos y detecta que el valor **svctm** supera los 6 segundos durante 10 periodos consecutivos en 30 segundos.
  - El sistema recoge datos cada 3 segundos, y detecta que el valor **avgqu-sz** es mayor que 0, el IOPS o ancho de banda es 0, y el valor **ioutil** es mayor que **99%** durante 10 períodos consecutivos en 30 segundos.
- Para las SSD, la alarma se activa cuando se cumple alguna de las siguientes condiciones:
  - El sistema recopila datos cada 3 segundos y detecta que el valor **svctm** supera los 2 segundos durante 10 periodos consecutivos en 30 segundos.
  - El sistema recoge datos cada 3 segundos, y detecta que el valor **avgqu-sz** es mayor que 0, el IOPS o ancho de banda es 0, y el valor **ioutil** es mayor que **99%** durante 10 períodos consecutivos en 30 segundos.

Esta alarma se borra automáticamente cuando las condiciones anteriores no se han cumplido durante 90s.

NOTA

- Ejecute el siguiente comando en el sistema operativo para recopilar datos:

  iostat -x -t 1 1

  Los parámetros son los siguientes:

  avgqu-sz indica la profundidad de la cola del disco.

  La suma de **r/s** y **w/s** es la IOPS.

  La suma de **rkB/s** y **wkB/s** es el ancho de banda.

  %util es el valor **ioutil**.

- MRS 3.1.0:

  Ejecute el comando **iostat -x -t** en el sistema operativo.

- Calcule **svctm** de la siguiente manera en versiones posteriores a MRS 3.1.0:

  svctm = (tot_ticks_new - tot_ticks_old)/(rd_ios_new + wr_ios_new - rd_ios_old - wr_ios_old)

  Si **rd_ios_new + wr_ios_new - rd_ios_old - wr_ios_old** es **0**, entonces **svctm** es **0**.

  Los parámetros se pueden obtener de la siguiente manera:

  El sistema ejecuta el comando **cat /proc/diskstats** cada 3 segundos para recopilar datos. Por ejemplo:

  En estos dos comandos:

  En los datos recopilados por primera vez, el número en la cuarta columna es el valor **rd_ios_old**, el número en la octava columna es el valor **wr_ios_old** y el número en la decimotercera columna es el valor **tot_ticks_old**.

  En los datos recopilados por segunda vez, el número en la cuarta columna es el valor **rd_ios_new**, el número en la octava columna es el valor **wr_ios_new** y el número en la decimotercera columna es el valor **tot_ticks_new**.

  En este caso, el valor de **svctm** es el siguiente:

  (19571460 - 19569526)/(1101553 + 28747977 - 1101553 - 28744856) = 0.6197

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
12180	Grave	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster o sistema para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Nombre	Significado
DiskName	Especifica el disco para el que se genera la alarma.

Impacto en el sistema

Un uso de E/S continuamente alto puede afectar negativamente a las operaciones de servicio y dar como resultado la pérdida de servicio.

Causas posibles

El disco está envejecido.

Procedimiento

Reemplazar el disco.

Paso 1 Inicie sesión en FusionInsight Manager y elija **O&M** > **Alarm** > **Alarms**.

Paso 2 Vea la información detallada sobre la alarma. Compruebe los valores de **HostName** y **DiskName** en la información de ubicación para obtener la información sobre el disco defectuoso para el que se informa la alarma.

Paso 3 Reemplace el disco duro.

Paso 4 Verifique si la alarma se ha borrado.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 5**.

Recopilar información de fallas.

Paso 5 En FusionInsight Manager, seleccione **O&M**. En el panel de navegación de la izquierda, elija **Log** > **Download**.

Paso 6 Seleccione **OMS** para **Service** y haga clic en **OK**.

Paso 7 Haga clic en  en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 8 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

Información relacionada

Ninguna

9.70 ALM-12190 Número de conexiones Knox supera el umbral

Descripción

El sistema comprueba periódicamente el número de conexiones a todas las topologías Knox. Esta alarma se genera cuando el número de conexiones a una topología supera el umbral (90% por defecto). Esta alarma se borra automáticamente cuando el número de conexiones a una topología cae por debajo del umbral.

NOTA

Esta alarma se aplica a clústeres de MRS 3.1.0 o posterior.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
12190	Grave	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster o sistema para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Topology	Especifica la topología de Knox para la que se genera la alarma.

Impacto en el sistema

La topología puede alcanzar el límite superior de conexiones y no reenviar solicitudes, afectando negativamente a las funciones de MRS.

Causas posibles

Hue o Manager se usa con demasiada frecuencia, pero el número máximo predeterminado de conexiones Knox es pequeño.

Procedimiento

Paso 1 Inicie sesión en los nodos OMS activos y en espera como usuario **root**, respectivamente.

Paso 2 Agregue la siguiente configuración al archivo **gateway-site.xml** en los nodos de OMS activo y en espera para aumentar el número de grupos de subprocesos:

vi /opt/knox/conf/gateway-site.xml

```
<property>
<name>gateway.httpclient.maxConnections</name>
<value>64</value>
</property>
```

Paso 3 Inicie sesión en el nodo OMS activo como usuario **omm** y ejecute el siguiente comando para reiniciar el proceso Knox:

sh /opt/knox/bin/restart-knox.sh

Paso 4 Después de 5 minutos, compruebe si la alarma está borrada.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 5**.

Paso 5 Póngase en contacto con para rectificar la falla.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

Información relacionada

Ninguna

9.71 ALM-13000 Servicio ZooKeeper no disponible

Descripción

El sistema comprueba el estado del servicio ZooKeeper cada 60 segundos. Esta alarma se genera cuando el servicio ZooKeeper no está disponible.

Esta alarma se borra cuando se recupera el servicio ZooKeeper.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
13000	Crítica	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

ZooKeeper no puede proporcionar servicios de coordinación para componentes de capa superior y los componentes que dependen de ZooKeeper pueden no ejecutarse correctamente.

Causas posibles

- El DNS se instala en el nodo ZooKeeper.
- La red está defectuosa.
- El servicio KrbServer es anormal.
- La instancia ZooKeeper es anormal.
- La capacidad del disco es insuficiente.

Procedimiento

Comprobar el DNS.

Paso 1 Compruebe si el DNS está instalado en el nodo donde se encuentra la instancia ZooKeeper. En el nodo Linux donde se encuentra la instancia ZooKeeper, ejecute el comando **cat /etc/resolv.conf** para comprobar si el archivo está vacío.

- En caso afirmativo, vaya a **Paso 2**.
- Si no, vaya a **Paso 3**.

Paso 2 Ejecute el comando **service named status** para comprobar si se ha iniciado el DNS.

- En caso afirmativo, vaya a **Paso 3**.
- Si no, vaya a **Paso 5**.

Paso 3 Ejecute el comando **service named stop** para detener el servicio DNS. Si "Shutting down name server BIND waiting for named to shut down (28s)" se muestra, el servicio DNS se detiene correctamente. Comente el contenido (si lo hubiera) en **/etc/resolv.conf**.

Paso 4 En la pestaña **O&M > Alarm > Alarms**, compruebe si la alarma está borrada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 5**.

Comprobar el estado de red.

Paso 5 En el nodo Linux donde se encuentra la instancia ZooKeeper, ejecute el comando **ping** para comprobar si los nombres de host de otros nodos donde se encuentra la instancia ZooKeeper se pueden hacer pings correctamente.

- En caso afirmativo, vaya a **Paso 9**.
- Si no, vaya a **Paso 6**.

Paso 6 Modifique las direcciones IP de **/etc/hosts** y agregue el nombre de host y la asignación de direcciones IP.

Paso 7 Ejecute de nuevo el comando **ping** para comprobar si los nombres de host de otros nodos donde se encuentra la instancia ZooKeeper se pueden hacer ping correctamente.

- En caso afirmativo, vaya a **Paso 8**.
- Si no, vaya a **Paso 23**.

Paso 8 En la pestaña **O&M > Alarm > Alarms**, compruebe si la alarma está borrada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 9**.

Verificar el estado del servicio KrbServer (Omita este paso si se usa el modo normal).

Paso 9 En FusionInsight Manager, seleccione **Cluster >** *Name of the desired cluster* **> Services**.

Paso 10 Compruebe si el servicio KrbServer es normal.

- En caso afirmativo, vaya a **Paso 13**.
- Si no, vaya a **Paso 11**.

Paso 11 Realice operaciones basadas en "ALM-25500 Servicio KrbServer no disponible" y compruebe si se ha recuperado el servicio KrbServer.

- En caso afirmativo, vaya a **Paso 12**.
- Si no, vaya a **Paso 23**.

Paso 12 En la pestaña **O&M > Alarm > Alarms**, compruebe si la alarma está borrada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 13**.

Verificar el estado de la instancia del servicio ZooKeeper.

Paso 13 En FusionInsight Manager, elija **Cluster >** *Name of the desired cluster* **> Services** > **ZooKeeper** > **quorumpeer**.

Paso 14 Compruebe si las instancias ZooKeeper son normales.

- En caso afirmativo, vaya a **Paso 18**.
- Si no, vaya a **Paso 15**.

Paso 15 Seleccione instancias cuyo estado no es bueno y elija **More** > **Restart Instance**.

Paso 16 Compruebe si el estado de la instancia es bueno después del reinicio.

- En caso afirmativo, vaya a **Paso 17**.
- Si no, vaya a **Paso 18**.

Paso 17 En la pestaña **O&M > Alarm > Alarms**, compruebe si la alarma está borrada.

- De ser así, no se requiere ninguna acción adicional.

- Si no, vaya a **Paso 18**.

Comprobar estado de disco.

Paso 18 En FusionInsight Manager, elija **Cluster >** *Name of the desired cluster* **> Service** > **ZooKeeper** > **quorumpeer** y compruebe la información del host del nodo de la instancia de ZooKeeper.

Paso 19 En FusionInsight Manager, haga clic en **Host**.

Paso 20 En la columna **Disk**, compruebe si el espacio en disco de cada nodo donde se encuentran las instancias de ZooKeeper es insuficiente (el uso del disco supera el 80%).

- En caso afirmativo, vaya a **Paso 21**.
- Si no, vaya a **Paso 23**.

Paso 21 Amplíe la capacidad del disco. Para obtener más información, consulte "ALM-12017 Capacidad insuficiente del disco".

Paso 22 En la pestaña **O&M > Alarm > Alarms**, compruebe si la alarma está borrada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 23**.

Recopilar información de fallas.

Paso 23 En el portal del FusionInsight Manager, elija **O&M** > **Log > Download**.

Paso 24 Seleccione los siguientes nodos en el clúster requerido desde el **Service**: (KrbServer no es necesario descargar los registros en modo normal.)

- ZooKeeper
- KrbServer

Paso 25 Haga clic en  en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 26 Póngase en contacto con el y envíe la información de registro recopilada.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.72 ALM-13001 Las conexiones de ZooKeeper disponibles son insuficientes

Descripción

El sistema comprueba las conexiones de ZooKeeper cada 60 segundos. Esta alarma se genera cuando el sistema detecta que el número de conexiones de instancia ZooKeeper usadas excede el umbral (80% de las conexiones máximas).

Cuando el **Trigger Count** es 1, esta alarma se borra cuando el número de conexiones de instancia de ZooKeeper usadas es menor o igual que el umbral. Cuando el **Trigger Count** es mayor que 1, esta alarma se borra cuando el número de conexiones de instancia de ZooKeeper usadas es menor o igual al 90% del umbral.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
13001	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el nombre del servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el nombre de host para el que se genera la alarma.
Trigger Condition	Especifica el umbral que activa la alarma. Si el valor del indicador actual excede este umbral, se genera la alarma.

Impacto en el sistema

Las conexiones de ZooKeeper disponibles son insuficientes. Cuando el uso de la conexión alcanza el 100%, las conexiones externas no se pueden manejar.

Causas posibles

El número de conexiones al nodo de ZooKeeper supera el umbral. La fuga de conexión ocurre en algunos procesos de conexión, o el número máximo de conexiones no cumple con el escenario real.

Procedimiento

Comprobar el estado de conexión.

Paso 1 En el portal del FusionInsight Manager, elija **O&M** > **Alarm** > **Alarms**. En la interfaz mostrada, haga clic en el botón desplegable de **Available ZooKeeper Connections Are Insufficient** y confirme la dirección IP del nodo del host para el que se genera la alarma en la Información de ubicación.

Paso 2 Obtenga el PID del proceso de ZooKeeper. Inicie sesión en el nodo involucrado en esta alarma como usuario **root** y ejecute el comando **pgrep -f proc_zookeeper**.

Paso 3 Compruebe si el PID se puede obtener correctamente.

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 15**.

Paso 4 Obtenga todas las direcciones IP conectadas a la instancia de ZooKeeper y el número de conexiones y compruebe 10 direcciones IP con conexiones superiores. Ejecute el siguiente comando basado en el PID obtenido: **lsof -i|grep** *$pid* **| awk '{print $9}' | cut -d : -f 2 | cut -d \>-f 2 | awk '{a[$1]++} END {for(i in a){print i,a[i] | "sort -r -g -k 2"}}' | head -10**. (Se usa el PID obtenido en la etapa anterior.)

Paso 5 Compruebe si las direcciones IP de nodo y el número de conexiones se obtienen correctamente.

- En caso afirmativo, vaya a **Paso 6**.
- Si no, vaya a **Paso 15**.

Paso 6 Obtenga el ID del puerto conectado al proceso. Ejecute el siguiente comando basado en el PID y la dirección IP obtenidos: **lsof -i|grep** *$pid* **| awk '{print $9}'|cut -d \> -f 2 |grep** *$IP*| **cut -d : -f 2**. (Se utilizan el PID y la dirección IP obtenidos en el paso anterior.)

Paso 7 Compruebe si el ID de puerto se ha obtenido correctamente.

- En caso afirmativo, vaya a **Paso 8**.
- Si no, vaya a **Paso 15**.

Paso 8 Obtenga el ID del proceso conectado. Inicie sesión en cada dirección IP y ejecute el siguiente comando basado en el ID de puerto obtenido: **lsof -i|grep** *$port*. (Se utiliza el ID de puerto obtenido en el paso anterior.)

Paso 9 Compruebe si el ID de proceso se obtiene correctamente.

- En caso afirmativo, vaya a **Paso 10**.
- Si no, vaya a **Paso 15**.

Paso 10 Compruebe si se produce una fuga de conexión en el proceso basándose en el ID de proceso obtenido.

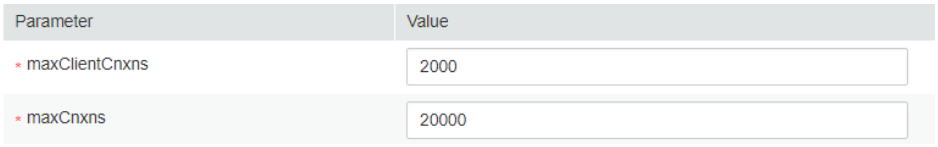
- En caso afirmativo, vaya a **Paso 11**.
- Si no, vaya a **Paso 12**.

Paso 11 Cierre el proceso donde se produce una fuga de conexión y compruebe si la alarma está desactivada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 12**.

Paso 12 En el portal de FusionInsight Manager, elija **Cluster >** *Name of the desired cluster* **> Services** > **ZooKeeper** > **Configurations** > **All Configurations** > **quorumpeer** > **Performance** y aumente el valor de **maxCnxns** según sea necesario.

Figura 9-14 maxCnxns



Paso 13 Guarde la configuración y reinicie el servicio ZooKeeper.

Paso 14 Verifique si la alarma se ha borrado.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 15**.

Recopilar información de fallas.

Paso 15 En el portal del FusionInsight Manager, elija **O&M** > **Log > Download**.

Paso 16 Seleccione **ZooKeeper** en el clúster requerido en el **Service**:

Paso 17 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 18 Póngase en contacto con el y envíe la información de registro recopilada.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.73 ALM-13002 El uso de memoria directa de ZooKeeper supera el umbral

Descripción

El sistema comprueba el uso de memoria directa del servicio ZooKeeper cada 30 segundos. La alarma se genera cuando el uso de memoria directa de una instancia de ZooKeeper excede el umbral (80% de la memoria máxima).

Cuando el **Trigger Count** es 1, esta alarma se borra cuando el uso de memoria directa ZooKeeper es menor que el umbral. Cuando el **Trigger Count** es mayor que 1, esta alarma se borra cuando el uso de memoria directa ZooKeeper es menor que 80% del umbral.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
13002	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el nombre del servicio para el que se genera la alarma.
RoleName	Especifica el nombre del rol para el que se genera la alarma.
HostName	Especifica el objeto (ID de host) para el que se genera la alarma.
Trigger Condition	Especifica el umbral que activa la alarma. Si el valor del indicador actual excede este umbral, se genera la alarma.

Impacto en el sistema

Si la memoria directa disponible del servicio ZooKeeper es insuficiente, se produce un desbordamiento de memoria y el servicio se interrumpe.

Causas posibles

La memoria directa de la instancia ZooKeeper se utiliza en exceso o la memoria directa se asigna de forma inapropiada.

Procedimiento

Comprobar el uso de la memoria directa.

Paso 1 En el portal del FusionInsight Manager, elija **O&M** > **Alarm** > **Alarms**. En la interfaz mostrada, haga clic en el botón desplegable de **ZooKeeper Direct Memory Usage Exceeds the Threshold**. Compruebe la dirección IP de la instancia que reporta la alarma.

Paso 2 En el portal del FusionInsight Manager, elija **Cluster >** *Name of the desired cluster* **> Services** > **ZooKeeper** > **Instance** > **quorumpeer(the IP address checked)**. Haga clic en el menú desplegable en la esquina superior derecha del **Chart**, elija **Customize** > **CPU and**

Memory y seleccione **ZooKeeper Heap And Direct Buffer Resource Percentage**, haga clic en **OK**.

Paso 3 Compruebe si la memoria intermedia directa utilizada de ZooKeeper alcanza el 80% de la memoria intermedia directa máxima especificada para ZooKeeper.

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 8**.

Paso 4 En el portal del FusionInsight Manager, seleccione **Cluster >** *Name of the desired cluster* **> Services** > **ZooKeeper** > **Configurations** > **All Configurations** > **quorumpeer** > **System** para comprobar si existe "-XX:MaxDirectMemorySize" en el parámetro **GC_OPTS**.

- Si es así, en el parámetro **GC_OPTS**, elimine "-XX:MaxDirectMemorySize" y vaya a **Paso 5**.
- Si no, vaya a **Paso 6**.

Paso 5 Guarde la configuración y reinicie el servicio ZooKeeper.

Paso 6 Compruebe si existe **ALM-13004 El uso de memoria heap de ZooKeeper excede el umbral**.

- En caso afirmativo, maneje la alarma haciendo referencia a **ALM-13004 El uso de memoria heap de ZooKeeper excede el umbral**.
- Si no, vaya a **Paso 7**.

Paso 7 Verifique si la alarma se ha borrado.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 8**.

Recopilar información de fallas.

Paso 8 En el portal del FusionInsight Manager, elija **O&M** > **Log > Download**.

Paso 9 Seleccione **ZooKeeper** en el clúster requerido en el **Service**.

Paso 10 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 11 Póngase en contacto con el y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.74 ALM-13003 GC La duración del proceso ZooKeeper supera el umbral

Descripción

El sistema comprueba la duración de la recolección de basura (GC) del proceso ZooKeeper cada 60 segundos. Esta alarma se genera cuando la duración de GC excede el umbral (12 segundos por defecto).

Esta alarma se borra cuando la duración de GC es menor que el umbral.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
13003	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger Condition	Especifica el umbral para activar la alarma.

Impacto en el sistema

Una larga duración GC del proceso ZooKeeper puede interrumpir los servicios.

Causas posibles

La memoria heap del proceso ZooKeeper se usa en exceso o se asigna de forma inapropiada, provocando la ocurrencia frecuente del proceso GC.

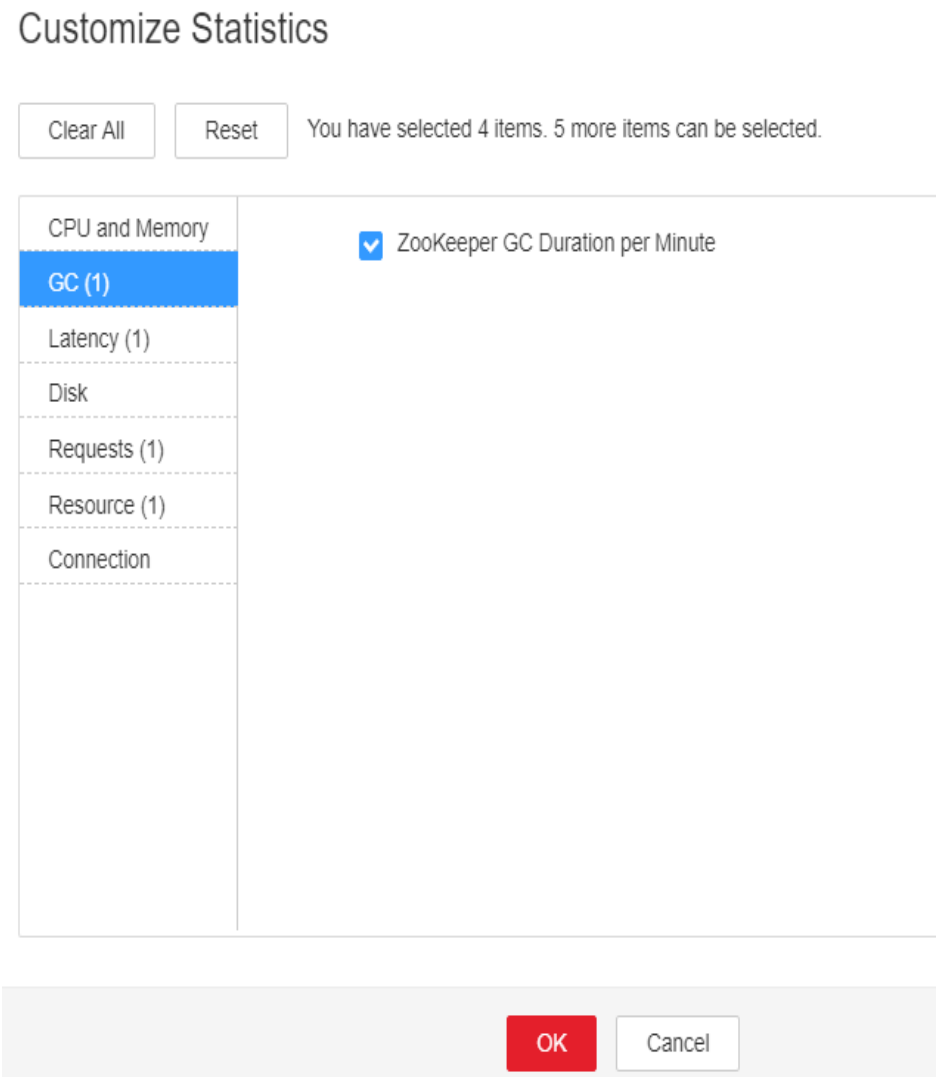
Procedimiento

Comprobar la duración del GC.

Paso 1 En FusionInsight Manager, seleccione **O&M** > **Alarm** > **Alarms**. En la página mostrada, haga clic en la lista desplegable de **GC Duration of the ZooKeeper Process Exceeds the Threshold**. Vea la dirección IP de la instancia para la que se genera la alarma.

Paso 2 En FusionInsight Manager, seleccione **Cluster** > *Name of the desired cluster* > **Services** > **ZooKeeper** > **Instance** > **quorumpeer**. Haga clic en la lista desplegable en la esquina superior derecha del **Chart**, elija **Customize** > **GC**, seleccione **ZooKeeper GC Duration per Minute** y haga clic **OK** para verificar las estadísticas de duración de GC del proceso ZooKeeper recopiladas cada minuto.

Figura 9-15 Duración de GC de ZooKeeper



Paso 3 Compruebe si la duración GC del proceso ZooKeeper recopilado cada minuto supera el umbral (12 segundos por defecto).

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 8**.

Paso 4 Compruebe si se produce una pérdida de memoria en la aplicación.

Paso 5 En la página **Home** del FusionInsight Manager, seleccione **Cluster** > **Services** > **ZooKeeper**. En la página que se muestra, haga clic en la pestaña **Configuration**, luego en la subpestaña

All Configurations y seleccione **quorumpeer** > **System**. Aumente el valor del parámetro **GC_OPTS** según sea necesario.

NOTA

Generalmente, **-Xmx** tiene el doble de capacidad de datos de ZooKeeper. Si la capacidad de ZooKeeper alcanza los 2 GB, ajuste **GC_OPTS** de la siguiente manera:

-Xms4G -Xmx4G -XX:NewSize=512M -XX:MaxNewSize=512M -XX:MetaspaceSize=64M -XX:MaxMetaspaceSize=64M -XX:CMSFullGCsBeforeCompaction=1

Paso 6 Guarde la configuración y reinicie el servicio ZooKeeper.

Paso 7 Verifique si la alarma se ha borrado.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 8**.

Recopilar información de fallas.

Paso 8 En FusionInsight Manager, seleccione **O&M**. En el panel de navegación de la izquierda, elija **Log** > **Download**.

Paso 9 Expanda la lista desplegable **Service** y seleccione **ZooKeeper** para el clúster de destino.

Paso 10 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 11 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

Información relacionada

Ninguna

9.75 ALM-13004 El uso de memoria heap de ZooKeeper supera el umbral

Descripción

El sistema comprueba el uso de memoria heap del servicio de ZooKeeper cada 60 segundos. La alarma se genera cuando el uso de memoria heap de una instancia de ZooKeeper excede el umbral (95% de la memoria máxima).

La alarma se borra cuando el uso de memoria es menor que el umbral.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
13004	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el nombre del servicio para el que se genera la alarma.
RoleName	Especifica el nombre del rol para el que se genera la alarma.
HostName	Especifica el objeto (ID de host) para el que se genera la alarma.
Trigger Condition	Especifica el umbral que activa la alarma. Si el valor del indicador actual excede este umbral, se genera la alarma.

Impacto en el sistema

Si la memoria heap de ZooKeeper disponible es insuficiente, se produce un desbordamiento de memoria y el servicio se interrumpe.

Causas posibles

La memoria heap de la instancia de ZooKeeper se utiliza en exceso o la memoria heap se asigna de forma inadecuada.

Procedimiento

Comprobar el uso de memoria heap.

Paso 1 En el portal del FusionInsight Manager, en la interfaz mostrada, haga clic en el botón desplegable de **ZooKeeper Heap Memory Usage Exceeds the Threshold** y confirme la dirección IP del nodo del host para el que se genera la alarma en la información de ubicación.

Paso 2 En el portal del FusionInsight Manager, elija **Cluster >** *Name of the desired cluster* **> Services** > **ZooKeeper** > **Instance** y haga clic en **quorumpeer** en la columna **Role** de la dirección IP correspondiente. Haga clic en el menú desplegable en la esquina superior derecha del **Chart**, elija **Customize** > **CPU and Memory** y seleccione **ZooKeeper Heap And Direct Buffer Resource Percentage**, haga clic en **OK**. Compruebe el uso de la memoria heap.

Paso 3 Compruebe si la memoria heap utilizada de ZooKeeper alcanza el 95% de la memoria heap máxima especificada para ZooKeeper.

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 7**.

Paso 4 En el portal del FusionInsight Manager, seleccione **Cluster >** *Name of the desired cluster* **> Services** > **ZooKeeper** > **Configurations** > **All Configurations** > **quorumpeer** > **System**. Aumente el valor de **-Xmx** en **GC_OPTS** según sea necesario. Los detalles son los siguientes:

1. En la pestaña **Instance**, haga clic en **quorumpeer** en la columna **Role** de la dirección IP correspondiente. Elija **Customize** > **CPU and Memory** en la esquina superior derecha, y seleccione **ZooKeeper Heap And Direct Buffer Resource**, haga clic en **OK** para comprobar la memoria de pila utilizada por ZooKeeper.
2. Cambie el valor de **-Xmx** en el parámetro **GC_OPTS** en función del uso real de memoria heap. Generalmente, el valor es el doble del tamaño del volumen de datos de ZooKeeper. Por ejemplo, si se utiliza una memoria heap de ZooKeeper de 2 GB, se recomiendan las siguientes configuraciones: -Xms4G -Xmx4G -XX:NewSize=512M -XX:MaxNewSize=512M -XX:MetaspaceSize=64M -XX:MaxMetaspaceSize=64M -XX:CMSFullGCsBeforeCompaction=1

Paso 5 Guarde la configuración y reinicie el servicio ZooKeeper.

Paso 6 Verifique si la alarma se ha borrado.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 7**.

Recopilar información de fallas.

Paso 7 En el portal del FusionInsight Manager, elija **O&M** > **Log > Download**.

Paso 8 Seleccione **ZooKeeper** en el clúster requerido en el **Service**.

Paso 9 Haga clic en  en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 10 Póngase en contacto con el y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.76 ALM-13005 No se pudo establecer la cuota de los principales directorios de los componentes de ZooKeeper

Descripción

El sistema establece cuotas para cada directorio de nivel superior ZooKeeper en el elemento de configuración y componentes **customized.quota** cada 5 horas. Esta alarma se genera cuando el sistema no puede establecer la cuota para un directorio.

Esta alarma se borra cuando la configuración se realiza correctamente después de una falla.

Atributo

ID de alarma	Gravedad de la alarma	Borrado automáticamente
13005	Leves	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el nombre del servicio para el que se genera la alarma.
ServiceDirectory	Especifica el directorio para el que se genera la alarma.
Trigger Condition	Especifica la causa de la alarma.

Impacto en el sistema

Los componentes pueden escribir una gran cantidad de datos en el directorio de nivel superior de ZooKeeper. Como resultado, el servicio ZooKeeper no está disponible.

Causas posibles

La cuota para el directorio de alarma es inapropiada.

Procedimiento

Comprobar si la cuota para el directorio de alarmas es adecuada.

Paso 1 Inicie sesión en FusionInsight Manager y elija **Cluster >** *Name of the desired cluster* **> Services** > **ZooKeeper**. En la página mostrada, elija **Configurations** > **All Configurations** >

Quota. Compruebe si el directorio para el que se informa la alarma y su cuota existen en el elemento de configuración **customized.quota**.

- En caso afirmativo, vaya a **Paso 5**.
- Si no, vaya a **Paso 2**.

Paso 2 Compruebe si el directorio de alarmas para el que se reporta la alarma se encuentra en la siguiente lista de alarmas.

Tabla 9-1 Directorio de alarmas de componentes

Componente	Directorio de alarmas
Hbase	/hbase
Hive	/beelinesql
Yarn	/rmstore
Storm	/stormroot
Streaming	/storm
Kafka	/kafka

- En caso afirmativo, vaya a **Paso 3**.
- Si no, vaya a **Paso 7**.

Paso 3 Vea el componente del directorio de alarma en la tabla, abra la página de servicio correspondiente y elija **Configurations** > **All Configurations**. En la página mostrada, busque **zk.quota** en la esquina superior derecha. El resultado de la búsqueda es la cuota del directorio de alarma.

Paso 4 Compruebe si la cuota del directorio de alarmas para el que se informa es apropiada. La cuota debe ser mayor o igual que el valor real, que se puede obtener en **Trigger Condition**.

Paso 5 Modifique el valor **services.quota** como se le solicite y guarde la configuración.

Paso 6 Después del tiempo especificado por **service.quotas.auto.check.cron.expression**, compruebe si la alarma está desactivada.

- Si lo es, no se requiere ninguna otra acción.
- Si no, vaya a **Paso 7**.

Recopilar información de fallas.

Paso 7 En el portal del FusionInsight Manager, elija **O&M** > **Log > Download**.

Paso 8 Seleccione **ZooKeeper** en el clúster requerido en el **Service**.

Paso 9 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 10 Póngase en contacto con el y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.77 ALM-13006 El número o la capacidad de Znode supera el umbral

Descripción

El sistema detecta periódicamente el estado del Znode secundario en el directorio de datos de servicio ZooKeeper cada cuatro horas. This alarm is generated when the number or capacity of secondary Znodes exceeds the threshold.

Atributo

ID de alarma	Gravedad de la alarma	Borrado automáticamente
13006	Leves	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el nombre del servicio para el que se genera la alarma.
ServiceDirectory	Especifica el directorio para el que se genera la alarma.
Trigger Condition	Especifica la causa de la alarma.

Impacto en el sistema

Se escribe una gran cantidad de datos en el directorio de datos de ZooKeeper. Como resultado, el ZooKeeper no puede proporcionar servicios normales.

Causas posibles

Se escribe una gran cantidad de datos en el directorio de datos de ZooKeeper. El umbral no es apropiado.

Procedimiento

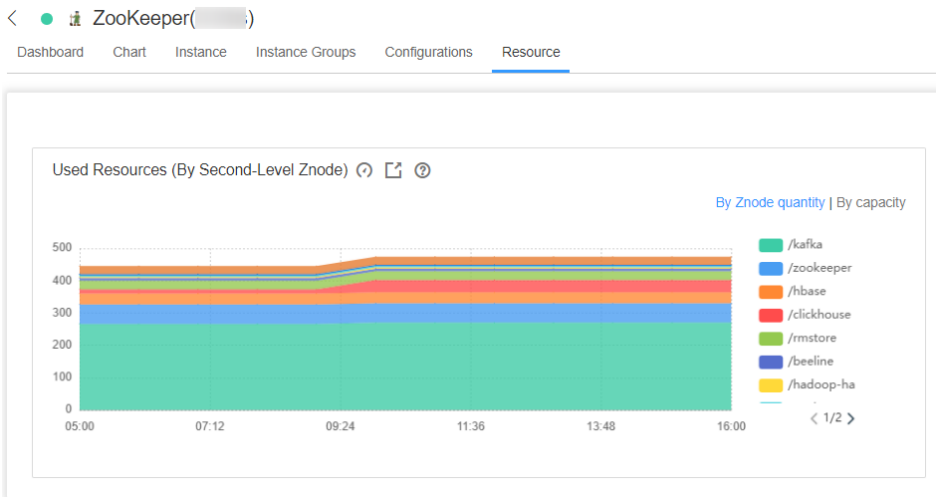
Compruebe si se escribe una gran cantidad de datos en el directorio para el que se genera la alarma.

Paso 1 En FusionInsight Manager, seleccione **O&M** > **Alarm** > **Alarms**. En la interfaz mostrada, haga clic en el botón desplegable de **Znode Number or Capacity Exceeds the Threshold**. Confirme el Znode para el que se genera la alarma en Información de ubicación.

Paso 2 Inicie sesión en FusionInsight Manager, abra la interfaz del servicio ZooKeeper y seleccione **Resource**. En la tabla **Used Resources (By Second-Level Znode)**, compruebe si se escribe una gran cantidad de datos en el Znode de nivel superior para el que se notifica la alarma.

- Si lo es, vaya a **Paso 3**.
- Si no es así, vaya a **Paso 4**.

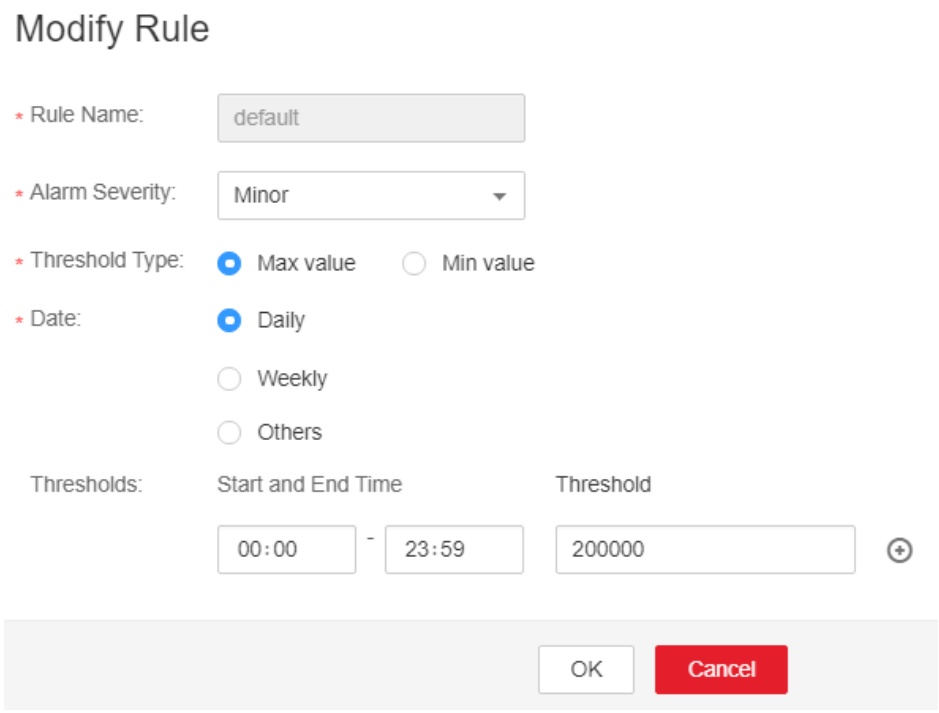
Figura 9-16 Recursos usados (por Znode de segundo nivel)



Paso 3 Inicie sesión en el cliente ZooKeeper y elimine los datos en el Znode de nivel superior.

Paso 4 Inicie sesión en el FusionInsight Manager y abra la interfaz del servicio ZooKeeper. En la página **Resource**, elija > **By Znode quantity** en **Used Resources (By Second-Level Znode)**. Se muestra **Threshold Configuration of By Znode quantity**. Haga clic en **Modify** en **Operation**. Aumente el umbral haciendo referencia al valor de **max.Znode.count** eligiendo **Cluster >** *Name of the desired cluster* **> Services** > **ZooKeeper** > **Configurations > All Configurations > Quota**.

Figura 9-17 Modificar regla



Paso 5 En el **Used Resources (By Second-Level Znode)**, elija > **By capacity**. Se muestra la página **Threshold Settings** de **By Capacity**. Haga clic en **Modify** en **Operation**. Aumente el umbral haciendo referencia al valor de **max.data.size** seleccionando **Cluster >** *Name of the desired cluster* **> Services** > **ZooKeeper** > **Configurations > All Configurations** > **Quota**.

Paso 6 Verifique si la alarma se ha borrado.

- Si lo es, no se requiere ninguna otra acción.
- Si no es así, vaya a **Paso 7**.

Recopilar información de fallas.

Paso 7 En el portal del FusionInsight Manager, elija **O&M** > **Log > Download**.

Paso 8 Seleccione **ZooKeeper** en el clúster requerido en el **Service**.

Paso 9 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 10 Póngase en contacto con el y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.78 ALM-13007 Las conexiones de cliente de ZooKeeper disponibles son insuficientes

Descripción

El sistema detecta periódicamente el número de procesos activos entre el cliente de ZooKeeper y el servidor de ZooKeeper cada 60 segundos. Esta alarma se genera cuando el número de conexiones excede el umbral.

Atributo

ID de alarma	Gravedad de la alarma	Borrado automáticamente
13007	Leves	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el nombre del servicio para el que se genera la alarma.
RoleName	Especifica el nombre del rol para el que se genera la alarma.
HostName	Especifica el nombre de host para el que se genera la alarma.
ClientIP	Especifica la dirección IP del cliente.
ServerIP	Especifica la dirección IP del servidor.
Trigger Condition	Especifica la causa de la alarma.

Impacto en el sistema

Un gran número de conexiones a ZooKeeper hizo que el ZooKeeper estuviera completamente conectado y no pudiera proporcionar servicios normales.

Causas posibles

Un gran número de procesos de cliente están conectados a ZooKeeper. Los umbrales no son apropiados.

Procedimiento

Compruebe si hay una gran cantidad de procesos de clientes conectados a ZooKeeper.

Paso 1 En FusionInsight Manager, seleccione **O&M** > **Alarm** > **Alarms**. En la interfaz mostrada, haga clic en el botón desplegable de **Available ZooKeeper Client Connections Are Insufficient**. Confirme la dirección IP del nodo del host para el que se genera la alarma en la información de ubicación.

Paso 2 Abra la interfaz del servicio de ZooKeeper, haga clic en **Resource** para entrar en la página **Resource** y compruebe si el número de conexiones del cliente con la dirección IP especificada por **Number of Connections (By Client IP Address)** es grande.

- Si lo es, vaya a **Paso 3**.
- Si no es así, vaya a **Paso 4**.

Paso 3 Compruebe si se produce una fuga de conexión en el proceso del cliente.

Paso 4 Haga clic en  en el **Number of Connections (by Client IP Address)** para entrar en la página **Thresholds** y haga clic en **Modify** en **Operation**. Aumente el umbral haciendo referencia al valor de **maxClientCnxns** seleccionando **Cluster >** *Name of the desired cluster* **> Services** > **ZooKeeper** > **Configurations > All Configurations > quorumpeer**.

Paso 5 Verifique si la alarma se ha borrado.

- Si lo es, no se requiere ninguna otra acción.
- Si no es así, vaya a **Paso 6**.

Recopilar información de fallas.

Paso 6 En el portal del FusionInsight Manager, elija **O&M** > **Log > Download**.

Paso 7 Seleccione **ZooKeeper** en el clúster requerido en el **Service**.

Paso 8 Haga clic en  en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 9 Póngase en contacto con el y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.79 ALM-13008 El uso de ZooKeeper Znode supera el umbral

Descripción

El sistema comprueba el estado de Znode de nivel 2 en el directorio de datos ZooKeeper cada hora. Esta alarma se genera cuando el sistema detecta que el uso de Znode de nivel 2 excede el umbral.

Atributo

ID de alarma	Gravedad de la alarma	Borrado automáticamente
13008	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el nombre del servicio para el que se genera la alarma.
ServiceDirectory	Especifica el directorio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
Trigger Condition	Especifica la causa de la alarma.

Impacto en el sistema

Se escribe una gran cantidad de datos en el directorio de datos de ZooKeeper. Como resultado, ZooKeeper no puede proporcionar los servicios correctamente.

Causas posibles

- Se escribe una gran cantidad de datos en el directorio de datos de ZooKeeper.
- El umbral definido por el usuario es inapropiado.

Procedimiento

Comprobar si se escribe una gran cantidad de datos en el directorio para el que se genera la alarma.

Paso 1 Inicie sesión en el Administrador de FusionInsight, elija **Cluster** > *Name of the desired cluster* > **Services** > **ZooKeeper** y haga clic en **Resource**. Haga clic en **By Znode quantity** en **Used Resources (By Second-Level Znode)** y compruebe si se escribe una gran cantidad de datos en el Znode superior.

- En caso afirmativo, vaya a **Paso 2**.
- Si no, vaya a **Paso 4**.

Paso 2 Inicie sesión en FusionInsight Manager, elija **O&M > Alarm > Alarms**, seleccione **Location** en el cuadro de lista desplegable junto a **ALM-13008 El uso de la cantidad de Znode de ZooKeeper supera el umbral** y obtenga la ruta de Znode en **ServiceDirectory**.

Paso 3 Inicie sesión en el cliente ZooKeeper como usuario del clúster y elimine los datos innecesarios del Znode correspondientes a la alarma.

Paso 4 Inicie sesión en FusionInsight Manager, elija **Cluster** > *Name of the desired cluster* > **Services** > **ZooKeeper** > **Configurations** > **All Configurations**, y busque **max.znode.count**, que es el número máximo de directorios de ZooKeeper. El umbral de alarma es el 80% de este parámetro. Aumente el valor de este parámetro, haga clic en **Save** y reinicie el servicio para que la configuración surta efecto.

Paso 5 Verifique si la alarma se ha borrado.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 6**.

Recopilar información de fallas.

Paso 6 En el portal del FusionInsight Manager, elija **O&M** > **Log > Download**.

Paso 7 Seleccione **ZooKeeper** en el clúster requerido en el **Service**.

Paso 8 Haga clic en  en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 9 Póngase en contacto con el y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.80 ALM-13009 El uso de la capacidad de Znode de ZooKeeper supera el umbral

Descripción

El sistema comprueba el estado de ZNode de nivel 2 en el directorio de datos ZooKeeper cada hora. Esta alarma se genera cuando el sistema detecta que el uso de capacidad excede el umbral.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
13009	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
ServiceDirectory	Especifica el directorio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
Trigger Condition	Especifica el umbral para activar la alarma.

Impacto en el sistema

Se escribe una gran cantidad de datos en el directorio de datos de ZooKeeper. Como resultado, ZooKeeper no puede proporcionar los servicios correctamente.

Causas posibles

- Se ha escrito un gran volumen de datos en el directorio de datos de ZooKeeper.
- El umbral está definido incorrectamente.

Procedimiento

Compruebe si se escribe un gran volumen de datos en el directorio de alarmas.

Paso 1 En FusionInsight Manager, seleccione **O&M**. En el panel de navegación de la izquierda, elija **Alarm** > **Alarms**. Haga clic en la lista desplegable de la fila que contiene **ALM-13009 ZooKeeper ZNode Capacity Usage Exceeds the Threshold** y busque el ZNode para el que se genera la alarma en el área **Location**.

Paso 2 Elija **Cluster** > **Services** > **ZooKeeper**. En la página que se muestra, haga clic en la pestaña **Resource**. En el área **Used Resources (By Second-Level ZNode)**, haga clic en **By capacity** y compruebe si se escribe una gran cantidad de datos en el directorio de ZNode de nivel superior.

- En caso afirmativo, registre el directorio en el que se escribe una gran cantidad de datos y vaya a **Paso 3**.
- Si no, vaya a **Paso 5**.

Paso 3 Compruebe si se pueden eliminar los datos del directorio.

AVISO

Eliminar datos de ZooKeeper es una operación de alto riesgo. Tenga cuidado cuando realice esta acción.

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 5**.

Paso 4 Inicie sesión en el cliente ZooKeeper y elimine los datos innecesarios del directorio en el que se escribe una gran cantidad de datos.

1. Inicie sesión en el directorio de instalación del cliente ZooKeeper por ejemplo, y configure las variables de entorno.

   cd /opt/client

   source bigdata_env

2. Ejecute el siguiente comando para autenticar al usuario (omita este paso para un clúster en modo normal):

   kinit *Component service user*

3. Ejecute el siguiente comando para iniciar sesión en la herramienta de cliente:

   zkCli.sh -server <*Service IP address of the node where any ZooKeeper instance resides*>**:**<*Client port*>

4. Ejecute el siguiente comando para eliminar datos innecesarios:

   delete *Path of the file to be deleted*

Paso 5 Inicie sesión en FusionInsight Manager y elija **Cluster** > **Services** > **ZooKeeper**. En la página que se muestra, haga clic en la pestaña **Configuration**, luego en la subpestaña **All Configurations** y busque **max.data.size**. El valor de **max.data.size** es la cuota de capacidad máxima del directorio ZooKeeper. La unidad es byte. Busque el elemento de configuración **GC_OPTS** y compruebe el valor de **Xmx**.

Paso 6 Compare los valores de **max.data.size** y **Xmx*0.65**. El umbral es el valor más pequeño multiplicado por 80%. Puede cambiar los valores de **max.data.size** y **Xmx*0.65** para aumentar el umbral.

Paso 7 Verifique si la alarma se ha borrado.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 8**.

Recopilar información de fallas.

Paso 8 En FusionInsight Manager, seleccione **O&M**. En el panel de navegación de la izquierda, elija **Log** > **Download**.

Paso 9 Expanda la lista desplegable **Service** y seleccione **ZooKeeper** para el clúster de destino.

Paso 10 Haga clic en  en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 11 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

Información relacionada

Ninguna

9.81 ALM-13010 El uso de Znode de un directorio con cuota configurada supera el umbral

Descripción

El sistema comprueba el uso de Znode de todos los directorios de servicio con cuota configurada cada hora. Esta alarma se genera cuando el sistema detecta que el uso de Znode de nivel 2 excede el umbral.

Atributo

ID de alarma	Gravedad de la alarma	Borrado automáticamente
13010	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.

Nombre	Significado
ServiceName	Especifica el nombre del servicio para el que se genera la alarma.
ServiceDirectory	Especifica el directorio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
Trigger Condition	Especifica la causa de la alarma.

Impacto en el sistema

Se escribe una gran cantidad de datos en el directorio de datos de ZooKeeper. Como resultado, ZooKeeper no puede proporcionar los servicios correctamente.

Causas posibles

- Se escribe una gran cantidad de datos en el directorio de datos de ZooKeeper.
- El umbral definido por el usuario es inapropiado.

Procedimiento

Comprobar si se escribe una gran cantidad de datos en el directorio para el que se genera la alarma.

Paso 1 En FusionInsight Manager, elija **O&M** >**Alarm > Alarms**. Confirme el Znode para el que se genera la alarma en **Location** de esta alarma.

Paso 2 Elija **Cluster** > *Name of the desired cluster* > **Services** > **ZooKeeper** y haga clic en **Resource**. En el caso de **Used Resources (By Second-Level Znode)**, compruebe si se escribe una gran cantidad de datos en el Znode superior.

- En caso afirmativo, vaya a **Paso 3**.
- Si no, vaya a **Paso 5**.

Paso 3 Inicie sesión en el administrador de FusionInsight, elija **O&M > Alarm > Alarms**, seleccione Location en el cuadro de lista desplegable junto a **ALM-13010 Znode Usage of a Directory with Quota Configured Exceeds the Threshold**, y obtenga la ruta de Znode de ServiceDirectory.

Paso 4 Inicie sesión en el cliente de ZooKeeper como usuario del clúster y elimine los datos no deseados en el Znode para el que se genera la alarma.

Paso 5 Inicie sesión en el Administrador de FusionInsight y elija **Cluster** > *Name of the desired cluster* > **Services** > *Component of the top Znode for which the alarm isgenerated*. Elija **Configurations** > **All Configurations**, busque **zk.quota.number**, aumente su valor, haga clic en **Save**.

AVISO

Si el componente del Znode superior para el que se genera la alarma es de ClickHouse, cambie el valor de **ClickHouse.zookeeper.quota.node.count**.

Paso 6 Verifique si la alarma se ha borrado.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 7**.

Recopilar información de fallas.

Paso 7 En el portal del FusionInsight Manager, elija **O&M** > **Log > Download**.

Paso 8 Seleccione **ZooKeeper** en el clúster requerido en el **Service**.

Paso 9 Haga clic en  en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 10 Póngase en contacto con el y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.82 ALM-14000 Servicio HDFS no disponible

Descripción

El sistema comprueba el estado del servicio NameService cada 60 segundos. Esta alarma se genera cuando todos los servicios de NameService son anormales y el sistema considera que el servicio HDFS no está disponible.

Esta alarma se borra cuando al menos un servicio NameService es normal y el sistema considera que el servicio HDFS se recupera.

Atributo

ID de alarma	Gravedad de la alarma	Borrado automáticamente
14000	Crítica	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

HDFS no proporciona servicios para componentes de capa superior basados en servicios HDFS, como HBase y MapReduce. Como resultado, los usuarios no pueden leer ni escribir archivos.

Causas posibles

- El servicio ZooKeeper es anormal.
- Todos los servicios de NameService son anormales.

Procedimiento

Verificar el estado del servicio de ZooKeeper.

Paso 1 En el portal del FusionInsight Manager, seleccione **O&M > Alarm > Alarms**. En la página Alarma, compruebe si se ha informado de **ALM-13000 Servicio ZooKeeper no disponible**.

- En caso afirmativo, vaya a **Paso 2**.
- Si no, vaya a **Paso 4**.

Paso 2 Consulte **ALM-13000 Servicio ZooKeeper no disponible** para corregir el estado de salud de la falla de ZooKeeper y comprueba si el **Running Status** del servicio ZooKeeper se restaura a **Normal**.

- En caso afirmativo, vaya a **Paso 3**.
- Si no, vaya a **Paso 7**.

Paso 3 En la página **O&M > Alarm > Alarms**, compruebe si la alarma está desactivada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 4**.

Manejar la alarma de excepción del servicio NameService.

Paso 4 En el portal del FusionInsight Manager, seleccione **O&M > Alarm > Alarms**. En la página Alarmas, compruebe si se ha informado de **ALM-14010 Servicio NameService no disponible**.

- En caso afirmativo, vaya a **Paso 5**.
- Si no, vaya a **Paso 7**.

Paso 5 Vea **ALM-14010 Servicio NameService no disponible** para controlar los servicios anormales de NameService y compruebe si cada alarma de excepción de servicio de NameService está desactivada.

- En caso afirmativo, vaya a **Paso 6**.
- Si no, vaya a **Paso 7**.

Paso 6 En la página **O&M > Alarm > Alarms**, compruebe si la alarma está desactivada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 7**.

Recopilar información de fallas.

Paso 7 En el portal del FusionInsight Manager, elija **O&M** > **Log > Download**.

Paso 8 Seleccione los siguientes nodos en el clúster requerido desde el **Service**:

- ZooKeeper
- HDFS

Paso 9 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 10 Póngase en contacto con el y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.83 ALM-14001 El uso del disco HDFS supera el umbral

Descripción

El sistema comprueba el uso del disco HDFS cada 30 segundos y compara el uso real del disco HDFS con el umbral. El indicador de uso del disco HDFS tiene un umbral predeterminado, esta alarma se genera cuando el valor del uso del disco de un indicador de sistema de archivos distribuido de Hadoop (HDFS) excede el umbral.

Para cambiar el umbral, elija **O&M** >**Alarm > Thresholds** >*Name of the desired cluster* **> HDFS**.

Cuando el **Trigger Count** es 1, esta alarma se borra cuando el valor del uso del disco del indicador de clúster HDFS es menor o igual que el umbral. Cuando el **Trigger Count** es mayor que 1, esta alarma se borra cuando el valor del uso del disco del indicador de clúster HDFS es menor o igual al 90% del umbral.

Atributo

ID de alarma	Gravedad de la alarma	Borrado automáticamente
14001	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
NameServiceName	Especifica el NameService para el que se genera la alarma.
Trigger Condition	Especifica el umbral que activa la alarma. Si el valor del indicador actual excede este umbral, se genera la alarma.

Impacto en el sistema

La escritura de datos del sistema de archivos distribuido (HDFS) de Hadoop se ve afectada.

Causas posibles

El espacio en disco configurado para el clúster HDFS es insuficiente.

Procedimiento

Compruebe la capacidad del disco y elimine los archivos innecesarios.

Paso 1 En el portal del FusionInsight Manager, elija **Cluster >** *Name of the desired cluster* **> Services** > **HDFS**.

Paso 2 Haga clic en el menú desplegable en la esquina superior derecha de **Chart**, elija **Customize** > **Disk**, y seleccione **Percentage of HDFS Capacity** para comprobar si el uso del disco HDFS excede el umbral (80% de forma predeterminada).

- En caso afirmativo, vaya a **Paso 3**.
- Si no, vaya a **Paso 11**.

Paso 3 En el área **Basic Information**, haga clic en el **NameNode(Active)** del NameService de errores y se mostrará la página HDFS WebUI.

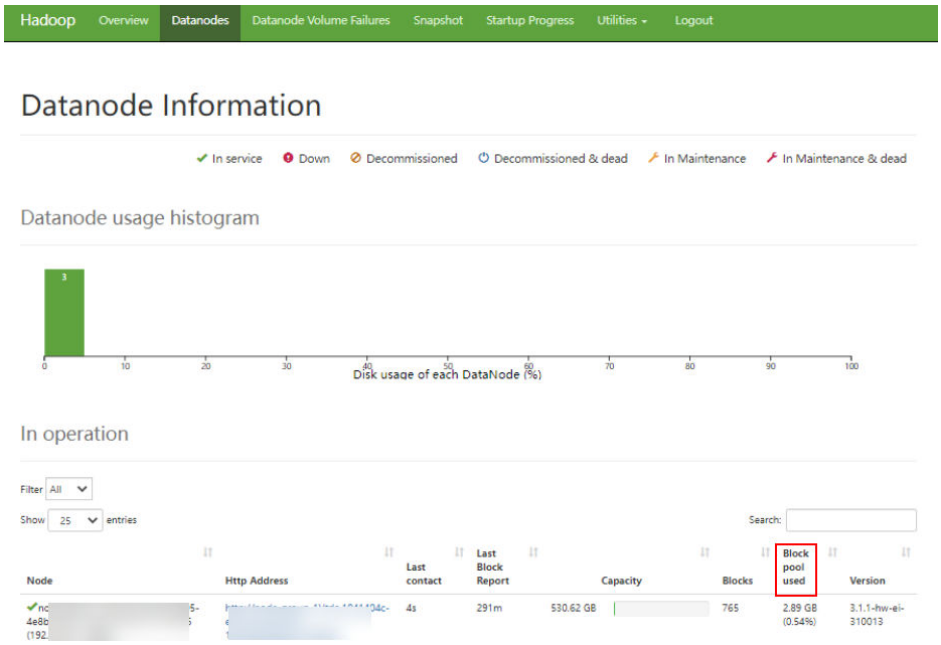
NOTA

De forma predeterminada, el usuario **admin** no tiene los permisos para gestionar otros componentes. Si la página no se puede abrir o el contenido mostrado está incompleto al acceder a la interfaz de usuario nativa de un componente debido a la falta de permisos, puede crear manualmente un usuario con los permisos para gestionar ese componente.

Paso 4 En la interfaz de usuario web HDFS (WebUI), haga clic en la pestaña **Datanodes**. En la columna **Block pool used**, vea el uso del disco de todos los DataNodes para comprobar si el uso del disco de cualquier DataNode excede el umbral.

- En caso afirmativo, vaya a **Paso 6**.
- Si no, vaya a **Paso 11**.

Figura 9-18 Información de Datanode



Paso 5 Inicie sesión en el nodo cliente de como usuario **root**.

Paso 6 Ejecute **cd /opt/client** para cambiar al directorio de instalación del cliente y ejecute **source bigdata_env**. Si el clúster utiliza el modo de seguridad, realice la autenticación de seguridad. Ejecute **kinit hdfs** e introduzca la contraseña como se le solicite. Por favor, obtenga la contraseña del administrador.

Paso 7 Ejecute el comando **hdfs dfs -rm -r** *file or directory* para eliminar archivos innecesarios.

Paso 8 Verifique si la alarma se ha borrado.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 9**.

Expandir el sistema.

Paso 9 Amplíe la capacidad del disco.

Paso 10 Verifique si la alarma se ha borrado.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 11**.

Recopilar información de fallas.

Paso 11 En el portal del FusionInsight Manager, elija **O&M** > **Log > Download**.

Paso 12 Seleccione los siguientes nodos en el clúster requerido desde el **Service**:

- ZooKeeper
- HDFS

Paso 13 Haga clic en  en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 14 Póngase en contacto con el y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.84 ALM-14002 El uso del disco de DataNode supera el umbral

Descripción

El sistema comprueba el uso del disco de DataNode cada 30 segundos y compara el uso real del disco con el umbral. Se proporciona un rango de umbral predeterminado para el uso del disco de DataNode. Esta alarma se genera cuando el uso del disco DataNode excede el umbral.

Para cambiar el umbral, elija **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster* > **HDFS**.

Si **Trigger Count** tiene un valor **1**, esta alarma se borra cuando el uso del disco DataNode es menor o igual al umbral. Si **Trigger Count** es mayor que **1**, esta alarma se borra cuando el uso del disco DataNode es menor o igual al 80% del umbral.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
14002	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger Condition	Especifica el umbral para activar la alarma.

Impacto en el sistema

La falta de espacio en disco afectará a la escritura de datos en HDFS.

Causas posibles

- El espacio en disco configurado para el clúster HDFS es insuficiente.
- La desviación de los datos se produce entre los DataNodes.

Procedimiento

Compruebe si la capacidad del disco del clúster está llena.

Paso 1 En FusionInsight Manager, seleccione **O&M** > **Alarm** > **Alarms** y compruebe si existe la alarma **ALM-14001 El uso del disco HDFS supera el umbral**.

- En caso afirmativo, vaya a **Paso 2**.
- Si no, vaya a **Paso 4**.

Paso 2 Maneje la alarma siguiendo las instrucciones en **ALM-14001 El uso del disco HDFS supera el umbral** y compruebe si la alarma está desactivada.

- En caso afirmativo, vaya a **Paso 3**.
- Si no, vaya a **Paso 11**.

Paso 3 Elija **O&M** > **Alarm** > **Alarms** y compruebe si la alarma está desactivada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 4**.

Verifique el estado del balanceo de DataNodes.

Paso 4 En FusionInsight Manager, seleccione **Hosts**. Compruebe si el número de DataNodes en cada rack es casi el mismo. Si la diferencia es grande, ajuste los racks a los que pertenecen DataNodes para asegurarse de que el número de DataNodes en cada rack es casi el mismo. Reinicie el servicio HDFS para que la configuración surta efecto.

Paso 5 Elija **Cluster** > *Name of the desired cluster* > **Services** > **HDFS**.

Paso 6 En el área **Basic Information**, haga clic en **NameNode(Active)**. Se muestra la HDFS web UI.

NOTA

De forma predeterminada, el usuario **admin** no tiene los permisos para gestionar otros componentes. Si la página no se puede abrir o el contenido mostrado está incompleto al acceder a la interfaz de usuario nativa de un componente debido a la falta de permisos, puede crear manualmente un usuario con los permisos para gestionar ese componente.

Paso 7 En el área **Summary** de la HDFS web UI, compruebe si el valor de **Max** es un 10% mayor que el de **Median** en **DataNodes usages**.

- En caso afirmativo, vaya a **Paso 8**.
- Si no, vaya a **Paso 11**.

Paso 8 Equilibre los datos sesgados en el clúster. Inicie sesión en el cliente de como usuario **root**. Si el clúster está en modo normal, ejecute el comando **su - omm** para cambiar a usuario **omm**. Ejecute el comando **cd** para ir al directorio de instalación del cliente y ejecute el comando **source bigdata_env**. Si el clúster utiliza el modo de seguridad, realice la autenticación de seguridad. Ejecute **kinit hdfs** e introduzca la contraseña como se le solicite. Obtenga la contraseña del administrador del clúster de MRS.

Paso 9 Ejecute el siguiente comando para equilibrar la distribución de datos:

hdfs balancer -threshold 10

Paso 10 Espere varios minutos y compruebe si la alarma está desactivada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 11**.

Recopilar información de fallas.

Paso 11 En FusionInsight Manager, seleccione **O&M**. En el panel de navegación de la izquierda, elija **Log** > **Download**.

Paso 12 Expanda la lista desplegable junto al campo **Service**. En el cuadro de diálogo **Services** que se muestra, seleccione **HDFS** para el clúster de destino.

Paso 13 Haga clic en  en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 14 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

Información relacionada

Ninguna

9.85 ALM-14003 El número de bloques HDFS perdidos supera el umbral

Descripción

El sistema comprueba los bloques perdidos cada 30 segundos y compara los bloques perdidos reales con el umbral. El indicador de bloques perdidos tiene un umbral predeterminado. Esta alarma se genera cuando el número de bloques HDFS perdidos excede el umbral.

Para cambiar el umbral, elija **O&M** >**Alarm > Thresholds** > *Name of the desired cluster* **> HDFS**.

Si **Trigger Count** es de **1**, esta alarma se borra cuando el valor de los bloques HDFS perdidos es menor o igual que el umbral. Si **Trigger Count** es mayor que **1**, esta alarma se borra cuando el valor de los bloques HDFS perdidos es menor o igual al 90% del umbral.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
14003	Importante **NOTA** La gravedad de la alarma en MRS 3.1.5 es de **Critical**.	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
NameServiceName	Especifica el NameService para el que se genera la alarma.
Trigger Condition	Especifica el umbral para activar la alarma.

Impacto en el sistema

Los datos almacenados en HDFS se pierden. HDFS puede entrar en el modo de seguridad y no puede proporcionar servicios de escritura. Los datos de bloques perdidos no se pueden restaurar.

Causas posibles

- La instancia DataNode es anormal.
- Los datos se eliminan.

Procedimiento

Comprobar la instancia de DataNode.

Paso 1 En FusionInsight Manager, elija **Cluster** > *Name of the desired cluster* > **Services** > **HDFS** > **Instance**.

Paso 2 Comprueba si el **Running Status** de todas las instancias de DataNode es de tipo **Normal**.

- En caso afirmativo, vaya a **Paso 11**.
- Si no, vaya a **Paso 3**.

Paso 3 Reinicie la instancia DataNode y compruebe si la instancia DataNode se reinicia correctamente.

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 5**.

Paso 4 Elija **O&M** > **Alarm** > **Alarms** y compruebe si la alarma está desactivada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 5**.

Eliminar el archivo dañado.

Paso 5 En FusionInsight Manager, seleccione **Cluster** > *Name of the desired cluster* > **Services** > **HDFS** > **NameNode(Active)**. En la página WebUI del HDFS, vea la información sobre los bloques perdidos.

NOTA

- Si se pierde un bloque, se muestra una línea en rojo en el WebUI.
- De forma predeterminada, el usuario **admin** no tiene los permisos para gestionar otros componentes. Si la página no se puede abrir o el contenido mostrado está incompleto al acceder a la interfaz de usuario nativa de un componente debido a la falta de permisos, puede crear manualmente un usuario con los permisos para gestionar ese componente.

Paso 6 El usuario comprueba si el archivo que contiene el bloque de datos perdido es útil.

NOTA

Los archivos generados en los directorios **/mr-history**, **/tmp/hadoop-yarn** y **/tmp/logs** durante la ejecución de tareas de MapReduce son innecesarios.

- En caso afirmativo, vaya a **Paso 7**.
- Si no, vaya a **Paso 8**.

Paso 7 El usuario comprueba si el archivo que contiene el bloque de datos perdido está respaldado.

- En caso afirmativo, vaya a **Paso 8**.
- Si no, vaya a **Paso 11**.

Paso 8 Inicie sesión en el cliente HDFS como usuario **root**. La contraseña de usuario la define el usuario antes de la instalación. Póngase en contacto con el administrador del clúster MRS para obtener la contraseña. Ejecute los siguientes comandos:

- Modo de seguridad:

  cd *Client installation directory*

  source bigdata_env

  kinit hdfs

- Modo normal:

  su - omm

  cd *Client installation directory*

  source bigdata_env

Paso 9 En el cliente de nodo, ejecute **hdfs fsck / -delete** para eliminar el archivo perdido. Si el archivo donde se encuentra el bloque perdido es un archivo útil, debe volver a escribir el archivo para restaurar los datos.

NOTA

Paso 10 Elija **O&M** > **Alarm** > **Alarms** y compruebe si la alarma está desactivada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 11**.

Recopilar información de fallas.

Paso 11 En FusionInsight Manager, elija **O&M** > **Log** > **Download**.

Paso 12 Expanda la lista desplegable junto al campo **Service**. En el cuadro de diálogo **Services** que se muestra, seleccione **HDFS** para el clúster de destino.

Paso 13 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 14 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

Información relacionada

Ninguna

9.86 ALM-14006 Número de archivos HDFS supera el umbral

Descripción

El sistema comprueba periódicamente el número de archivos HDFS cada 30 segundos y compara el número de archivos HDFS con el umbral. Esta alarma se genera cuando el sistema detecta que el número de archivos HDFS excede el umbral.

Si **Trigger Count** es **1**, esta alarma se borra cuando el número de archivos HDFS es inferior o igual al umbral. Si **Trigger Count** es mayor que **1**, esta alarma se borra cuando el número de archivos HDFS es menor o igual al 90% del umbral.

Atributo

ID de alarma	Gravedad de la alarma	Borrado automático
14006	Leves	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
NameServiceName	Especifica el NameService para el que se genera la alarma.
Trigger Condition	Especifica el umbral para activar la alarma.

Impacto en el sistema

El espacio de almacenamiento en disco es insuficiente, lo que puede provocar un error en la importación de datos. El rendimiento del sistema HDFS se ve afectado.

Causas posibles

El número de archivos HDFS excede el umbral.

Procedimiento

Comprobar el número de archivos en el sistema.

Paso 1 En FusionInsight Manager, compruebe el número de archivos HDFS. Específicamente, elija **Cluster** > *Name of the desired cluster* > **Services** > **HDFS**. Haga clic en el menú desplegable en la esquina superior derecha de **Chart**, elija **Customize** > **File and Block** y seleccione **HDFS File** y **Total Blocks**.

Paso 2 Seleccione **Cluster** > *Name of the desired cluster* > **Services** > **HDFS** > **Configurations** > **All Configurations** y busque el parámetro **GC_OPTS** en **NameNode**.

Paso 3 Configure el umbral del número de objetos del archivo de configuración. Específicamente, cambie el valor de **Xmx** (GB) en el parámetro **GC_OPTS**. El umbral (especificado por y) se calcula de la siguiente manera: y = 0.2007 x Xmx - 0.6312, donde x indica la capacidad de memoria Xmx (GB) e indica el número de archivos (unidad: kW). Ajuste el tamaño de la memoria según sea necesario.

Paso 4 Confirme que el valor de **GC_PROFILE** es **custom** para que la configuración **GC_OPTS** surta efecto. Haga clic en **Save** y elija **More** > **Restart Instance** para reiniciar el servicio.

Paso 5 Verifique si la alarma se ha borrado.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 6**.

Compruebe si existen archivos innecesarios en el sistema.

Paso 6 Inicie sesión en el cliente HDFS como usuario **root**. Ejecute **cd** para cambiar al directorio de instalación del cliente y ejecute **source bigdata_env** para configurar las variables de entorno.

Si el clúster utiliza el modo de seguridad, realice la autenticación de seguridad.

Ejecute el comando **kinit hdfs** e introduzca la contraseña como se le solicite. Obtenga la contraseña del administrador del clúster de MRS.

Paso 7 Ejecute **hdfs dfs -ls** *file or directory* para comprobar si se pueden eliminar los archivos del directorio.

- En caso afirmativo, vaya a **Paso 8**.
- Si no, vaya a **Paso 9**.

Paso 8 Ejecute el comando **hdfs dfs -rm -r** *file or directory path*. Después de eliminar los archivos innecesarios, espere hasta que los archivos se conserven en la papelera de reciclaje durante un período más largo que el valor de **fs.trash.interval** en el NameNode. Después compruebe si la alarma se ha rectificado.

NOTA

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 9**.

Recopilar información de fallas.

Paso 9 En FusionInsight Manager, elija **O&M** > **Log** > **Download**.

Paso 10 Expanda la lista desplegable junto al campo **Service**. En el cuadro de diálogo **Services** que se muestra, seleccione **HDFS** para el clúster de destino.

Paso 11 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 12 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

Información relacionada

Reglas de configuración del parámetro JVM de NameNode

Valor predeterminado del parámetro JVM de NameNode **GC_OPTS**:

-Xms2G -Xmx4G -XX:NewSize=128M -XX:MaxNewSize=256M -XX:MetaspaceSize=128M -XX:MaxMetaspaceSize=128M -XX:+UseConcMarkSweepGC -XX:+CMSParallelRemarkEnabled -XX:CMSInitiatingOccupancyFraction=65 -XX:+PrintGCDetails -Dsun.rmi.dgc.client.gcInterval=0x7FFFFFFFFFFFFE -Dsun.rmi.dgc.server.gcInterval=0x7FFFFFFFFFFFFE -XX:-OmitStackTraceInFastThrow -XX:+PrintGCDateStamps -XX:+UseGCLogFileRotation -XX:NumberOfGCLogFiles=10 -XX:GCLogFileSize=1M -Djdk.tls.ephemeralDHKeySize=3072 -Djdk.tls.rejectClientInitiatedRenegotiation=true -Djava.io.tmpdir=${Bigdata_tmp_dir}

El número de archivos NameNode es proporcional al tamaño de memoria utilizado del NameNode. Cuando los objetos de archivo cambian, debe cambiar **-Xms2G -Xmx4G -XX:NewSize=128M -XX:MaxNewSize=256M** en el valor predeterminado. En la siguiente tabla se enumeran los valores de referencia.

Tabla 9-2 Configuración de JVM de NameNode

Número de objetos de archivo	Valor de referencia
10,000,000	-Xms6G -Xmx6G -XX:NewSize=512M -XX:MaxNewSize=512M
20,000,000	-Xms12G -Xmx12G -XX:NewSize=1G -XX:MaxNewSize=1G
50,000,000	-Xms32G -Xmx32G -XX:NewSize=3G -XX:MaxNewSize=3G
100,000,000	-Xms64G -Xmx64G -XX:NewSize=6G -XX:MaxNewSize=6G
200,000,000	-Xms96G -Xmx96G -XX:NewSize=9G -XX:MaxNewSize=9G
300,000,000	-Xms164G -Xmx164G -XX:NewSize=12G -XX:MaxNewSize=12G

9.87 ALM-14007 El uso de memoria heap de NameNode supera el umbral

Descripción

El sistema comprueba el uso de la memoria heap de HDFS NameNode cada 30 segundos y compara el uso real de la memoria heap con el umbral. El uso de la memoria heap de HDFS NameNode tiene un umbral predeterminado. Esta alarma se genera cuando el uso de la memoria heap de HDFS NameNode excede el umbral.

Puede cambiar el umbral en **O&M** > **Alarm > Thresholds** > *Name of the desired cluster* **> HDFS**.

Cuando el **Trigger Count** es 1, esta alarma se borra cuando el uso de memoria heap de HDFS NameNode es menor o igual que el umbral. Cuando el **Trigger Count** es mayor que 1, esta alarma se borra cuando el uso de memoria heap de HDFS NameNode es menor o igual al 90% del umbral.

Atributo

ID de alarma	Gravedad de la alarma	Borrado automáticamente
14007	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger condition	Especifica el umbral que activa la alarma. Si el valor del indicador actual excede este umbral, se genera la alarma.

Impacto en el sistema

El uso de la memoria heap de HDFS NameNode es demasiado alto, lo que afecta al rendimiento de lectura/escritura de datos del HDFS.

Causas posibles

La memoria heap de HDFS NameNode es insuficiente.

Procedimiento

Eliminar archivos innecesarios.

Paso 1 Inicie sesión en el cliente HDFS como usuario **root**. Ejecute **cd** para cambiar al directorio de instalación del cliente y ejecute **source bigdata_env**.

Si el clúster utiliza el modo de seguridad, realice la autenticación de seguridad.

Ejecute el comando **kinit hdfs** e introduzca la contraseña como se le solicite. Obtenga la contraseña del administrador.

Paso 2 Ejecute el comando **hdfs dfs -rm -r** *file or directory* para eliminar archivos innecesarios.

Paso 3 Verifique si la alarma se ha borrado.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 4**.

Comprobar el uso y la configuración de la memoria JVM de NameNode.

Paso 4 En el portal del FusionInsight Manager, elija **Cluster** > *Name of the desired cluster* > **Services** > **HDFS**.

Paso 5 En el área **Basic Information**, haga clic en **NameNode(Active)** para ir a HDFS WebUI.

NOTA

De forma predeterminada, el usuario **admin** no tiene los permisos para gestionar otros componentes. Si la página no se puede abrir o el contenido mostrado está incompleto al acceder a la interfaz de usuario nativa de un componente debido a la falta de permisos, puede crear manualmente un usuario con los permisos para gestionar ese componente.

Paso 6 En HDFS WebUI, haga clic en la pestaña **Overview**. En **Summary**, compruebe el número de archivos, directorios y bloques en el HDFS.

Paso 7 En el portal del FusionInsight Manager, elija **Cluster** > *Name of the desired cluster* > **Services** > **HDFS** > **Configurations** > **All Configurations**. En **Search**, escriba **GC_OPTS** para comprobar el parámetro de memoria **GC_OPTS** de **HDFS->NameNode**.

Ajustar la configuración en el sistema.

Paso 8 Compruebe si la memoria está configurada correctamente según el número de archivos en **Paso 6** y los parámetros de memoria heap de NameNode en **Paso 7**.

- En caso afirmativo, vaya a **Paso 9**.
- Si no, vaya a **Paso 11**.

NOTA

La asignación recomendada entre el número de objetos de archivo HDFS (objetos de sistema de archivos = archivos + bloques) y los parámetros JVM configurados para NameNode es la siguiente:

- Si el número de objetos de archivo llega a 10,000,000, se recomienda establecer los parámetros de JVM de la siguiente manera: -Xms6G -Xmx6G -XX:NewSize=512M -XX:MaxNewSize=512M
- Si el número de objetos de archivo llega a 20,000,000, se recomienda establecer los parámetros JVM de la siguiente manera: -Xms12G -Xmx12G -XX:NewSize=1G -XX:MaxNewSize=1G
- Si el número de objetos de archivo llega a 50,000,000, se recomienda establecer los parámetros JVM de la siguiente manera: -Xms32G -Xmx32G -XX:NewSize=3G -XX:MaxNewSize=3G
- Si el número de objetos de archivo llega a 100,000,000, se recomienda establecer los parámetros JVM de la siguiente manera: -Xms64G -Xmx64G -XX:NewSize=6G -XX:MaxNewSize=6G
- Si el número de objetos de archivo llega a 200,000,000, se recomienda establecer los parámetros JVM de la siguiente manera: -Xms96G -Xmx96G -XX:NewSize=9G -XX:MaxNewSize=9G
- Si el número de objetos de archivo llega a 300,000,000, se recomienda establecer los parámetros JVM de la siguiente manera: -Xms164G -Xmx164G -XX:NewSize=12G -XX:MaxNewSize=12G

Paso 9 Modifique los parámetros de memoria heap del NameNode basándose en la asignación entre el número de objetos de archivo y la memoria. Haga clic en **Save** y elija **Dashboard** > **More** > **Restart Service**.

Paso 10 Verifique si la alarma se ha borrado.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 11**.

Recopilar información de fallas.

Paso 11 En el portal del FusionInsight Manager, elija **O&M** > **Log > Download**.

Paso 12 Seleccione los siguientes nodos en el clúster requerido desde el **Service**:

- ZooKeeper
- HDFS

Paso 13 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 14 Póngase en contacto con el y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.88 ALM-14008 El uso de memoria heap de DataNode supera el umbral

Descripción

El sistema comprueba el uso de la memoria heap de HDFS DataNode cada 30 segundos y compara el uso real de la memoria heap con el umbral. El uso de la memoria heap de HDFS DataNode tiene un umbral predeterminado. Esta alarma se genera cuando el uso de la memoria heap de HDFS DataNode excede el umbral.

Puede cambiar el umbral en **O&M** > **Alarm > Thresholds** > *Name of the desired cluster* **> HDFS**.

Cuando el **Trigger Count** es 1, esta alarma se borra cuando el uso de la memoria heap de HDFS de DataNode es menor o igual al umbral. Cuando el **Trigger Count** es mayor que 1, esta alarma se borra cuando el uso de memoria heap de HDFS DataNode es menor o igual al 90% del umbral.

Atributo

ID de alarma	Gravedad de la alarma	Borrado automáticamente
14008	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger condition	Especifica el umbral que activa la alarma. Si el valor del indicador actual excede este umbral, se genera la alarma.

Impacto en el sistema

El uso de la memoria heap de HDFS DataNode es demasiado alto, lo que afecta al rendimiento de lectura/escritura de datos del HDFS.

Causas posibles

La memoria heap de HDFS DataNode es insuficiente.

Procedimiento

Eliminar archivos innecesarios.

Paso 1 Inicie sesión en el cliente HDFS como usuario **root**. Ejecute **cd** para cambiar al directorio de instalación del cliente y ejecute **source bigdata_env**.

Si el clúster utiliza el modo de seguridad, realice la autenticación de seguridad.

Ejecute el comando **kinit hdfs** e introduzca la contraseña como se le solicite. Obtenga la contraseña del administrador.

Paso 2 Ejecute el comando **hdfs dfs -rm -r** *file or directory* para eliminar archivos innecesarios.

Paso 3 Verifique si la alarma se ha borrado.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 4**.

Comprobar el uso y la configuración de la memoria JVM de DataNode.

Paso 4 En el portal del FusionInsight Manager, elija **Cluster** > *Name of the desired cluster* > **Services** > **HDFS**.

Paso 5 En el área **Basic Information**, haga clic en **NameNode(Active)** para ir a HDFS WebUI.

NOTA

De forma predeterminada, el usuario **admin** no tiene los permisos para gestionar otros componentes. Si la página no se puede abrir o el contenido mostrado está incompleto al acceder a la interfaz de usuario nativa de un componente debido a la falta de permisos, puede crear manualmente un usuario con los permisos para gestionar ese componente.

Paso 6 En HDFS WebUI, haga clic en la pestaña **DataNodes** y compruebe el número de bloques de todos los DataNodes relacionados con la alarma.

Paso 7 En el portal del FusionInsight Manager, elija **Cluster** > *Name of the desired cluster* > **Services** > **HDFS** > **Configurations** > **All Configurations**. En **Search**, introduzca **GC_OPTS** para comprobar el parámetro de memoria GC_OPTS de **HDFS->DataNode**.

Ajustar la configuración en el sistema.

Paso 8 Compruebe si la memoria está configurada correctamente según el número de bloques en **Paso 6** y los parámetros de memoria heap de DataNode en **Paso 7**.

- En caso afirmativo, vaya a **Paso 9**.
- Si no, vaya a **Paso 11**.

NOTA

La asignación entre el número promedio de bloques de una instancia de DataNode y la memoria DataNode es la siguiente:

- Si el número promedio de bloques de una instancia de DataNode llega a 2,000,000, los valores de referencia de los parámetros JVM del DataNode son los siguientes: -Xms6G -Xmx6G -XX:NewSize=512M -XX:MaxNewSize=512M
- Si el número promedio de bloques de una instancia de DataNode llega a 5,000,000, los valores de referencia de los parámetros JVM del DataNode son los siguientes: -Xms12G -Xmx12G -XX:NewSize=1G -XX:MaxNewSize=1G

Paso 9 Modifique los parámetros de memoria heap del DataNode basándose en la asignación entre el número de bloques y la memoria. Haga clic en **Save** y elija **Dashboard** > **More** > **Restart Service**.

Paso 10 Verifique si la alarma se ha borrado.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 11**.

Recopilar información de fallas.

Paso 11 En el portal del FusionInsight Manager, elija **O&M** > **Log > Download**.

Paso 12 Seleccione **HDFS** en el clúster requerido en el **Service**.

Paso 13 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 14 Póngase en contacto con el y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.89 ALM-14009 Número de Dead DataNodes supera el umbral

Descripción

El sistema detecta periódicamente el número de DataNodes muertos en el clúster HDFS cada 30 segundos y compara el número con el umbral. El número de DataNodes en el estado Dead tiene un umbral predeterminado. Esta alarma se genera cuando el número excede el umbral.

Puede cambiar el umbral en **O&M** > **Alarm > Thresholds** > *Name of the desired cluster* **> HDFS**.

Cuando el **Trigger Count** es 1, esta alarma se borra cuando el número de DataNodes muertos es menor o igual que el umbral. Cuando el **Trigger Count** es mayor que 1, esta alarma se borra cuando el número de DataNodes muertos es menor o igual al 90% del umbral.

Atributo

ID de alarma	Gravedad de la alarma	Borrado automáticamente
14009	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
NameServiceName	Especifica el NameService para el que se genera la alarma.
Trigger condition	Especifica el umbral que activa la alarma. Si el valor del indicador actual excede este umbral, se genera la alarma.

Impacto en el sistema

Los DataNodes que están en estado Dead no pueden proporcionar servicios HDFS.

Causas posibles

- DataNodes están defectuosos o sobrecargados.
- La red entre el NameNode y el DataNode está desconectada u ocupada.
- Los NameNodes están sobrecargados.
- Los NameNodes no se reinician después de eliminar el DataNode.

Procedimiento

Comprobar si los DataNodes están defectuosos.

Paso 1 En el portal del FusionInsight Manager, elija **Cluster >** *Name of the desired cluster* **> Services** > **HDFS**. Se muestra la página **HDFS Status**.

Paso 2 En el área **Basic Information**, haga clic en **NameNode(Active)** para ir a HDFS WebUI.

NOTA

De forma predeterminada, el usuario **admin** no tiene los permisos para gestionar otros componentes. Si la página no se puede abrir o el contenido mostrado está incompleto al acceder a la interfaz de usuario nativa de un componente debido a la falta de permisos, puede crear manualmente un usuario con los permisos para gestionar ese componente.

Paso 3 En HDFS WebUI, haga clic en la pestaña **Datanodes**. En el área **In operation**, haga clic en **Filter** para comprobar si **down** está en la lista desplegable.

- En caso afirmativo, seleccione **down**, registre la información sobre el DataNodes filtrado y vaya a **Paso 4**.
- Si no, vaya a **Paso 8**.

Paso 4 En el portal del FusionInsight Manager, seleccione **Cluster >** *Name of the desired cluster* > **Services** > **HDFS** > **Instance** para comprobar si las DataNodes registradas existen en la lista de instancias.

- Si existen todas las DataNodes grabadas, vaya a **Paso 5**.
- Si no existe ninguna de las DataNodes grabadas, vaya a **Paso 6**.
- Si existen algunos de los DataNodes grabados, vaya a **Paso 7**.

Paso 5 Localice la instancia DataNode, haga clic en **More** > **Restart Instance** para reiniciarla y compruebe si la alarma está borrada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 8**.

Paso 6 Seleccione todas las instancias de NameNode, elija **More** > **Instance Rolling Restart** para reiniciarlas y compruebe si la alarma está desactivada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 16**.

Paso 7 Seleccione todas las instancias de NameNode y elija **More** > **Instance Rolling Restart** para reiniciarlas. Localice la instancia DataNode, haga clic en **More** > **Restart Instance** para reiniciarla y compruebe si la alarma está borrada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 8**.

Comprobar el estado de la red entre NameNode y DataNode.

Paso 8 Inicie sesión en el DataNode defectuoso en la página de gestión como usuario **root**, y ejecute el comando **ping** *IP address of the NameNode* para comprobar si la red entre el DataNode y el NameNode es anormal.

En la página FusionInsight Manager, elija **Cluster >** *Name of the desired cluster* **> Services** > **HDFS** > **Instance**. En la lista de instancias, vea la dirección IP del plano de servicio del DataNode defectuoso.

- En caso afirmativo, vaya a **Paso 9**.
- Si no, vaya a **Paso 10**.

Paso 9 Rectifique la falla de red y compruebe si la alarma está borrada.

- De ser así, no se requiere ninguna acción adicional.

- Si no, vaya a **Paso 10**.

Comprobar si el DataNode está sobrecargado.

Paso 10 En el portal del FusionInsight Manager, seleccione **O&M > Alarm > Alarms** y compruebe si existe la alarma **ALM-14008 El uso de memoria de HDFS DataNode supera el umbral**.

- En caso afirmativo, vaya a **Paso 11**.
- Si no, vaya a **Paso 13**.

Paso 11 Vea **ALM-14008 El uso de memoria de HDFS DataNode supera el umbral** para manejar la alarma y comprobar si la alarma está desactivada.

- En caso afirmativo, vaya a **Paso 12**.
- Si no, vaya a **Paso 13**.

Paso 12 Compruebe si la alarma está borrada de la lista de alarmas.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 13**.

Comprobar si NameNode está sobrecargado.

Paso 13 En el portal del FusionInsight Manager, seleccione **O&M > Alarm > Alarms** y compruebe si existe la alarma **ALM-14007 El uso de memoria de NameNode de HDFS supera el umbral**.

- En caso afirmativo, vaya a **Paso 14**.
- Si no, vaya a **Paso 16**.

Paso 14 Vea **ALM-14007 El uso de memoria de NameNode de HDFS supera el umbral** para manejar la alarma y comprobar si la alarma está desactivada.

- En caso afirmativo, vaya a **Paso 15**.
- Si no, vaya a **Paso 16**.

Paso 15 Compruebe si la alarma está borrada de la lista de alarmas.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 16**.

Recopilar información de fallas.

Paso 16 En el portal del FusionInsight Manager, elija **O&M** > **Log > Download**.

Paso 17 Seleccione **HDFS** en el clúster requerido en el **Service**.

Paso 18 Haga clic en  en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 19 Póngase en contacto con el y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.90 ALM-14010 El servicio NameService es anormal

Descripción

El sistema comprueba el estado del servicio NameService cada 180 segundos. Esta alarma se genera cuando el servicio NameService no está disponible.

Esta alarma se borra cuando se recupera el servicio NameService.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
14010	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
NameServiceName	Especifica el NameService para el que se genera la alarma.

Impacto en el sistema

HDFS no proporciona servicios para componentes de capa superior basados en el servicio NameService, como HBase y MapReduce. Como resultado, los usuarios no pueden leer ni escribir archivos.

Causas posibles

- El servicio KrbServer es anormal.
- El JournalNode es defectuosa.
- El DataNode es defectuosa.

- La capacidad del disco es insuficiente.
- El NameNode entra en modo seguro.

Procedimiento

Comprobar el estado de servicio KrbServer.

Paso 1 En FusionInsight Manager, elija **Cluster** > *Name of the desired cluster* > **Services**.

Paso 2 Compruebe si el servicio KrbServer existe.

- En caso afirmativo, vaya a **Paso 3**.
- Si no, vaya a **Paso 6**.

Paso 3 Haga clic en **KrbServer**.

Paso 4 Haga clic en **Instances**. En la página de gestión del KrbServer, seleccione la instancia defectuosa y elija **More** > **Restart Instance**. Compruebe si la instancia se reinicia correctamente.

- En caso afirmativo, vaya a **Paso 5**.
- Si no, vaya a **Paso 24**.

Paso 5 Elija **O&M** > **Alarm** > **Alarms** y compruebe si la alarma está desactivada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 6**.

Comprobar el estado de instancia de JournalNode.

Paso 6 En FusionInsight Manager, elija **Cluster** > *Name of the desired cluster* > **Services**.

Paso 7 Elija **HDFS** > **Instances**.

Paso 8 Comprueba si el **Running Status** del JournalNode es **Normal**.

- En caso afirmativo, vaya a **Paso 11**.
- Si no, vaya a **Paso 9**.

Paso 9 Seleccione el JournalNode defectuoso y elija **More** > **Restart Instance**. Compruebe si el JournalNode se reinicia correctamente.

- En caso afirmativo, vaya a **Paso 10**.
- Si no, vaya a **Paso 24**.

Paso 10 Elija **O&M** > **Alarm** > **Alarms** y compruebe si la alarma está desactivada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 11**.

Comprobar el estado de instancia de DataNode.

Paso 11 En FusionInsight Manager, elija **Cluster** > *Name of the desired cluster* > **Services** > **HDFS**.

Paso 12 Haga clic en **Instances** y verifique si el **Running Status** de todos los DataNodes es **Normal**.

- En caso afirmativo, vaya a **Paso 15**.
- Si no, vaya a **Paso 13**.

Paso 13 Haga clic en **Instances**. En la página de gestión del DataNode, seleccione la instancia defectuosa y elija **More** > **Restart Instance**. Compruebe si el DataNode se reinicia correctamente.

- En caso afirmativo, vaya a **Paso 14**.
- Si no, vaya a **Paso 15**.

Paso 14 Elija **O&M** > **Alarm** > **Alarms** y compruebe si la alarma está desactivada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 15**.

Comprobar estado de disco.

Paso 15 En FusionInsight Manager, elija **Cluster** > *Name of the desired cluster* > **Host**.

Paso 16 En la columna **Disk**, compruebe si el espacio en disco es insuficiente.

- En caso afirmativo, vaya a **Paso 17**.
- Si no, vaya a **Paso 19**.

Paso 17 Amplíe la capacidad del disco.

Paso 18 Elija **O&M** > **Alarm** > **Alarms** y compruebe si la alarma está desactivada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 19**.

Comprobar si NameNode está en el modo seguro.

Paso 19 En FusionInsight Manager, elija **Cluster** > *Name of the desired cluster* > **Services** > **HDFS**. Haga clic en **NameNode(Active)** del NameService anormal. Se muestra NameNode web UI.

NOTA

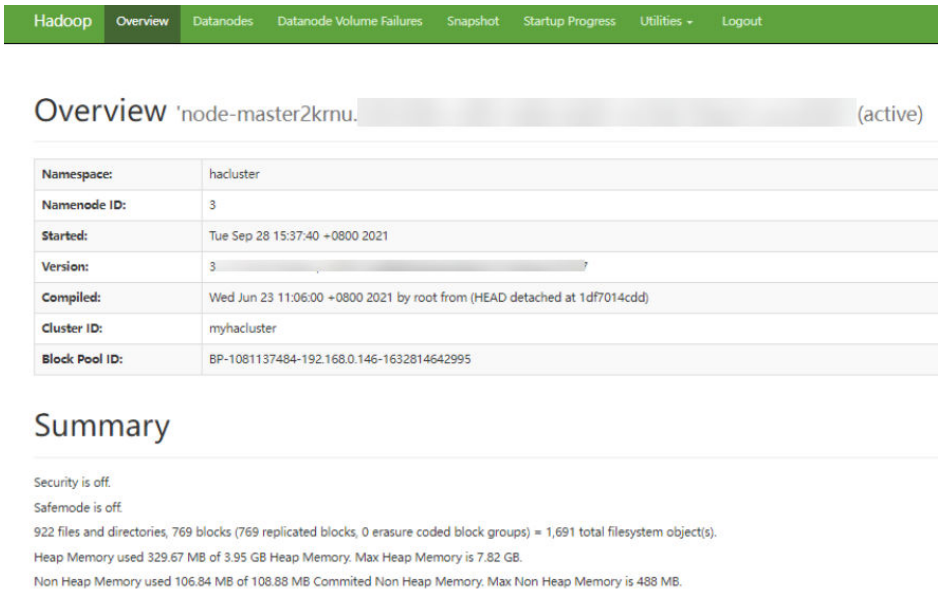
De forma predeterminada, el usuario admin no tiene los derechos de gestión de otros componentes. Si la página no se puede abrir o el contenido no se muestra completamente debido a un permiso insuficiente al acceder a la página nativa de un componente, puede crear manualmente un usuario con los derechos de gestión del componente correspondiente para iniciar sesión en el componente.

Paso 20 En la NameNode web UI, compruebe si se muestra "Safe mode is ON."

La información detrás de **Safe mode is ON** es información de alarma y se muestra en función de las condiciones reales.

- En caso afirmativo, vaya a **Paso 21**.
- Si no, vaya a **Paso 24**.

Figura 9-19 Descripción



Paso 21 Inicie sesión en el cliente como usuario **root**. Ejecute el comando **cd** para ir al directorio de instalación del cliente y ejecute el comando **source bigdata_env**. Si el clúster utiliza el modo de seguridad, realice la autenticación de seguridad. Ejecute el comando **kinit hdfs** e introduzca la contraseña como se le solicite. La contraseña se puede obtener del administrador del clúster MRS. Si el clúster utiliza el modo de no seguridad, inicie sesión como usuario **omm** y ejecute el comando. Asegúrese de que el usuario **omm** tiene el permiso de ejecución del cliente.

Paso 22 Ejecute **hdfs dfsadmin -safemode leave**.

Paso 23 Elija **O&M** > **Alarm** > **Alarms** y compruebe si la alarma está desactivada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 24**.

Recopilar información de fallas.

Paso 24 En FusionInsight Manager, seleccione **O&M**. En el panel de navegación de la izquierda, elija **Log** > **Download**.

Paso 25 En el área **Service**, seleccione los siguientes nodos del clúster deseado.

- ZooKeeper
- HDFS

Paso 26 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 27 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

Información relacionada

Ninguna

9.91 ALM-14011 El directorio de datos de DataNode no está configurado correctamente

Descripción

El parámetro de DataNode **dfs.datanode.data.dir** especifica los directorios de datos de DataNode. Esta alarma se genera cuando no se puede crear un directorio de datos configurado, un directorio de datos utiliza el mismo disco que otros directorios críticos del sistema o varios directorios utilizan el mismo disco inmediatamente.

Esta alarma se borra cuando el directorio de datos de DataNode está configurado correctamente y este DataNode para el que se genera la alarma se reinicia.

Atributo

ID de alarma	Gravedad de la alarma	Borrado automáticamente
14011	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

Si el directorio de datos de DataNode está montado en el directorio raíz o en un directorio crítico, el espacio en disco del directorio raíz o directorio crítico se agotará después de mucho tiempo en ejecución y el sistema estará defectuoso.

Si el directorio de datos de DataNode no está configurado correctamente, el rendimiento de HDFS se deteriorará.

Causas posibles

- No se puede crear el directorio de datos de DataNode.
- El directorio de datos de DataNode utiliza el mismo disco que los directorios críticos, como / o **/boot**.
- Varios directorios en el directorio de datos de DataNode utilizan el mismo disco.

Procedimiento

Comprobar la causa de la alarma y la información sobre el DataNode para el que se genera la alarma.

Paso 1 En el portal de FusionInsight Manager, seleccione **O&M > Alarm > Alarms**. En la lista de alarmas, haga clic en la alarma.

Paso 2 En el **HostName** de **Location**, se obtiene el nombre de host del DataNode para el que se genera la alarma.

Eliminar directorios que no cumplan con el plan de disco del directorio de datos de DataNode.

Paso 3 Elija **Cluster >** *Name of the desired cluster* **> Services** >**HDFS** >**Instance**. En la lista de instancias, haga clic en la instancia DataNode en el nodo para el que se genera la alarma.

Paso 4 Haga clic en **Instance Configurations** y vea el valor del parámetro de DataNode **dfs.datanode.data.dir**.

Paso 5 Compruebe si todos los directorios de datos de DataNode son coherentes con el plan de disco.

- En caso afirmativo, vaya a **Paso 6**.
- Si no, vaya a **Paso 9**.

Paso 6 Modifique el parámetro de DataNode **dfs.datanode.data.dir** y elimine los directorios incorrectos.

Paso 7 Elija **Cluster >** *Name of the desired cluster* **> Services** > **HDFS** > **Instance** y reinicie la instancia DataNode.

Paso 8 Verifique si la alarma se ha borrado.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 9**.

Paso 9 Inicie sesión en el DataNode para el que se genera la alarma como **root**.

- Si la causa de la alarma es "No se puede crear el directorio de datos de DataNode", vaya a **Paso 10**.
- Si la causa de la alarma es "El directorio de datos de DataNode utiliza el mismo disco con directorios críticos, como / o **/boot**", Vaya a **Paso 17**.
- Si la causa de la alarma es "Múltiples directorios en el directorio de datos de DataNode utilizan el mismo disco", vaya a **Paso 21**.

Comprobar si el directorio de datos de DataNode falla al crearse.

Paso 10 Ejecute el comando **su - omm** para cambiar a usuario **omm**.

Paso 11 Ejecute el comando **ls** para comprobar si los directorios existen en el directorio de datos de DataNode.

- En caso afirmativo, vaya a **Paso 26**.
- Si no, vaya a **Paso 12**.

Paso 12 Ejecute el comando **mkdir** *data directory* para crear el directorio y verifique si el directorio se puede crear correctamente.

- En caso afirmativo, vaya a **Paso 24**.
- Si no, vaya a **Paso 13**.

Paso 13 En el portal del FusionInsight Manager, seleccione **O&M > Alarm > Alarms** para comprobar si existe una alarma **ALM-12017 Capacidad de disco insuficiente**.

- En caso afirmativo, vaya a **Paso 14**.
- Si no, vaya a **Paso 15**.

Paso 14 Ajuste la capacidad del disco y compruebe si la alarma **ALM-12017 Capacidad de disco insuficiente** está borrado. Para obtener más información, consulte **ALM-12017 Capacidad de disco insuficiente**.

- En caso afirmativo, vaya a **Paso 12**.
- Si no, vaya a **Paso 15**.

Paso 15 Compruebe si el usuario **omm** tiene el permiso **rwx** o **x** de todos los directorios de capa superior del directorio. (Por ejemplo, para **/tmp/abc/**, el usuario **omm** tiene el permiso **x** para el directorio **tmp** y el permiso **rwx** para el directorio **abc**.)

- En caso afirmativo, vaya a **Paso 24**.
- Si no, vaya a **Paso 16**.

Paso 16 Ejecute el comando **chmod u+rwx** *path* o **chmod u+x** *path* como usuario **root** para asignar el permiso **rwx** o **x** de estos directorios al usuario **omm**. Entonces vaya a **Paso 12**.

Comprobar si el directorio de datos de DataNode utiliza el mismo disco que otros directorios críticos del sistema.

Paso 17 Ejecute el comando **df** para obtener la información de montaje en disco de cada directorio en el directorio de datos de DataNode.

Paso 18 Compruebe si los directorios montados en el disco son directorios críticos, como **/** o **/boot**.

- En caso afirmativo, vaya a **Paso 19**.
- Si no, vaya a **Paso 24**.

Paso 19 Cambie el valor del parámetro DataNode **dfs.datanode.data.dir** y elimine los directorios que utilizan el mismo disco que los directorios críticos.

Paso 20 Vaya a **Paso 24**.

Comprobar si varios directorios en el directorio de datos de DataNode utilizan el mismo disco.

Paso 21 Ejecute el comando **df** para obtener la información de montaje en disco de cada directorio en el directorio de datos de DataNode. Registre el directorio montado en la salida del comando.

Paso 22 Modifique los parámetros de nodo de DataNode **dfs.DataNode.data.dir** para reservar solo un directorio entre los directorios que montaron en el mismo directorio de disco.

Paso 23 Vaya a **Paso 24**.

Reiniciar el DataNode y comprobar si la alarma se ha borrado.

Paso 24 En el portal de FusionInsight Manager, elija **Cluster >** *Name of the desired cluster* **> Services** > **HDFS** > **Instance** > y reinicie la instancia DataNode

Paso 25 Verifique si la alarma se ha borrado.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 26**.

Recopilar información de fallas.

Paso 26 En el portal del FusionInsight Manager, elija **O&M** > **Log > Download**.

Paso 27 Seleccione **HDFS** en el clúster requerido en el **Service**.

Paso 28 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 29 Póngase en contacto con el y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.92 ALM-14012 El JournalNode no está sincronizado

Descripción

En el NameNode activo, el sistema comprueba la consistencia de los datos de todos los JournalNodes del clúster cada 5 minutos. Esta alarma se genera cuando los datos en un JournalNode son inconsistentes con los datos en el otro JournalNodes.

Esta alarma se borra en 5 minutos después de que los datos de JournalNodes sean consistentes.

Atributo

ID de alarma	Gravedad de la alarma	Borrado automáticamente
14012	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
NameServiceName	Especifica el NameService para el que se genera la alarma.

Impacto en el sistema

Cuando un JournalNode está funcionando incorrectamente, los datos en el nodo se vuelven inconsistentes con los del otro JournalNodes. Si los datos de más de la mitad de JournalNodes son inconsistentes, el NameNode no puede funcionar correctamente, lo que hace que el servicio HDFS no esté disponible.

Causas posibles

- La instancia JournalNode no existe (eliminada o migrada).
- La instancia JournalNode no se ha iniciado o se ha detenido.
- La instancia JournalNode funciona incorrectamente.
- La red del JournalNode es inalcanzable.

Procedimiento

Comprobar si la instancia de JournalNode se ha iniciado.

Paso 1 En el portal de FusionInsight Manager, seleccione **O&M > Alarm > Alarms**. En la lista de alarmas, haga clic en la alarma.

Paso 2 Compruebe **Location** y obtenga la dirección IP del JournalNode para el que se genera la alarma.

Paso 3 Elija **Cluster >** *Name of the desired cluster* **> Services** >**HDFS** >**Instance**. En la lista de instancias, compruebe si la instancia JournalNode existe en el nodo para el que se genera la alarma.

- En caso afirmativo, vaya a **Paso 5**.
- Si no, vaya a **Paso 4**.

Paso 4 Elija **O&M** >**Alarm** >**Alarms**. En la lista de alarmas, haga clic en **Clear** en la columna **Operation** de la alarma. En el cuadro de diálogo que se muestra, haga clic en **OK**. No es necesario adoptar más medidas.

Paso 5 Haga clic en la instancia JournalNode y compruebe si su **Configuration Status** es **Synchronized**.

- En caso afirmativo, vaya a **Paso 8**.
- Si no, vaya a **Paso 6**.

Paso 6 Seleccione la instancia JournalNode y elija **Start Instance** para iniciar la instancia.

Paso 7 Después de 5 minutos, compruebe si la alarma está borrada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 15**.

Comprobar si la instancia de JournalNode funciona correctamente.

Paso 8 Comprueba si **Running Status** de la instancia JournalNode es **Normal**.

- En caso afirmativo, vaya a **Paso 11**.
- Si no, vaya a **Paso 9**.

Paso 9 Seleccione la instancia JournalNode y elija **More** > **Restart Instance** para iniciar la instancia.

Paso 10 Después de 5 minutos, compruebe si la alarma está borrada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 15**.

Comprobar si se puede acceder a la red de JournalNode.

Paso 11 En el portal del FusionInsight Manager, elija **Cluster >** *Name of the desired cluster* **> Services** > **HDFS** > **Instance** para comprobar la dirección IP del servicio del NameNode activo.

Paso 12 Inicie sesión en el NameNode activo como usuario **root**.

Paso 13 Ejecute el comando **ping** para comprobar si se produce un tiempo de espera o si la red es inalcanzable entre el NameNode activo y el JournalNode.

ping *service IP address of the JournalNode*

- En caso afirmativo, vaya a **Paso 14**.
- Si no, vaya a **Paso 15**.

Paso 14 Póngase en contacto con el administrador de la red para rectificar la falla de la red y comprobar si la alarma se borra 5 minutos después.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 15**.

Recopilar información de fallas.

Paso 15 En el portal del FusionInsight Manager, elija **O&M** > **Log > Download**.

Paso 16 Seleccione **HDFS** en el clúster requerido en el **Service**.

Paso 17 Haga clic en  en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 30 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 18 Póngase en contacto con el y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.93 ALM-14013 Error al actualizar el archivo NameNode FsImage

Descripción

Los metadatos HDFS se almacenan en el archivo FsImage del directorio de datos NameNode especificado por el elemento de configuración **dfs.NameNode.name.dir**. El NameNode en espera combina periódicamente archivos FsImage existentes y archivos Editlog almacenados en el JournalNode para generar un nuevo archivo FsImage y, a continuación, envía el nuevo archivo FsImage al directorio de datos del NameNode activo. Este período se especifica mediante el elemento de configuración **dfs.namenode.checkpoint.period** de HDFS. El valor predeterminado es 3600s, es decir, una hora. Si el archivo FsImage en el directorio de datos del NameNode activo no se actualiza, la función de combinación de metadatos HDFS es anormal y requiere rectificación.

En el NameNode activo, el sistema comprueba la información del archivo FsImage cada cinco minutos. Esta alarma se genera cuando no se genera ningún archivo FsImage dentro de tres períodos de combinación.

Esta alarma se borra cuando se genera un nuevo archivo FsImage y se envía al NameNode activo, lo que indica que la función de combinación de metadatos HDFS se puede usar correctamente.

Atributo

ID de alarma	Gravedad de la alarma	Borrado automáticamente
14013	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.

Nombre	Significado
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
NameServiceName	Especifica el NameService para el que se genera la alarma.

Impacto en el sistema

Si el archivo FsImage en el directorio de datos del NameNode activo no se actualiza, la función de combinación de metadatos HDFS es anormal y requiere rectificación. Si no se rectifica, los archivos de Editlog aumentan continuamente después de que HDFS se ejecute durante un período. En este caso, el reinicio HDFS consume mucho tiempo porque es necesario cargar un gran número de archivos Editlog. Además, esta alarma también indica que el NameNode en espera es anormal y que el mecanismo de alta disponibilidad de NameNode (HA) no es válido. Cuando el NameNode activo es defectuoso, el servicio HDFS no está disponible.

Causas posibles

- El NameNode en espera se detiene.
- La instancia de NameNode en espera funciona incorrectamente.
- El NameNode en espera no genera un archivo FsImage nuevo.
- El espacio del directorio de datos en el NameNode en espera es insuficiente.
- El NameNode en espera no puede empujar el archivo FsImage al NameNode activo.
- El espacio del directorio de datos en el NameNode activo es insuficiente.

Procedimiento

Comprobar si el NameNode en espera está detenido.

Paso 1 En el portal de FusionInsight Manager, seleccione **O&M > Alarm > Alarms**. En la lista de alarmas, haga clic en la alarma.

Paso 2 Vea **Location** y obtenga el nombre de host del NameNode activo para el que se genera la alarma y el nombre del NameService donde reside el NameNode activo.

Paso 3 Elija **Cluster >** *Name of the desired cluster* **> Services** > **HDFS** > **Instance**, busque la instancia NameNode en espera del NameService en la lista de instancias y compruebe si su **Configuration Status** es **Synchronized**.

- En caso afirmativo, vaya a **Paso 6**.
- Si no, vaya a **Paso 4**.

Paso 4 Seleccione la instancia de NameNode en espera, elija **Start Instance** y espere hasta que finalice el inicio.

Paso 5 Espere un período de combinación de metadatos de NameNode y compruebe si la alarma está borrada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 6**.

Comprobar si la instancia de NameNode funciona correctamente.

Paso 6 Compruebe si el **Running Status** de la instancia de NameNode en espera es el **Normal**.

- En caso afirmativo, vaya a **Paso 9**.
- Si no, vaya a **Paso 7**.

Paso 7 Seleccione la instancia de NameNode en espera, elija **More** > **Restart Instance** y espere hasta que finalice el inicio.

Paso 8 Espere un período de combinación de metadatos de NameNode y compruebe si la alarma está borrada.

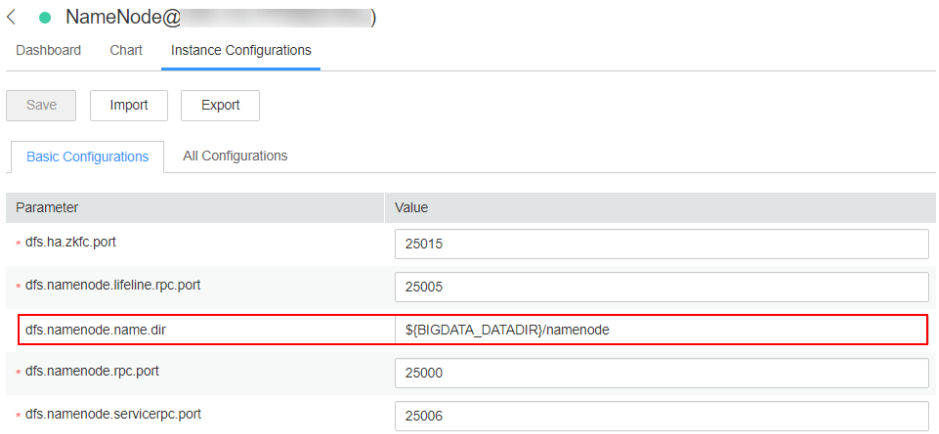
- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 30**.

Comprobar si el NameNode en espera no puede generar un nuevo archivo FsImage.

Paso 9 En el portal del FusionInsight Manager, elija **Cluster >** *Name of the desired cluster* **> Services** > **HDFS** > **Configurations** > **All Configurations**, y busque y obtenga el valor de **dfs.namenode.checkpoint.period**. Este valor es el período de combinación de metadatos de NameNode.

Paso 10 Elija **Cluster >** *Name of the desired cluster* **> Services** > **HDFS** > **Instance** y obtenga las direcciones IP de servicio del NameNodes activo y en espera del NameService para el que se genera la alarma.

Paso 11 Haga clic en **NameNode(***xx***,Standy)** y **Instance Configurations** para obtener el valor de **dfs.namenode.name.dir**. Este valor es el directorio de almacenamiento de FsImage del NameNode en espera.



Paso 12 Inicie sesión en el NameNode en espera como usuario **root** o **omm**.

Paso 13 Vaya al directorio de almacenamiento de FsImage y compruebe el tiempo de generación del archivo FsImage más reciente.

cd *Storage directory of the standby NameNode*/**current**

stat -c %y $(ls -t | grep "fsimage_[0-9]*$" | head -1)

Paso 14 Ejecute el comando **date** para obtener la hora actual del sistema.

Paso 15 Calcule la diferencia de tiempo entre el tiempo de generación del archivo FsImage más reciente y la hora actual del sistema y compruebe si la diferencia de tiempo es mayor que tres veces del período de combinación de metadatos.

- En caso afirmativo, vaya a **Paso 16**.
- Si no, vaya a **Paso 20**.

Paso 16 La función de combinación de metadatos del NameNode en espera es defectuosa. Ejecute el siguiente comando para comprobar si el fallo es causado por espacio de almacenamiento insuficiente.

Vaya al directorio de almacenamiento de FsImage y compruebe el tamaño del archivo FsImage más reciente (en MB).

cd *Storage directory of the standby NameNode*/**current**

du -m $(ls -t | grep "fsimage_[0-9]*$" | head -1) | awk '{print $1}'

Paso 17 Ejecute el siguiente comando para comprobar el espacio disponible en disco del NameNode en espera (en MB).

df -m ./ | awk 'END{print $4}'

Paso 18 Compare el tamaño del archivo FsImage y el espacio disponible en disco y determine si se puede almacenar otro archivo FsImage en el disco.

- En caso afirmativo, vaya a **Paso 7**.
- Si no, vaya a **Paso 19**.

Paso 19 Borre los archivos redundantes del disco donde reside el directorio para reservar espacio suficiente para los metadatos. Después de la liquidación, espere un período de combinación de metadatos de NameNode y compruebe si la alarma está borrada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 20**.

Comprobar si el NameNode en espera no puede enviar el archivo FsImage al NameNode activo.

Paso 20 Inicie sesión en el NameNode en espera como usuario **root**.

Paso 21 Ejecute el comando **su - omm** para cambiar a usuario **omm**.

Paso 22 Ejecute el siguiente comando para comprobar si el NameNode en espera puede enviar el archivo al NameNode activo.

tmpFile=/tmp/tmp_test_$(date +%s)

echo "test" > $tmpFile

scp $tmpFile *Service IP address of the active NameNode*:**/tmp**

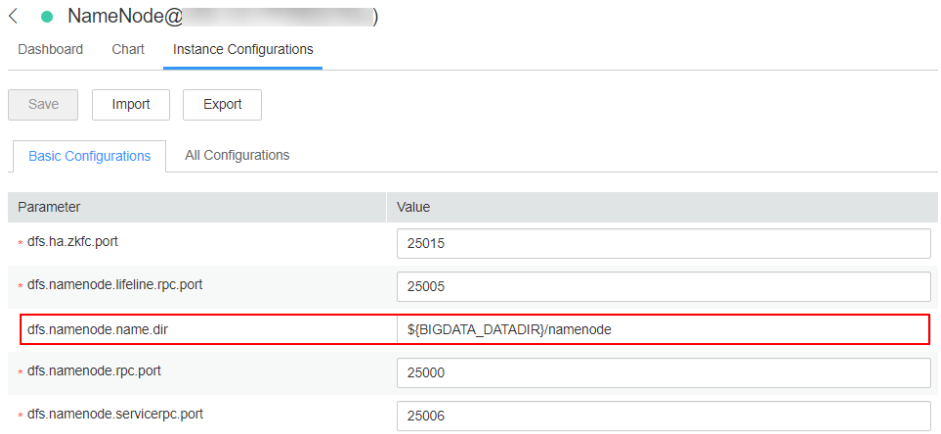
- En caso afirmativo, vaya a **Paso 24**.
- Si no, vaya a **Paso 23**.

Paso 23 Cuando el NameNode en espera no puede enviar datos al NameNode activo como usuario **omm**, póngase en contacto con el administrador del sistema para manejar el error. Espere un período de combinación de metadatos de NameNode y compruebe si la alarma está borrada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 24**.

Comprobar si el espacio en el directorio de datos del NameNode activo es insuficiente.

Paso 24 En el portal de FusionInsight Manager, elija **Cluster** > *Name of the desired cluster* > **Services** > **HDFS** > **Instance**, haga clic en el NameNode activo del NameService para el que se genera la alarma y, a continuación, haga clic en **Instance Configurations** para obtener el valor de **dfs.namenode.name.dir**. Este valor es el directorio de almacenamiento de FsImage del NameNode activo.



Paso 25 Inicie sesión en el NameNode activo como usuario **root** o **omm**.

Paso 26 Vaya al directorio de almacenamiento de FsImage y compruebe el tamaño del archivo FsImage más reciente (en MB).

cd *Storage directory of the active NameNode*/**current**

du -m $(ls -t | grep "fsimage_[0-9]*$" | head -1) | awk '{print $1}'

Paso 27 Ejecute el siguiente comando para comprobar el espacio disponible en disco del NameNode activo (en MB).

df -m ./ | awk 'END{print $4}'

Paso 28 Compare el tamaño del archivo FsImage y el espacio disponible en disco y determine si se puede almacenar otro archivo FsImage en el disco.

- En caso afirmativo, vaya a **Paso 30**.
- Si no, vaya a **Paso 29**.

Paso 29 Borre los archivos redundantes del disco donde reside el directorio para reservar espacio suficiente para los metadatos. Después de la liquidación, espere un período de combinación de metadatos de NameNode y compruebe si la alarma está borrada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 30**.

Recopilar información de fallas.

Paso 30 En el portal del FusionInsight Manager, elija **O&M** > **Log** > **Download**.

Paso 31 Seleccione **NameNode** en el clúster requerido en el **Service**.

Paso 32 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 30 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 33 Póngase en contacto con el y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.94 ALM-14014 El tiempo de GC de NameNode supera el umbral

Descripción

El sistema comprueba la duración de la recolección de basura (GC) del proceso NameNode cada 60 segundos. Esta alarma se genera cuando la duración de GC excede el umbral (12 segundos por defecto).

Esta alarma se borra cuando la duración de GC es menor que el umbral.

Atributo

ID de alarma	Gravedad de la alarma	Borrado automáticamente
14014	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Nombre	Significado
Trigger Condition	Especifica el umbral que activa la alarma. Si el valor del indicador actual excede este umbral, se genera la alarma.

Impacto en el sistema

Una larga duración de GC del proceso NameNode puede interrumpir los servicios.

Causas posibles

La memoria heap de la instancia NameNode se utiliza en exceso o la memoria heap se asigna de forma inadecuada. Como resultado, los GC ocurren con frecuencia.

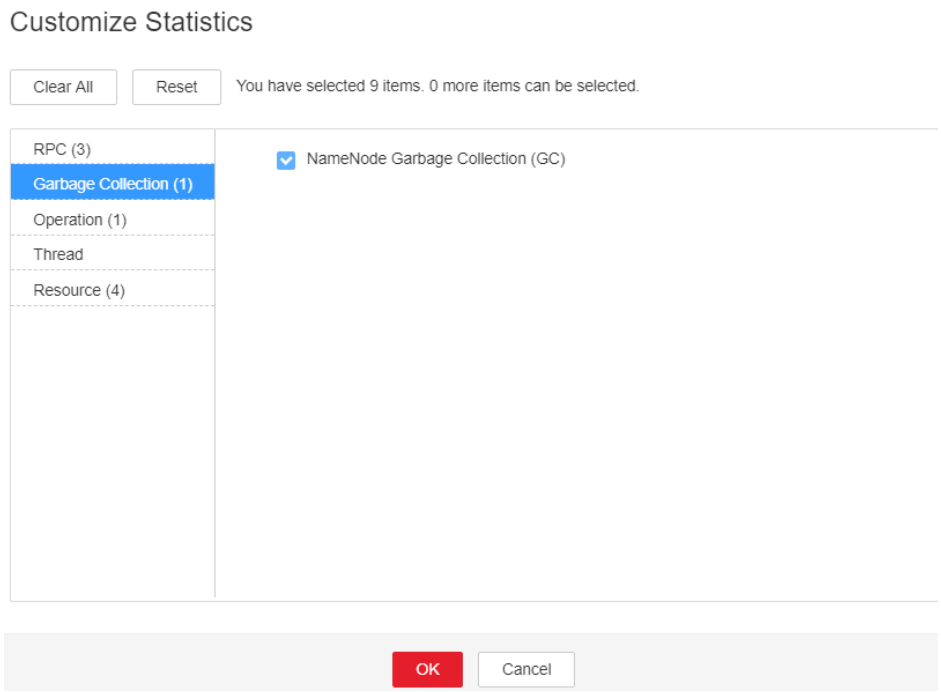
Procedimiento

Compruebe la duración del GC.

Paso 1 En el portal del FusionInsight Manager, elija **O&M** > **Alarm** > **Alarms**. En la interfaz mostrada, haga clic en el botón desplegable de **ALM-14014 NameNode GC Time Exceeds the Threshold.** Luego compruebe el nombre del rol de **Location** y confirme la dirección IP de la instancia.

Paso 2 En el portal del FusionInsight Manager, seleccione **Cluster** > *Name of the desired cluster* > **Services** > **HDFS** > **Instance** > **NameNode (IP address for which the alarm is generated)**. Haga clic en el menú desplegable en la esquina superior derecha del **Chart**, seleccione **Customize** > **Garbage Collection**, y seleccione **NameNode Garbage Collection (GC)** para comprobar las estadísticas de duración de GC del proceso NameNode recopilados cada minuto.

Figura 9-20 NameNode Garbage Collection (GC)



Paso 3 Compruebe si la duración GC del proceso NameNode recopilado cada minuto supera el umbral (12 segundos por defecto).

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 7**.

Paso 4 En el portal de FusionInsight Manager, elija **Cluster >** *Name of the desired cluster* **> Services** > **HDFS** > **Configurations** > **All Configurations** > **NameNode** > **System** para aumentar el valor del parámetro **GC_OPTS** según sea necesario.

NOTA

La asignación recomendada entre el número de objetos de archivo HDFS (objetos de sistema de archivos = archivos + bloques) y los parámetros JVM configurados para NameNode es la siguiente:

- Si el número de objetos de archivo llega a 10,000,000, se recomienda establecer los parámetros de JVM de la siguiente manera: -Xms6G -Xmx6G -XX:NewSize=512M -XX:MaxNewSize=512M
- Si el número de objetos de archivo llega a 20,000,000, se recomienda establecer los parámetros JVM de la siguiente manera: -Xms12G -Xmx12G -XX:NewSize=1G -XX:MaxNewSize=1G
- Si el número de objetos de archivo llega a 50,000,000, se recomienda establecer los parámetros JVM de la siguiente manera: -Xms32G -Xmx32G -XX:NewSize=3G -XX:MaxNewSize=3G
- Si el número de objetos de archivo llega a 100,000,000, se recomienda establecer los parámetros JVM de la siguiente manera: -Xms64G -Xmx64G -XX:NewSize=6G -XX:MaxNewSize=6G
- Si el número de objetos de archivo llega a 200,000,000, se recomienda establecer los parámetros JVM de la siguiente manera: -Xms96G -Xmx96G -XX:NewSize=9G -XX:MaxNewSize=9G
- Si el número de objetos de archivo llega a 300,000,000, se recomienda establecer los parámetros JVM de la siguiente manera: -Xms164G -Xmx164G -XX:NewSize=12G -XX:MaxNewSize=12G

Paso 5 Guarde la configuración y reinicie la instancia NameNode.

Paso 6 Verifique si la alarma se ha borrado.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 7**.

Recopilar información de fallas.

Paso 7 En el portal del FusionInsight Manager, elija **O&M** > **Log > Download**.

Paso 8 Seleccione **NameNode** en el clúster requerido en el **Service**.

Paso 9 Haga clic en  en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 10 Póngase en contacto con el y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.95 ALM-14015 El tiempo de GC de DataNode supera el umbral

Descripción

El sistema comprueba la duración de la recolección de basura (GC) del proceso DataNode cada 60 segundos. Esta alarma se genera cuando la duración de GC excede el umbral (12 segundos por defecto).

Esta alarma se borra cuando la duración de GC es menor que el umbral.

Atributo

ID de alarma	Gravedad de la alarma	Borrado automáticamente
14015	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger Condition	Especifica el umbral que activa la alarma. Si el valor del indicador actual excede este umbral, se genera la alarma.

Impacto en el sistema

Una larga duración GC del proceso DataNode puede interrumpir los servicios.

Causas posibles

La memoria heap de la instancia DataNode se utiliza en exceso o la memoria heap se asigna de forma inadecuada. Como resultado, los GC ocurren con frecuencia.

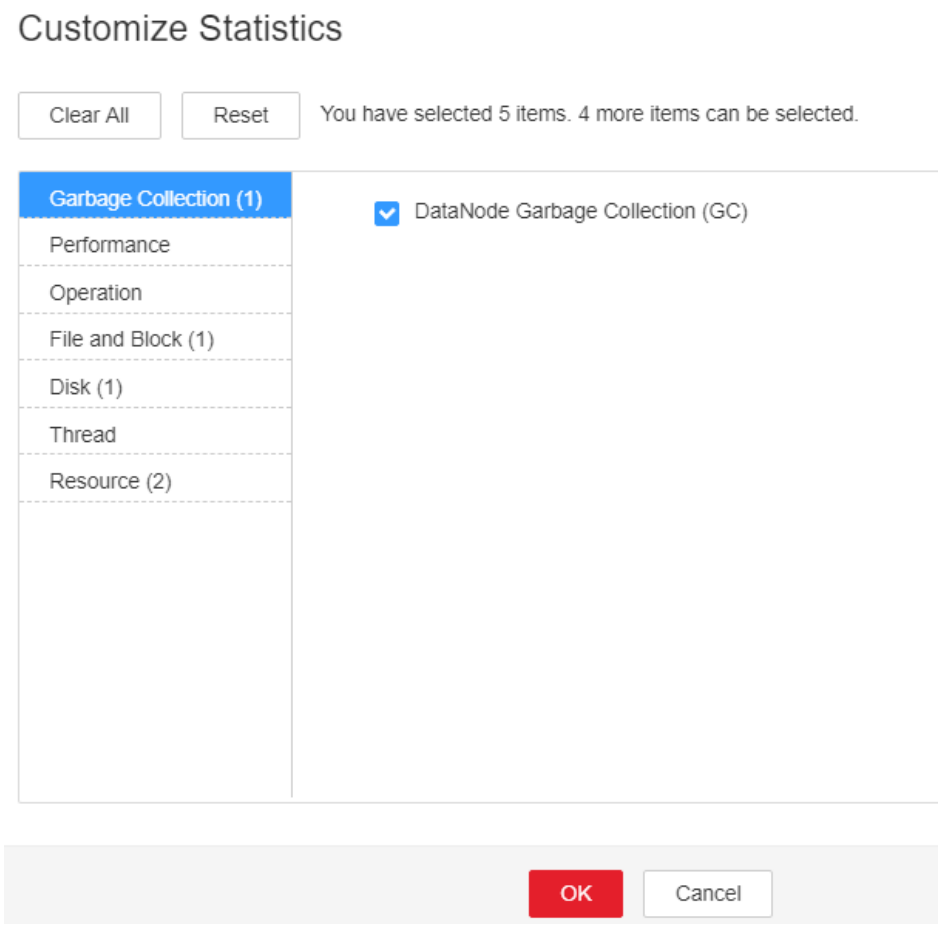
Procedimiento

Comprobar la duración del GC.

Paso 1 En el portal del FusionInsight Manager, elija **O&M** > **Alarm** > **Alarms**. En la interfaz mostrada, haga clic en el botón desplegable de **ALM-14015 El tiempo del GC de DataNode supera el umbral**. A continuación, compruebe el nombre del rol de **Location** y confirme la dirección IP de la instancia.

Paso 2 En el portal del FusionInsight Manager, seleccione **Cluster >** *Name of the desired cluster* **> Services** > **HDFS** > **Instance** > **DataNode (IP address for which the alarm is generated)**. Haga clic en el menú desplegable en la esquina superior derecha del **Chart**, seleccione **Customize** > **Garbage Collection**, y seleccione **DataNode Garbage Collection (GC)** para comprobar las estadísticas de duración de GC del proceso DataNode recopilados cada minuto.

Figura 9-21 Recopilación de basura (GC)



Paso 3 Compruebe si la duración GC del proceso DataNode recopilado cada minuto supera el umbral (12 segundos por defecto).

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 7**.

Paso 4 En el portal de FusionInsight Manager, elija **Cluster >** *Name of the desired cluster* **> Services** > **HDFS** > **Configurations** > **All Configurations** > **DataNode** > **System** para aumentar el valor del parámetro **GC_OPTS** según sea necesario.

NOTA

La asignación entre el número promedio de bloques de una instancia de DataNode y la memoria DataNode es la siguiente:

- Si el número promedio de bloques de una instancia de DataNode llega a 2,000,000, los valores de referencia de los parámetros JVM del DataNode son los siguientes: -Xms6G -Xmx6G -XX:NewSize=512M -XX:MaxNewSize=512M
- Si el número promedio de bloques de una instancia de DataNode llega a 5,000,000, los valores de referencia de los parámetros JVM del DataNode son los siguientes: -Xms12G -Xmx12G -XX:NewSize=1G -XX:MaxNewSize=1G

Paso 5 Guarde la configuración y reinicie la instancia DataNode.

Paso 6 Verifique si la alarma se ha borrado.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 7**.

Recopilar información de fallas.

Paso 7 En el portal del FusionInsight Manager, elija **O&M** > **Log > Download**.

Paso 8 Seleccione **DataNode** en el clúster requerido en el **Service**.

Paso 9 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 10 Póngase en contacto con el y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.96 ALM-14016 El uso de memoria directa de DataNode supera el umbral

Descripción

El sistema comprueba el uso de memoria directa de HDFS cada 30 segundos. Esta alarma se genera cuando el uso de memoria directa de las instancias de DataNode excede el umbral (90% de la memoria máxima).

Esta alarma se borra automáticamente cuando el uso de memoria directa es menor que el umbral.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
14016	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger Condition	Especifica el umbral para activar la alarma.

Impacto en el sistema

Si la memoria directa disponible de las instancias de DataNode es insuficiente, puede producirse un desbordamiento de memoria y el servicio se interrumpe.

Causas posibles

La memoria directa de las instancias de DataNode se utiliza en exceso o la memoria directa se asigna de forma inapropiada.

Procedimiento

Comprobar el uso de la memoria directa.

Paso 1 En la página **Home** del FusionInsight Manager, seleccione **O&M** > **Alarms** > **Alarms**. En la página que se muestra, haga clic en la lista desplegable de la fila que contiene **ALM-14016 El uso de la memoria directa de DataNode supera el umbral** y vea el nombre del rol y la dirección IP de la instancia para la que se genera la alarma en el área **Location**.

Paso 2 En la página **Home** del FusionInsight Manager, seleccione **Cluster** > **HDFS** > **HDFS**. En la página que se muestra, haga clic en la pestaña **Instance**. En la lista de instancias, seleccione **DataNode** (dirección IP de la instancia para la que se genera esta alarma). Haga clic en la lista desplegable en la esquina superior derecha del gráfico, elija **Customize** > **Resource** y seleccione **DataNode Memory** para comprobar el uso de la memoria directa.

Paso 3 Compruebe si la memoria directa utilizada de una instancia de DataNode alcanza el 90% (umbral predeterminado) de la memoria directa máxima asignada a ella.

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 8**.

Paso 4 En la página **Home** del FusionInsight Manager, seleccione **Cluster** > **HDFS** > **HDFS**. En la página que se muestra, haga clic en la pestaña **Configuration**, luego en la subpestaña **All Configurations** y seleccione **DataNode** > **System**. Compruebe si existe **-XX:MaxDirectMemorySize** en el parámetro **GC_OPTS**.

- En caso afirmativo, vaya a **Paso 5**.
- Si no, vaya a **Paso 6**.

Paso 5 Ajusta el valor de **-XX:MaxDirectMemorySize**.

1. En el **GC_OPTS** compruebe el valor de **-Xmx** y compruebe si la memoria del nodo es suficiente.

   NOTA

   Puede determinar si la memoria del nodo es suficiente en función del entorno real. Por ejemplo, puede utilizar el siguiente método:

   Utilice la dirección IP para iniciar sesión en la instancia para la que se genera la alarma como usuario **root** y ejecute el comando **free -g** para comprobar el valor de **Mem** en la columna **free**. El valor indica la memoria disponible del nodo. En el siguiente ejemplo, la memoria disponible del nodo es de 4 GB.

   ```
                 total        used        free      shared  buff/cache
   available
   Mem:            112          48           4          10
   58          46
   ......
   ```

   Si el valor de **Mem** es al menos el de **-Xmx**, la memoria de nodo es suficiente. Si el valor de **Mem** es menor que el de **-Xmx**, la memoria de nodo es insuficiente.

   – En caso afirmativo, cambie el valor de **-XX:MaxDirectMemorySize** por el de **-Xmx**.
   – Si no, aumente **-XX:MaxDirectMemorySize** a un valor no mayor que el de **Mem**.

2. Guarde la configuración y reinicie las instancias DataNode.

Paso 6 Compruebe si existe **ALM-14008 El uso de la memoria heap de DataNode supera el umbral**.

- En caso afirmativo, rectifique la falla haciendo referencia a **ALM-14008 El uso de la memoria heap de DataNode supera el umbral**.
- Si no, vaya a **Paso 7**.

Paso 7 Verifique si la alarma se ha borrado.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 8**.

Recopilar información de fallas.

Paso 8 En FusionInsight Manager, seleccione **O&M**. En el panel de navegación de la izquierda, elija **Log** > **Download**.

Paso 9 Expanda la lista desplegable **Service** y seleccione **DataNode** para el clúster de destino.

Paso 10 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 11 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

Información relacionada

Ninguna

9.97 ALM-14017 El uso de memoria directa NameNode supera el umbral

Descripción

El sistema comprueba el uso memoria directa del servicio HDFS cada 30 segundos. Esta alarma se genera cuando el uso directo de memoria de una instancia de NameNode excede el umbral (90% de la memoria máxima).

La alarma se borra cuando el uso directo de memoria es menor que el umbral.

Atributo

ID de alarma	Gravedad de la alarma	Borrado automáticamente
14017	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger Condition	Especifica el umbral que activa la alarma. Si el valor del indicador actual excede este umbral, se genera la alarma.

Impacto en el sistema

Si la memoria directa disponible del servicio HDFS es insuficiente, se produce un desbordamiento de memoria y el servicio se interrumpe.

Causas posibles

La memoria directa de la instancia NameNode se utiliza en exceso o la memoria directa se asigna de forma inapropiada.

Procedimiento

Comprobar el uso de la memoria directa.

Paso 1 En el portal de FusionInsight Manager, elija **O&M** > **Alarm** > **Alarms**. En la interfaz mostrada, haga clic en el botón desplegable de **ALM-14017 El uso de memoria directa de NameNode supera el umbral**. A continuación, compruebe el nombre del rol de **Location** y confirme la dirección IP de la instancia.

Paso 2 En el portal del FusionInsight Manager, seleccione **Cluster >** *Name of the desired cluster* **> Services** > **HDFS** > **Instance** > **NameNode (IP address for which the alarm is generated)**. Haga clic en el menú desplegable en la esquina superior derecha de **Chart**, elija **Customize** > **Resource**, y seleccione **NameNode Memory** para comprobar el uso de memoria directa.

Paso 3 Compruebe si la memoria directa utilizada de NameNode alcanza el 90% de la memoria directa máxima especificada para NameNode de forma predeterminada.

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 8**.

Paso 4 En el portal del FusionInsight Manager, seleccione **Cluster >** *Name of the desired cluster* **> Services** > **HDFS** > **Configurations** > **All Configurations** > **NameNode** > **System** para comprobar si existe "-XX:MaxDirectMemorySize" en el parámetro **GC_OPTS**.

- En caso afirmativo, vaya a **Paso 5**.
- Si no, vaya a **Paso 6**.

Paso 5 En el parámetro **GC_OPTS**, elimine "-XX:MaxDirectMemorySize". Guarde la configuración y reinicie la instancia NameNode.

Paso 6 Compruebe si el **ALM-14007 El uso de la memoria heap de NameNode supera el umbral** existe.

- En caso afirmativo, maneje la alarma haciendo referencia a **ALM-14007 El uso de la memoria heap de NameNode supera el umbral**.
- Si no, vaya a **Paso 7**.

Paso 7 Verifique si la alarma se ha borrado.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 8**.

Recopilar información de fallas.

Paso 8 En el portal del FusionInsight Manager, elija **O&M** > **Log > Download**.

Paso 9 Seleccione **NameNode** en el clúster requerido en el **Service**.

Paso 10 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 11 Póngase en contacto con el y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.98 ALM-14018 El uso de memoria no heap de NameNode supera el umbral

Descripción

El sistema comprueba el uso de memoria no heap del HDFS NameNode cada 30 segundos y compara el uso real con el umbral. El uso de memoria no heap del HDFS NameNode tiene un umbral predeterminado. Esta alarma se genera cuando el uso de memoria no heap del HDFS NameNode excede el umbral.

Los usuarios pueden elegir **O&M > Alarm > Thresholds >** *Name of the desired cluster* > **HDFS** para cambiar el umbral.

Esta alarma se borra cuando el uso de memoria no heap del HDFS NameNode es menor o igual que el umbral.

Atributo

ID de alarma	Gravedad de la alarma	Borrado automáticamente
14018	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.

Nombre	Significado
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger condition	Especifica el umbral que activa la alarma. Si el valor del indicador actual excede este umbral, se genera la alarma.

Impacto en el sistema

Si el uso de memoria del HDFS NameNode es demasiado alto, el rendimiento de lectura/escritura de datos de HDFS se verá afectado.

Causas posibles

La memoria no heap del HDFS NameNode es insuficiente.

Procedimiento

Eliminar archivos innecesarios.

Paso 1 Inicie sesión en el cliente HDFS como usuario **root**. Ejecute el comando **cd** para ir al directorio de instalación del cliente y ejecute el comando **source bigdata_env**.

Si el clúster adopta el modo de seguridad, realice la autenticación de seguridad.

Ejecute el comando **kinit hdfs** e introduzca la contraseña como se le solicite. Obtenga la contraseña del administrador.

Paso 2 Ejecute el comando **hdfs dfs -rm -r** *file or directory path* para eliminar archivos innecesarios.

Paso 3 Compruebe si la alarma se ha borrado.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 4**.

Comprobar el uso y la configuración de la memoria no heap de JVM de NameNode.

Paso 4 En el portal del FusionInsight Manager, elija **Cluster** > *Name of the desired cluster* > **Services** > **HDFS**. Se muestra la página de estado HDFS.

Paso 5 En el área **Basic Information**, haga clic en **NameNode(Active)**. Se muestra el HDFS WebUI.

NOTA

De forma predeterminada, el usuario **admin** no tiene los permisos para gestionar otros componentes. Si la página no se puede abrir o el contenido mostrado está incompleto al acceder a la interfaz de usuario nativa de un componente debido a la falta de permisos, puede crear manualmente un usuario con los permisos para gestionar ese componente.

Paso 6 En HDFS WebUI, haga clic en la pestaña **Overview**. En **Summary**, compruebe el número de archivos, directorios y bloques en HDFS.

Paso 7 En el portal del FusionInsight Manager, elija **Cluster** > *Name of the desired cluster* > **Services** > **HDFS** > **Configurations** > **All Configurations**. En **Search**, escriba **GC_OPTS** para comprobar el parámetro de memoria no heap de **GC_OPTS** de **HDFS->NameNode**.

Ajustar las configuraciones del sistema.

Paso 8 Compruebe si la memoria no heap está configurada correctamente según el número de objetos de archivo en **Paso 6** y los parámetros no heap configurados para NameNode en **Paso 7**.

- En caso afirmativo, vaya a **Paso 9**.
- Si no, vaya a **Paso 12**.

NOTA

La asignación recomendada entre el número de objetos de archivo HDFS (objetos de sistema de archivos = archivos + bloques) y los parámetros JVM configurados para NameNode es la siguiente:

- Si el número de objetos de archivo llega a 10,000,000, se recomienda establecer los parámetros de JVM de la siguiente manera: -Xms6G -Xmx6G -XX:NewSize=512M -XX:MaxNewSize=512M
- Si el número de objetos de archivo llega a 20,000,000, se recomienda establecer los parámetros JVM de la siguiente manera: -Xms12G -Xmx12G -XX:NewSize=1G -XX:MaxNewSize=1G
- Si el número de objetos de archivo llega a 50,000,000, se recomienda establecer los parámetros JVM de la siguiente manera: -Xms32G -Xmx32G -XX:NewSize=3G -XX:MaxNewSize=3G
- Si el número de objetos de archivo llega a 100,000,000, se recomienda establecer los parámetros JVM de la siguiente manera: -Xms64G -Xmx64G -XX:NewSize=6G -XX:MaxNewSize=6G
- Si el número de objetos de archivo llega a 200,000,000, se recomienda establecer los parámetros JVM de la siguiente manera: -Xms96G -Xmx96G -XX:NewSize=9G -XX:MaxNewSize=9G
- Si el número de objetos de archivo llega a 300,000,000, se recomienda establecer los parámetros JVM de la siguiente manera: -Xms164G -Xmx164G -XX:NewSize=12G -XX:MaxNewSize=12G

Paso 9 Modifique el parámetro **GC_OPTS** del NameNode en función de la asignación entre el número de objetos de archivo y la memoria no heap.

Paso 10 Guarde la configuración y haga clic en **Dashboard** > **More** > **Restart Service**.

Paso 11 Verifique si la alarma se ha borrado.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 12**.

Recopilar información de fallas.

Paso 12 En el portal del FusionInsight Manager, elija **O&M** > **Log** > **Download**.

Paso 13 Seleccione los siguientes servicios en el clúster requerido en **Service**.

- ZooKeeper
- HDFS

Paso 14 Haga clic en  en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 15 Póngase en contacto con el y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.99 ALM-14019 El uso de memoria no heap de DataNode supera el umbral

Descripción

El sistema comprueba el uso de memoria no heap del HDFS DataNode cada 30 segundos y compara el uso real con el umbral. El uso de memoria no heap del HDFS DataNode tiene un umbral predeterminado. Esta alarma se genera cuando el uso de memoria no heap del HDFS DataNode excede el umbral.

Los usuarios pueden elegir **O&M > Alarm > Thresholds>** *Name of the desired cluster* **> HDFS** para cambiar el umbral.

Esta alarma se borra cuando el uso de memoria no heap del DataNode HDFS es menor o igual que el umbral.

Atributo

ID de alarma	Gravedad de la alarma	Borrado automáticamente
14019	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger condition	Especifica el umbral que activa la alarma. Si el valor del indicador actual excede este umbral, se genera la alarma.

Impacto en el sistema

Si el uso de memoria del HDFS DataNode es demasiado alto, el rendimiento de lectura/escritura de datos de HDFS se verá afectado.

Causas posibles

La memoria no heap del HDFS DataNode es insuficiente.

Procedimiento

Eliminar archivos innecesarios.

Paso 1 Inicie sesión en el cliente HDFS como usuario **root**. Ejecute el comando **cd** para ir al directorio de instalación del cliente y ejecute el comando **source bigdata_env**.

Si el clúster adopta el modo de seguridad, realice la autenticación de seguridad.

Ejecute el comando **kinit hdfs** e introduzca la contraseña como se le solicite. Obtenga la contraseña del administrador.

Paso 2 Ejecute el comando **hdfs dfs -rm -r** *file or directory path* para eliminar archivos innecesarios.

Paso 3 Verifique si la alarma se ha borrado.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 4**.

Comprobar el uso y la configuración de la memoria que no es de almacenamiento dinámico de la JVM de DataNode.

Paso 4 En el portal del FusionInsight Manager, elija **Cluster** > *Name of the desired cluster* > **Services** > **HDFS**.

Paso 5 En el área **Basic Information**, haga clic en **NameNode(Active)**. Se muestra el HDFS WebUI.

NOTA

De forma predeterminada, el usuario **admin** no tiene los permisos para gestionar otros componentes. Si la página no se puede abrir o el contenido mostrado está incompleto al acceder a la interfaz de usuario nativa de un componente debido a la falta de permisos, puede crear manualmente un usuario con los permisos para gestionar ese componente.

Paso 6 En HDFS WebUI, haga clic en la pestaña **DataNodes** para ver el número de bloques de todos los DataNodes que reportan alarmas.

Paso 7 En el portal del FusionInsight Manager, elija **Cluster** > *Name of the desired cluster* > **Services** > **HDFS** > **Configurations** > **All Configurations**. En **Search**, escriba **GC_OPTS** para comprobar el parámetro de memoria no heap **GC_OPTS** de **HDFS->DataNode**.

Ajustar las configuraciones del sistema.

Paso 8 Comprobar si la memoria está configurada correctamente en función del número de bloques en **Paso 6** y los parámetros de memoria configurados para DataNode en **Paso 7**.

- En caso afirmativo, vaya a **Paso 9**.
- Si no, vaya a **Paso 12**.

NOTA

La asignación entre el número promedio de bloques de una instancia de DataNode y la memoria DataNode es la siguiente:

- Si el número promedio de bloques de una instancia de DataNode llega a 2,000,000, los valores de referencia de los parámetros JVM del DataNode son los siguientes: -Xms6G -Xmx6G -XX:NewSize=512M -XX:MaxNewSize=512M
- Si el número promedio de bloques de una instancia de DataNode llega a 5,000,000, los valores de referencia de los parámetros JVM del DataNode son los siguientes: -Xms12G -Xmx12G -XX:NewSize=1G -XX:MaxNewSize=1G

Paso 9 Modifique el parámetro **GC_OPTS** del DataNode en función de la asignación entre el número de bloques y la memoria.

Paso 10 Guarde la configuración y haga clic en **Dashboard** > **More** > **Restart Service**.

Paso 11 Verifique si la alarma se ha borrado.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 12**.

Recopilar información de fallas.

Paso 12 En el portal del FusionInsight Manager, elija **O&M** > **Log > Download**.

Paso 13 Seleccione los siguientes servicios en el clúster requerido en **Service**.

- ZooKeeper
- HDFS

Paso 14 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 15 Póngase en contacto con el y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.100 ALM-14020 Número de entradas en el directorio de HDFS supera el umbral

Descripción

El sistema obtiene el número de subarchivos y subdirectorios en un directorio especificado cada hora y comprueba si alcanza el porcentaje del umbral (el número máximo de subarchivos y subdirectorios en un directorio HDFS, el umbral para activar una alarma es de **90%** de forma predeterminada). Si excede el porcentaje del umbral, se activa una alarma.

Cuando el número de subarchivos y subdirectorios en el directorio la alarma es menor que el porcentaje del umbral, la alarma se borra automáticamente. Cuando el conmutador de monitorización está desactivado, se borran las alarmas correspondientes a todos los directorios. Si se elimina un directorio de la lista de supervisión, se borran las alarmas correspondientes al directorio.

NOTA

- El parámetro **dfs.namenode.fs-limits.max-directory-items** especifica el número máximo de subarchivos y subdirectorios en el directorio HDFS. Su valor predeterminado es **1048576**. Si el número de subarchivos y subdirectorios de un directorio excede el valor del parámetro, no se pueden crear subarchivos y subdirectorios en el directorio.
- El parámetro **dfs.namenode.directory-items.monitor** especifica la lista de directorios que se van a supervisar. Su valor predeterminado es **/tmp,/SparkJobHistory,/mr-history**.
- El parámetro **dfs.namenode.directory-items.monitor.enabled** se utiliza para activar o desactivar el conmutador de supervisión. Su valor predeterminado es **true**, lo que significa que el conmutador de monitorización está habilitado de forma predeterminada.

Atributo

ID de alarma	Gravedad de la alarma	Borrado automáticamente
14020	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
NameServiceName	Especifica el servicio NameService para el que se genera la alarma.
Directory	Especifica el directorio para el que se genera la alarma.
Trigger Condition	Especifica el umbral que activa la alarma. Si el valor del indicador actual excede este umbral, se genera la alarma.

Impacto en el sistema

Si el número de entradas en el directorio supervisado supera el 90% del umbral, se activa una alarma, pero se pueden agregar entradas al directorio. Una vez que se supera el umbral máximo, las entradas no se agregarán al directorio.

Causas posibles

El número de entradas en el directorio supervisado supera el 90% del umbral.

Procedimiento

Comprobar si existen archivos innecesarios en el sistema.

Paso 1 Inicie sesión en el cliente HDFS como usuario **root**. Ejecute el comando **cd** para ir al directorio de instalación del cliente y ejecute el comando **source bigdata_env** para establecer las variables de entorno.

Si el clúster está en modo de seguridad, se requiere autenticación de seguridad.

Ejecute el comando **kinit hdfs** e introduzca la contraseña como se le solicite. Obtenga la contraseña del administrador.

Paso 2 Ejecute el siguiente comando para comprobar si se pueden eliminar archivos y directorios en el directorio con la alarma:

hdfs dfs -ls *Directory with the alarm*

- En caso afirmativo, vaya a **Paso 3**.
- Si no, vaya a **Paso 5**.

Paso 3 Ejecute el siguiente comando para eliminar archivos innecesarios.

hdfs dfs -rm -r -f *File or directory path*

NOTA

Paso 4 Espere 1 hora y compruebe si la alarma está desactivada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 5**.

Comprobar si el umbral está configurado correctamente.

Paso 5 En el portal del FusionInsight Manager, elija **Cluster >** *Name of the desired cluster* **> Services** > **HDFS** > **Configurations** > **All Configurations**. Busque el parámetro **dfs.namenode.fs-limits.max-directory-items** y compruebe si el valor del parámetro es apropiado.

- En caso afirmativo, vaya a **Paso 9**.
- Si no, vaya a **Paso 6**.

Paso 6 Aumente el valor del parámetro.

Paso 7 Guarde la configuración y haga clic en **Dashboard** > **More** > **Restart Service**.

Paso 8 Espere 1 hora y compruebe si la alarma está desactivada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 9**.

Recopilar información de fallas.

Paso 9 En el portal del FusionInsight Manager, elija **O&M** > **Log > Download**.

Paso 10 Seleccione **HDFS** en el clúster requerido en el **Service**.

Paso 11 Haga clic en  en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 12 Póngase en contacto con el y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.101 ALM-14021 El tiempo promedio de procesamiento de RPC de NameNode supera el umbral

Descripción

El sistema comprueba el tiempo promedio de procesamiento RPC de NameNode cada 30 segundos, y compara el tiempo promedio real de procesamiento RPC con el umbral (valor predeterminado: 100 ms). Esta alarma se genera cuando el sistema detecta que el tiempo promedio de procesamiento de RPC excede el umbral durante varias veces consecutivas (10 veces por defecto).

Puede elegir **O&M > Alarm > Thresholds >** *Name of the desired cluster* > **HDFS** para cambiar el umbral.

Cuando el **Trigger Count** es 1, esta alarma se borra cuando el tiempo promedio de procesamiento de RPC de NameNode es menor o igual que el umbral. Cuando el **Trigger Count** es mayor que 1, esta alarma se borra cuando el tiempo promedio de procesamiento de RPC de NameNode es menor que o igual al 90% del umbral.

Atributo

ID de alarma	Gravedad de la alarma	Borrado automáticamente
14021	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
NameServiceName	Especifica el servicio NameService para el que se genera la alarma.
Trigger condition	Especifica el umbral que activa la alarma. Si el valor del indicador actual excede este umbral, se genera la alarma.

Impacto en el sistema

NameNode no puede procesar las solicitudes RPC de clientes HDFS, servicios de capa superior que dependen de HDFS y DataNode de manera oportuna. Específicamente, los servicios que acceden a HDFS se ejecutan lentamente o el servicio HDFS no está disponible.

Causas posibles

- El rendimiento de la CPU de los nodos NameNode es insuficiente y, por lo tanto, los nodos NameNode no pueden procesar mensajes de manera oportuna.
- La memoria NameNode configurada es demasiado pequeña y se produce la congelación de fotogramas en la JVM debido a la recolección de basura completa frecuente.
- Los parámetros de NameNode no están configurados correctamente, por lo que NameNode no puede aprovechar al máximo el rendimiento del sistema.

Procedimiento

Obtener información de alarma.

Paso 1 En el portal del FusionInsight Manager, seleccione **O&M > Alarm > Alarms**. En la lista de alarmas, haga clic en la alarma.

Paso 2 Comprueba la alarma. Obtenga el nombre de host del nodo NameNode involucrado en esta alarma a partir de la información **HostName** de **Location**. A continuación, obtenga el nombre del nodo NameService involucrado en esta alarma a partir de la información **NameServiceName** de **Location**.

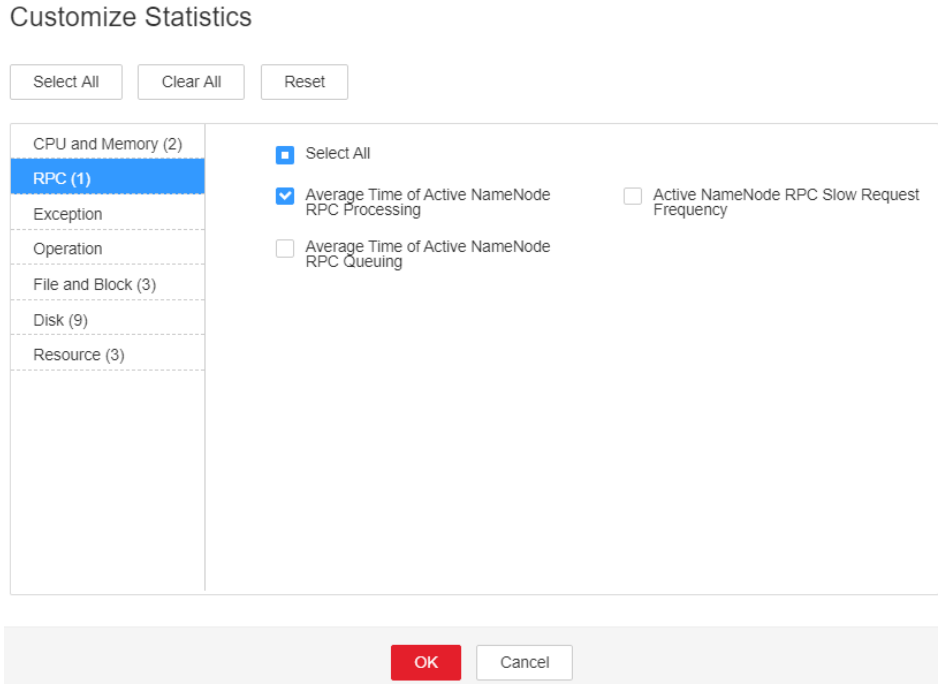
Comprobar si el umbral es demasiado pequeño.

Paso 3 Compruebe el estado de los servicios que dependen de HDFS. Compruebe si los servicios se ejecutan lentamente o si se agota el tiempo de ejecución de la tarea.

- En caso afirmativo, vaya a **Paso 8**.
- Si no, vaya a **Paso 4**.

Paso 4 En el portal del FusionInsight Manager, elija **Cluster** > *Name of the desired cluster* > **Services** > **HDFS**. Haga clic en el menú desplegable en la esquina superior derecha del **Chart**, elija **Customize** > **RPC**, y seleccione **Average Time of Active NameNode RPC Processing** y haga clic en **OK**.

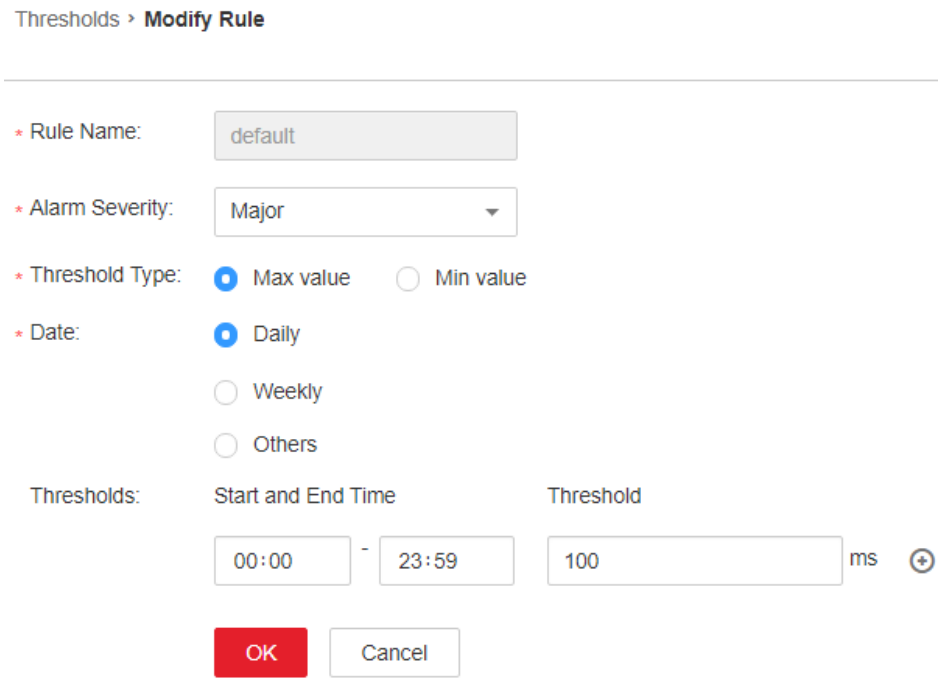
Figura 9-22 Tiempo promedio de procesamiento de RPC de NameNode activo



Paso 5 En la página de monitorización **Average Time of Active NameNode RPC Processing** , obtenga el valor del nodo de NameService involucrado en esta alarma.

Paso 6 En el portal del FusionInsight Manager, seleccione **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster* > **HDFS**. Busque **Average Time of Active NameNode RPC Processing** y haga clic en el **Modify** en la columna **Operation** de la regla predeterminada. Se muestra la página **Modify Rule**. Cambie el **Threshold** al 150% del valor máximo dentro de un día antes y después de que se genere la alarma. Haga clic en **OK** para guardar el nuevo umbral.

Figura 9-23 Modificar regla



Paso 7 Espere 5 minutos y luego compruebe si la alarma se borra automáticamente.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 8**.

Comprobar si el rendimiento de la CPU del nodo NameNode es suficiente.

Paso 8 En el portal de FusionInsight Manager, haga clic en **O&M > Alarm >Alarms** y compruebe si se genera **ALM-12016 El uso de CPU excede el umbral** para el nodo de NameNode.

- En caso afirmativo, vaya a **Paso 9**.
- Si no, vaya a **Paso 11**.

Paso 9 Maneje el **ALM-12016 El uso de la CPU supera el umbral** tomando las medidas recomendadas.

Paso 10 Espere 10 minutos y compruebe si la alarma 14021 se borra automáticamente.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 11**.

Comprobar si la memoria del nodo NameNode es demasiado pequeña.

Paso 11 En el portal de FusionInsight Manager, haga clic en **O&M > Alarm >Alarms** y compruebe si se genera **ALM-14007 El uso de la memoria en montón de NameNode de HDFS supera el umbral** para el nodo de NameNode.

- En caso afirmativo, vaya a **Paso 12**.
- Si no, vaya a **Paso 14**.

Paso 12 Maneje el **ALM-14007 El uso de la memoria en montón de NameNode de HDFS supera el umbral** tomando las medidas recomendadas.

Paso 13 Espere 10 minutos y compruebe si la alarma 14021 se borra automáticamente.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 14**.

Comprobar si los parámetros de NameNode están configurados correctamente.

Paso 14 En el portal del FusionInsight Manager, elija **Cluster >** *Name of the desired cluster* **> Services** > **HDFS** > **Configurations** > **All Configurations**. Busque el parámetro **dfs.namenode.handler.count** y vea su valor. Si el valor es menor o igual a 128, cámbielo a **128**. Si el valor es mayor que 128 pero menor que 192, cámbielo a **192**.

Paso 15 Busque el parámetro **ipc.server.read.threadpool.size** y vea su valor. Si el valor es menor que 5, cámbielo a **5**.

Paso 16 Haga clic en **Save** y haga clic en **OK**.

Paso 17 En la página **Instance** de HDFS, seleccione el NameNode en espera de NameService involucrado en esta alarma y elija **More** > **Restart Instance**. Ingrese la contraseña y haga clic en **OK**. Espere hasta que se inicie el NameNode en espera.

Paso 18 En la página **Instance** de HDFS, seleccione el NameNode activo de NameService involucrado en esta alarma y elija **More** > **Restart Instance**. Ingrese la contraseña y haga clic en **OK**. Espere hasta que se inicie el NameNode activo.

Paso 19 Espere 1 hora y luego compruebe si la alarma se borra automáticamente.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 20**.

Recopilar información de fallas.

Paso 20 En el portal del FusionInsight Manager, elija **O&M** > **Log > Download**.

Paso 21 Seleccione el nodo siguiente en el clúster requerido desde el **Service**.

- HDFS

Paso 22 Haga clic en  en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 23 Póngase en contacto con el y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.102 ALM-14022 El tiempo medio de cola de RPC de NameNode supera el umbral

Descripción

El sistema comprueba el tiempo promedio de cola de RPC de NameNode cada 30 segundos y compara el tiempo promedio real de cola de RPC con el umbral (valor predeterminado: 200 ms). Esta alarma se genera cuando el sistema detecta que el tiempo medio de cola de RPC excede el umbral durante varias veces consecutivas (10 veces por defecto).

Puede elegir **O&M > Alarm > Thresholds >** *Name of the desired cluster* > **HDFS** para cambiar el umbral.

Cuando el **Trigger Count** es 1, esta alarma se borra cuando el tiempo medio de cola de RPC de NameNode es menor o igual que el umbral. Cuando el **Trigger Count** es mayor que 1, esta alarma se borra cuando el tiempo medio de cola de RPC de NameNode es menor o igual al 90% del umbral.

Atributo

ID de alarma	Gravedad de la alarma	Borrado automáticamente
14022	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
NameServiceName	Especifica el servicio NameService para el que se genera la alarma.
Trigger condition	Especifica el umbral que activa la alarma. Si el valor del indicador actual excede este umbral, se genera la alarma.

Impacto en el sistema

NameNode no puede procesar las solicitudes RPC de clientes HDFS, servicios de capa superior que dependen de HDFS y DataNode de manera oportuna. Específicamente, los servicios que acceden a HDFS se ejecutan lentamente o el servicio HDFS no está disponible.

Causas posibles

- El rendimiento de la CPU de los nodos NameNode es insuficiente y, por lo tanto, los nodos NameNode no pueden procesar mensajes de manera oportuna.
- La memoria NameNode configurada es demasiado pequeña y se produce la congelación de fotogramas en la JVM debido a la recolección de basura completa frecuente.
- Los parámetros de NameNode no están configurados correctamente, por lo que NameNode no puede aprovechar al máximo el rendimiento del sistema.
- El volumen de servicios que acceden a HDFS es demasiado grande y, por lo tanto, NameNode está sobrecargado.

Procedimiento

Obtener información de alarma.

Paso 1 En el portal del FusionInsight Managert, seleccione **O&M > Alarm > Alarms**. En la lista de alarmas, haga clic en la alarma.

Paso 2 Comprueba la alarma. Obtenga el tiempo de generación de alarmas de **Generated**. Obtenga el nombre de host del nodo NameNode involucrado en esta alarma a partir de la información **HostName** de **Location**. A continuación, obtenga el nombre del nodo NameService involucrado en esta alarma a partir de la información **NameServiceName** de **Location**.

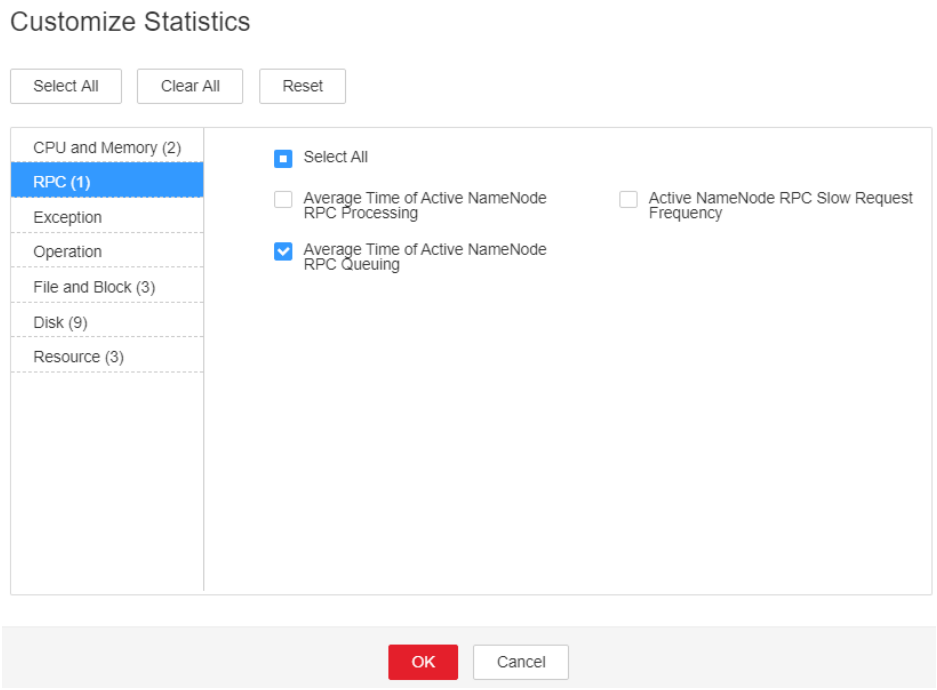
Comprobar si el umbral es demasiado pequeño.

Paso 3 Compruebe el estado de los servicios que dependen de HDFS. Compruebe si los servicios se ejecutan lentamente o si se agota el tiempo de ejecución de la tarea.

- En caso afirmativo, vaya a **Paso 8**.
- Si no, vaya a **Paso 4**.

Paso 4 En el portal del FusionInsight Manager, elija **Cluster >** *Name of the desired cluster* **> Services** > **HDFS**. Haga clic en el menú desplegable en la esquina superior derecha del **Chart**, elija **Customize** > **RPC** y seleccione **Average Time of Active NameNode RPC Queuing** y haga clic en **OK**.

Figura 9-24 Tiempo promedio de la cola RPC de NameNode activa



Paso 5 En la página de monitorización **Average Time of Active NameNode RPC Queuing** , obtenga el valor del nodo NameService involucrado en esta alarma.

Paso 6 En el portal del FusionInsight Manager, seleccione **O&M > Alarm > Thresholds >** *Name of the desired cluster* **> HDFS**. Busque **Average Time of Active NameNode RPC Queuing** y haga clic en el **Modify** en la columna **Operation** de la regla predeterminada. Se muestra la página **Modify Rule**. Cambie el **Threshold** al 150% del valor monitorizado. Haga clic en **OK** para guardar el nuevo umbral.

Paso 7 Espere 1 minuto y compruebe si la alarma se borra automáticamente.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 8**.

Comprobar si el rendimiento de la CPU del nodo NameNode es suficiente.

Paso 8 En el portal del FusionInsight Manager, haga clic en **O&M > Alarm > Alarms** y compruebe si se ha generado el **ALM-12016 HDFS NameNode Memory Usage Exceeds the Threshold**.

- En caso afirmativo, vaya a **Paso 9**.
- Si no, vaya a **Paso 11**.

Paso 9 Manejar el **ALM-12016 El uso de la CPU supera el umbral** tomando las medidas recomendadas.

Paso 10 Espere 10 minutos y compruebe si la alarma 14022 se borra automáticamente.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 11**.

Comprobar si la memoria del nodo NameNode es demasiado pequeña.

Paso 11 En el portal del FusionInsight Manager, haga clic en **O&M > Alarm > Alarms** y compruebe si se ha generado el **ALM-14007 El uso de memoria de NameNode de HDFS supera el umbral**.

- En caso afirmativo, vaya a **Paso 12**.
- Si no, vaya a **Paso 14**.

Paso 12 Maneje **ALM-14007 El uso de la CPU supera el umbral** tomando las acciones recomendadas.

Paso 13 Espere 10 minutos y compruebe si la alarma 14022 se borra automáticamente.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 14**.

Comprobar si los parámetros de NameNode están configurados correctamente.

Paso 14 En el portal del FusionInsight Manager, elija **Cluster >** *Name of the desired cluster* **> Services** > **HDFS** > **Configurations** > **All Configurations**. Busque el parámetro **dfs.namenode.handler.count** y vea su valor. Si el valor es menor o igual a 128, cámbielo a **128**. Si el valor es mayor que 128 pero menor que 192, cámbielo a **192**.

Paso 15 Busque el parámetro **ipc.server.read.threadpool.size** y vea su valor. Si el valor es menor que 5, cámbielo a **5**.

Paso 16 Haga clic en **Save** y, a continuación, haga clic en **OK**.

Paso 17 En la página **Instance** de HDFS, seleccione el NameNode en espera de NameService involucrado en esta alarma y elija **More** > **Restart Instance**. Ingrese la contraseña y haga clic en **OK**. Espere hasta que se inicie el NameNode en espera.

Paso 18 En la página **Instance** de HDFS, seleccione el NameNode activo de NameService involucrado en esta alarma y elija **More** > **Restart Instance**. Ingrese la contraseña y haga clic en **OK**. Espere hasta que se inicie el NameNode activo.

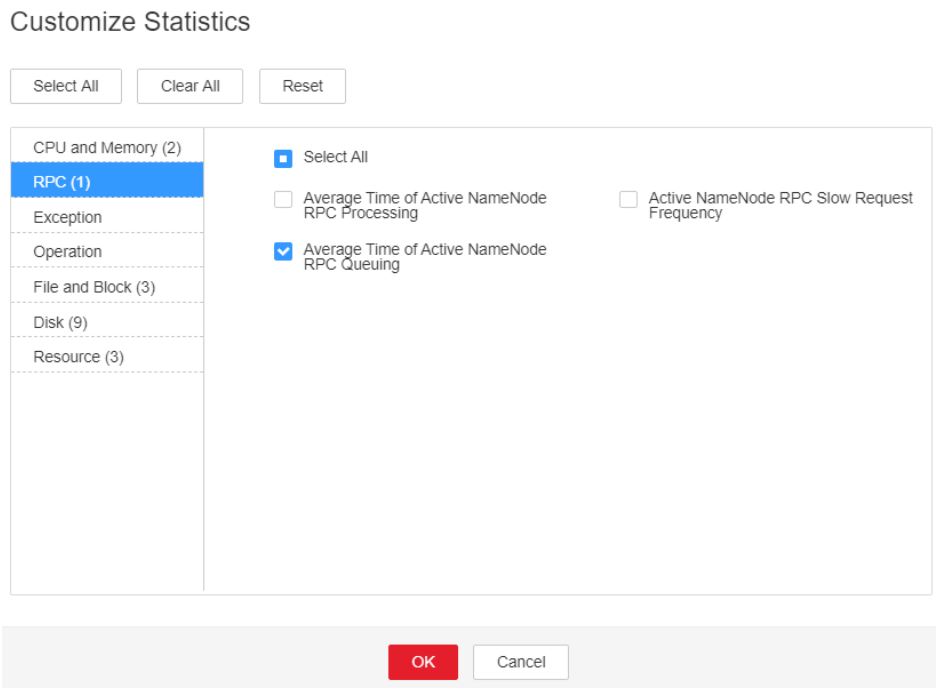
Paso 19 Espere 1 hora y luego compruebe si la alarma se borra automáticamente.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 20**.

Comprobar si la carga de trabajo de HDFS cambia y reducir la carga de trabajo correctamente.

Paso 20 En el portal del FusionInsight Manager, elija **Cluster >** *Name of the desired cluster* **> Services** > **HDFS**. Haga clic en el menú desplegable en la esquina superior derecha de **Chart**, haga clic en **Customize**, seleccione **Average Time of Active NameNode RPC Queuing** y haga clic en **OK**.

Figura 9-25 Tiempo promedio de la cola RPC de NameNode activa



Paso 21 Haga clic en . Se muestra la página **Details**.

Paso 22 Establezca el período de visualización de datos de monitoreo, desde 5 días antes del tiempo de generación de alarma hasta el tiempo de generación de alarma. Haga clic en **OK**.

Paso 23 En la página de supervisión **Average RPC Queuing Time**, compruebe si existe el punto en el tiempo en que el tiempo de espera aumenta bruscamente.

- En caso afirmativo, vaya a **Paso 24**.
- Si no, vaya a **Paso 27**.

Paso 24 Confirme y compruebe el punto en el tiempo. Compruebe si una nueva tarea accede con frecuencia a HDFS y si se puede reducir la frecuencia de acceso.

Paso 25 Si una tarea de Balancer comienza en ese momento, detenga la tarea o especifique un nodo para que la tarea reduzca la carga de trabajo de HDFS.

Paso 26 Espere 1 hora y luego compruebe si la alarma se borra automáticamente.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 27**.

Recopilar información de fallas.

Paso 27 En el portal del FusionInsight Manager, elija **O&M** > **Log** > **Download**.

Paso 28 Seleccione **HDFS** en el clúster requerido en el **Service**.

Paso 29 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 30 Póngase en contacto con el y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.103 ALM-14023 El porcentaje del espacio total en disco reservado para réplicas supera el umbral

Descripción

El sistema comprueba el porcentaje de espacio total en disco reservado para las réplicas (Espacio total reservado en disco para réplicas/(Espacio total reservado en disco para réplicas + Espacio total restante en disco) cada 30 segundos y compara el porcentaje real con el umbral (el **90%** por defecto). Esta alarma se genera cuando el porcentaje de espacio total reservado en disco para réplicas supera el umbral por varias veces consecutivas (**Trigger Count**).

La alarma se borra en los dos escenarios siguientes: El valor de **Trigger Count** es de **1** y el porcentaje del espacio total reservado en disco para réplicas es inferior o igual al umbral; el valor de **Trigger Count** es mayor que **1** y el porcentaje de espacio total reservado en disco para réplicas es menor o igual al 90% del umbral.

Atributo

ID de alarma	Gravedad de la alarma	Borrado automáticamente
14023	Leves	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
NameServiceName	Especifica el servicio NameService para el que se genera la alarma.

Nombre	Significado
Trigger condition	Especifica el umbral que activa la alarma. Si el valor del indicador actual excede este umbral, se genera la alarma.

Impacto en el sistema

El rendimiento de la escritura de datos en HDFS se ve afectado. Si todo el espacio DataNode restante está reservado para réplicas, se produce un error al escribir datos HDFS.

Causas posibles

- El umbral de alarma está configurado incorrectamente.
- El espacio en disco configurado para el clúster HDFS es insuficiente.
- El volumen de servicios que acceden a HDFS es demasiado grande y, por lo tanto, DataNode está sobrecargado.

Procedimiento

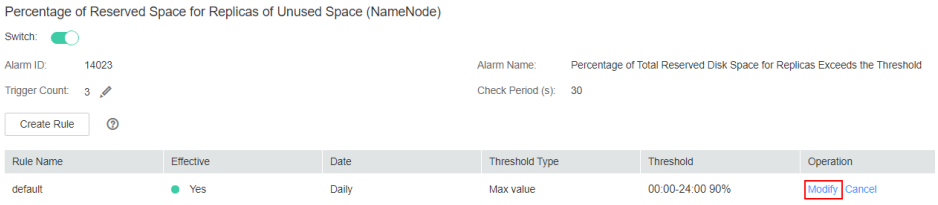
Comprobar si el umbral de alarma es adecuado.

Paso 1 En el portal del FusionInsight Manager, seleccione **O&M > Alarm > Thresholds >** *Name of the desired cluster* > **HDFS** > **Disk** > **Percentage of Reserved Space for Replicas of Unused Space** para comprobar si el umbral de alarma es apropiado. (El umbral predeterminado es **90%**. Los usuarios pueden cambiarlo según sea necesario.)

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 2**.

Paso 2 Elija **O&M > Alarm > Thresholds >** *Name of the desired cluster* > **HDFS** > **Disk** > **Percentage of Reserved Space for Replicas of Unused Space** y haga clic en **Modify,** para cambiar el umbral en función del uso real.

Figura 9-26 Modificar Umbrales



Paso 3 Espere 5 minutos y compruebe si la alarma está desactivada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 4**.

Comprobar si se genera una alarma que indica espacio en disco insuficiente.

Paso 4 En el portal del FusionInsight Manager, compruebe si existe **ALM-14001 El uso del disco HDFS supera el umbral** o **ALM-14002 El uso del disco de DataNode supera el umbral** en la página **O&M > Alarm > Alarms**.

- En caso afirmativo, vaya a **Paso 5**.
- Si no, vaya a **Paso 7**.

Paso 5 Maneje la alarma haciendo referencia a las instrucciones de **ALM-14001 El uso del disco HDFS supera el umbral** y **ALM-14002 El uso del disco de DataNode supera el umbral** y compruebe si la alarma está desactivada.

- En caso afirmativo, vaya a **Paso 6**.
- Si no, vaya a **Paso 7**.

Paso 6 Espere 5 minutos y compruebe si la alarma está desactivada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 7**.

Expandir la capacidad de DataNode.

Paso 7 Amplíe la capacidad del DataNode.

Paso 8 Espere 5 minutos y compruebe si la alarma está desactivada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 9**.

Recopilar información de fallas.

Paso 9 En el portal del FusionInsight Manager, elija **O&M** > **Log > Download**.

Paso 10 Seleccione **HDFS** en el clúster requerido en el **Service**.

Paso 11 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 20 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 12 Póngase en contacto con el y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.104 ALM-14024 El uso del espacio del tenant supera el umbral

Descripción

El sistema comprueba el uso de espacio (espacio usado de cada directorio/espacio asignado a cada directorio) de cada directorio asociado con un tenant cada hora y compara el uso de espacio de cada directorio con el umbral establecido para el directorio. Esta alarma se genera cuando el uso de espacio excede el umbral.

Esta alarma se borra cuando el uso de espacio es menor o igual que el umbral.

Atributo

ID de alarma	Gravedad de la alarma	Borrado automáticamente
14024	Leves	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
TenantName	Especifica el inquilino para el que se genera la alarma.
DirectoryName	Especifica el directorio para el que se genera la alarma.
Trigger condition	Especifica el umbral para activar la alarma.

Impacto en el sistema

Esta alarma se genera si el uso de espacio del directorio del tenant excede el umbral personalizado. La escritura de archivos en el directorio no se ve afectada. Si el espacio utilizado excede el espacio de almacenamiento máximo asignado al directorio, el HDFS no puede escribir datos en el directorio.

Causas posibles

- El umbral de alarma está configurado incorrectamente.
- El espacio asignado al tenant es inadecuado.

Procedimiento

Comprobar si el umbral de alarma es adecuado.

Paso 1 Vea la información de ubicación de la alarma para obtener el nombre del tenant y el directorio del tenant para el que se genera la alarma.

Paso 2 En el portal del FusionInsight Manager, elija la página **Tenant Resources** y seleccione el tenant para el que se genera la alarma y haga clic en **Resources**. Compruebe si el umbral de

espacio de almacenamiento configurado para el directorio de tenant para el que se genera la alarma es adecuado. (El valor predeterminado 90% es un valor apropiado. Puede configurarlo en función de los requisitos del sitio.)

- En caso afirmativo, vaya a **Paso 5**.
- Si no, vaya a **Paso 3**.

Paso 3 En la página **Resources**, haga clic en **Modify** para modificar o eliminar el umbral de espacio de almacenamiento.

Paso 4 Aproximadamente un minuto más tarde, compruebe si la alarma está desactivada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 5**.

Comprobar si el espacio asignado al tenant es adecuado.

Paso 5 En el portal del FusionInsight Manager, elija la página **Tenant Resources** y seleccione el tenant para el que se genera la alarma y haga clic en **Resources**. Compruebe si la cuota de espacio de almacenamiento del directorio de tenants para el que se genera la alarma es adecuada basándose en el estado de servicio real del directorio de tenant.

- En caso afirmativo, vaya a **Paso 8**.
- Si no, vaya a **Paso 6**.

Paso 6 En la página **Resources**, haga clic en **Modify** para modificar la cuota de espacio de almacenamiento.

Paso 7 Aproximadamente un minuto más tarde, compruebe si la alarma está desactivada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 8**.

Recopilar información de fallas.

Paso 8 En el portal del FusionInsight Manager, seleccione **O&M** > **Log** > **Download**.

Paso 9 Seleccione **HDFS** en el clúster requerido y **NodeAgent** en **Manager** en el **Service**.

Paso 10 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 20 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 11 Póngase en contacto con el y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.105 ALM-14025 El uso de objetos de archivo de tenant supera el umbral

Descripción

El sistema comprueba el uso del objeto de archivo (objetos de archivo usados de cada directorio/número de objetos de archivo asignados a cada directorio) de cada directorio asociado con un tenant cada hora y compara el uso de objeto de archivo de cada directorio con el umbral establecido para el directorio. Esta alarma se genera cuando el uso del objeto de archivo excede el umbral.

Esta alarma se borra cuando el uso del objeto de archivo es menor o igual que el umbral.

Atributo

ID de alarma	Gravedad de la alarma	Borrado automáticamente
14025	Leves	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
TenantName	Especifica el inquilino para el que se genera la alarma.
DirectoryName	Especifica el directorio para el que se genera la alarma.
Trigger condition	Especifica el umbral para activar la alarma.

Impacto en el sistema

Esta alarma se genera si el uso de objetos de archivo en un directorio de tenant supera el umbral personalizado. La escritura de archivos en el directorio no se ve afectada. Si el número de objetos de archivo usados excede el número máximo de objetos de archivo asignados al directorio, el HDFS no puede escribir datos en el directorio.

Causas posibles

- El umbral de alarma está configurado incorrectamente.
- El número máximo de objetos de archivo asignados al directorio del tenant es inapropiado.

Procedimiento

Comprobar si el umbral de alarma es adecuado.

Paso 1 Vea la información de ubicación de la alarma para obtener el nombre del tenant y el directorio del tenant para el que se genera la alarma.

Paso 2 En el portal del FusionInsight Manager, elija la página **Tenant Resources** y seleccione el tenant para el que se genera la alarma y haga clic en **Resources**. Compruebe si el umbral de objeto de archivo configurado para el directorio de tenant para el que se genera la alarma es adecuado. (El valor predeterminado 90% es un valor apropiado. Puede configurarlo en función de los requisitos del sitio.)

- En caso afirmativo, vaya a **Paso 5**.
- Si no, vaya a **Paso 3**.

Paso 3 En la página **Resources**, haga clic en **Modify** para modificar o eliminar el umbral de objeto de archivo del directorio de inquilino para el que se genera la alarma..

Paso 4 Aproximadamente un minuto más tarde, compruebe si la alarma está desactivada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 5**.

Compruebe si el número máximo de objetos de archivo asignados al tenant es adecuado.

Paso 5 En el portal del FusionInsight Manager, elija la página **Tenant Resources** y seleccione el tenant para el que se genera la alarma y haga clic en **Resources**. Compruebe si el número máximo de objetos de archivo configurados para el directorio del inquilino para el que se genera la alarma es adecuado en función del estado de servicio real del directorio del tenant.

- En caso afirmativo, vaya a **Paso 8**.
- Si no, vaya a **Paso 6**.

Paso 6 En la página **Resources**, haga clic en **Modify** para modificar o eliminar el número máximo de objetos de archivo configurados para el directorio del tenant.

Paso 7 Aproximadamente un minuto más tarde, compruebe si la alarma está desactivada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 8**.

Recopilar información de fallas.

Paso 8 En el portal del FusionInsight Manager, seleccione **O&M** > **Log** > **Download**.

Paso 9 Seleccione **HDFS** en el clúster requerido y **NodeAgent** en **Manager** en el **Service**.

Paso 10 Haga clic en  en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 20 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 11 Póngase en contacto con el y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.106 ALM-14026 Bloques en el DataNode superan el umbral

Descripción

El sistema comprueba el número de bloques de cada DataNode cada 30 segundos. Esta alarma se genera cuando el número de bloques en el DataNode excede el umbral.

Si **Trigger Count** es de **1** y el número de bloques en el DataNode es menor o igual que el umbral, esta alarma se borra. Si **Trigger Count** es mayor que **1** y el número de bloques en el DataNode es menor o igual al 90% del umbral, esta alarma se borra.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
14026	Leves	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger condition	Especifica el umbral para activar la alarma.

Impacto en el sistema

Si se informa de esta alarma, hay demasiados bloques en el DataNode. En este caso, la escritura de datos en el HDFS puede fallar debido a espacio en disco insuficiente.

Causas posibles

- El umbral de alarma está configurado incorrectamente.
- La desviación de los datos se produce entre los DataNodes.
- El espacio en disco configurado para el clúster HDFS es insuficiente.

Procedimiento

Cambiar el umbral.

Paso 1 En FusionInsight Manager, elija **Cluster**, haga clic en el nombre del clúster deseado y elija **HDFS**. A continuación, elija **Configurations** > **All Configurations**. En la página mostrada, busque el parámetro **GC_OPTS** en la sección **HDFS->DataNode**.

Paso 2 Establezca el umbral de los bloques de DataNode. Específicamente, cambie el valor de **Xmx** del parámetro **GC_OPTS**. **Xmx** especifica la memoria, y cada memoria GB admite un máximo de bloques de 500,000 DataNode. Establezca la memoria según sea necesario. Confirme que **GC_PROFILE** está establecido en **custom** y guarde la configuración.

Paso 3 Elija **Cluster**, haga clic en el nombre del clúster deseado y elija Instancia **HDFS** > **Instance**. Seleccione la instancia DataNode cuyo estado es **Expired**, haga clic en **More** y seleccione **Restart Instance** para que la configuración de **GC_OPTS** surta efecto.

Paso 4 Compruebe si la alarma se borra 5 minutos más tarde.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 5**.

Comprobar si se informan las alarmas asociadas.

Paso 5 En FusionInsight Manager seleccione **O&M** > **Alarm** > **Alarms** y compruebe si existe la alarma **ALM-14002 El uso del disco de DataNode supera el umbral**.

- En caso afirmativo, vaya a **Paso 6**.
- Si no, vaya a **Paso 8**.

Paso 6 Maneje la alarma siguiendo las instrucciones en **ALM-14002 El uso del disco de DataNode supera el umbral** y compruebe si la alarma está desactivada.

- En caso afirmativo, vaya a **Paso 7**.
- Si no, vaya a **Paso 8**.

Paso 7 Compruebe si la alarma se borra 5 minutos más tarde.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 8**.

Expandir la capacidad de DataNode.

Paso 8 Amplíe la capacidad del DataNode.

Paso 9 En FusionInsight Manager, espere 5 minutos y compruebe si la alarma está desactivada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 10**.

Recopilar información de fallas.

Paso 10 En FusionInsight Manager, seleccione **O&M**. En el panel de navegación de la izquierda, elija **Log** > **Download**.

Paso 11 Expanda la lista desplegable junto al campo **Service**. En el cuadro de diálogo **Services** que se muestra, seleccione **HDFS** para el clúster de destino.

Paso 12 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 20 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 13 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

Información relacionada

Reglas de configuración del parámetro JVM de DataNode.

Valor predeterminado del parámetro DataNode JVM **GC_OPTS**:

-Xms2G -Xmx4G -XX:NewSize=128M -XX:MaxNewSize=256M -XX:MetaspaceSize=128M -XX:MaxMetaspaceSize=128M -XX:+UseConcMarkSweepGC -XX:+CMSParallelRemarkEnabled -XX:CMSInitiatingOccupancyFraction=65 -XX:+PrintGCDetails -Dsun.rmi.dgc.client.gcInterval=0x7FFFFFFFFFFFFE -Dsun.rmi.dgc.server.gcInterval=0x7FFFFFFFFFFFFE -XX:-OmitStackTraceInFastThrow -XX:+PrintGCDateStamps -XX:+UseGCLogFileRotation -XX:NumberOfGCLogFiles=10 -XX:GCLogFileSize=1M -Djdk.tls.ephemeralDHKeySize=2048

El número promedio de bloques almacenados en cada instancia de DataNode en el clúster es: Número de bloques HDFS x 3/Número de DataNodes. Si cambia el número promedio de bloques, debe cambiar **-Xms2G -Xmx4G -XX:NewSize=128M -XX:MaxNewSize=256M** en el valor predeterminado. En la siguiente tabla se enumeran los valores de referencia.

Tabla 9-3 Configuración de DataNode JVM

Número medio de bloques en una instancia de DataNode	Valor de referencia
2,000,000	-Xms6G -Xmx6G -XX:NewSize=512M -XX:MaxNewSize=512M
5,000,000	-Xms12G -Xmx12G -XX:NewSize=1G -XX:MaxNewSize=1G

Xmx especifica la memoria que corresponde al umbral del número de bloques de DataNode y cada memoria GB soporta un máximo de bloques de 500,000 DataNode. Establezca la memoria según sea necesario.

9.107 ALM-14027 Falla de disco de DataNode

Descripción

El sistema comprueba el estado del disco de DataNodes cada 60 segundos. Esta alarma se genera cuando un disco está defectuoso.

Después de recuperar todos los discos defectuosos en el DataNode, debe borrar manualmente la alarma y reiniciar el DataNode.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
14027	Importante	No

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Failed Volumes	Especifica la lista de discos defectuosos.

Impacto en el sistema

Si se informa de esta alarma, en el DataNode hay particiones de disco anormales. Esto puede causar la pérdida de archivos escritos.

Causas posibles

- El disco duro presenta fallas.
- Los permisos de disco están configurados incorrectamente.

Procedimiento

Comprobar si se genera una alarma de disco.

Paso 1 En FusionInsight Manager, seleccione **O&M** > **Alarm** > **Alarms** y compruebe si existe **ALM-12014 Partición perdida** o **ALM-12033 Error de disco lento**.

- En caso afirmativo, vaya a **Paso 2**.
- Si no, vaya a **Paso 4**.

Paso 2 Rectifique la falla consultando el procedimiento de manejo de **ALM-12014 Partición perdida** o **ALM-12033 Error de disco lento**. Luego, verifique si la alarma se rectificó.

- En caso afirmativo, vaya a **Paso 3**.
- Si no, vaya a **Paso 4**.

Paso 3 Espere 5 minutos y compruebe si la alarma está desactivada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 4**.

Modificar permisos de disco.

Paso 4 Elija **O&M** > **Alarm** > **Alarms** y vea **Location** e **Additional Information** de la alarma para obtener la ubicación del disco defectuoso.

Paso 5 Inicie sesión en el nodo para el que se genera la alarma como usuario **root**. Vaya al directorio donde se encuentra el disco defectuoso y ejecute el comando **ll** para comprobar si el permiso del disco defectuoso es de **711** y si el usuario es de **omm**.

- En caso afirmativo, vaya a **Paso 8**.
- Si no, vaya a **Paso 6**.

Paso 6 Modifique el permiso del disco defectuoso. Por ejemplo, si el disco defectuoso es de **data1**, ejecute los siguientes comandos:

chown omm:wheel data1

chmod 711 data1

Paso 7 En la lista de alarmas del Manager, haga clic en **Clear** en la columna **Operation** de la alarma para borrarla manualmente. Seleccione **Cluster** > **Services** > **HDFS** > **Instance**, seleccione DataNode, elija **More** > **Restart Instance**, espere 5 minutos y compruebe si se notifica una nueva alarma.

- En caso negativo, no se requiere ninguna otra acción.
- En caso afirmativo, vaya a **Paso 8**.

Recopilar información de fallas.

Paso 8 En FusionInsight Manager, seleccione **O&M**. En el panel de navegación de la izquierda, elija **Log** > **Download**.

Paso 9 Expanda la lista desplegable **Service** y seleccione **HDFS** y **OMS** para el clúster de destino.

Paso 10 Haga clic en  en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 20 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 11 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema no borra automáticamente esta alarma y es necesario borrar manualmente la alarma.

Información relacionada

Ninguna

9.108 ALM-14028 El número de bloques a complementar supera el umbral

Descripción

El sistema comprueba el número de bloques a complementar cada 30 segundos y compara el número con el umbral. El número de bloques que se van a complementar tiene un umbral por defecto. Esta alarma se genera cuando el número de bloques a complementar excede el umbral.

Puede cambiar el umbral especificado por **Blocks Under Replicated (NameNode)** seleccionando **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster* > **HDFS** > **File and Block**.

Si **Trigger Count** se establece en **1** y el número de bloques a complementar es menor o igual que el umbral, esta alarma se borra. Si **Trigger Count** es mayor que **1** y el número de bloques a complementar es menor o igual al 90% del umbral, esta alarma se borra.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
14028	Minor	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.

Nombre	Significado
HostName	Especifica el host para el que se genera la alarma.
NameServiceName	Especifica el NameService para el que se genera la alarma.
Trigger Condition	Especifica el umbral para activar la alarma.

Impacto en el sistema

Los datos almacenados en HDFS se pierden. HDFS puede entrar en el modo de seguridad y no puede proporcionar servicios de escritura. Los datos de bloques perdidos no se pueden restaurar.

Causas posibles

- La instancia DataNode es anormal.
- Los datos se eliminan.
- El número de réplicas escritas en el archivo es mayor que el número de DataNodes.

Procedimiento

Paso 1 En FusionInsight Manager, seleccione **O&M**. En el panel de navegación de la izquierda, elija **Alarm** > **Alarms**. En la página que se muestra, compruebe si se genera la alarma **ALM-14003 El número de bloques HDFS perdidos supera el umbral**.

- En caso afirmativo, vaya a **Paso 2**.
- Si no, vaya a **Paso 3**.

Paso 2 Rectifique la falla de acuerdo con el procedimiento de manejo de **ALM-14003 El número de bloques HDFS perdidos supera el umbral**. Cinco minutos más tarde, compruebe si la alarma está borrada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 3**.

Paso 3 Inicie sesión en el cliente HDFS como usuario **root**. La contraseña de usuario la define el usuario antes de la instalación. Póngase en contacto con el administrador del clúster MRS para obtener la contraseña. Ejecute los siguientes comandos:

- Modo de seguridad:

  cd *Client installation directory*

  source bigdata_env

  kinit hdfs

- Modo normal:

  su - omm

  cd *Client installation directory*

  source bigdata_env

Paso 4 Ejecute el comando **hdfs fsck / >> fsck.log** para obtener el estado del clúster actual.

Paso 5 Ejecute el siguiente comando para contar el número (*M*) de bloques a replicar:

cat fsck.log | grep "Under-replicated"

Paso 6 Ejecute el siguiente comando para contar el número (*N*) de bloques a replicar en el directorio **/tmp/hadoop-yarn/staging/**:

cat fsck.log | grep "Under replicated" | grep "/tmp/hadoop-yarn/staging/" | wc -l

NOTA

/tmp/hadoop-yarn/staging/ es el directorio predeterminado. Si se modifica el directorio, obtenerlo del elemento de configuración **yarn.app.mapreduce.am.staging-dir** en el archivo **mapred-site.xml**.

Paso 7 Compruebe si el porcentaje de *N* es superior al 50% (N/M > 50%).

- En caso afirmativo, vaya a **Paso 8**.
- Si no, vaya a **Paso 9**.

Paso 8 Ejecute el siguiente comando para reconfigurar el número de réplicas de archivos en el directorio (establezca el número de réplicas de archivos en el número de DataNodes o el número predeterminado de réplicas de archivos):

hdfs dfs -setrep -w *Number of file replicas*/tmp/hadoop-yarn/staging/

NOTA

Para obtener el número predeterminado de réplicas de archivos:

Inicie sesión en el FusionInsight Manager, elija **Cluster > Services > HDFS > Configurations > All Configurations** y busque el parámetro **dfs.replication**. El valor de este parámetro es el número predeterminado de réplicas de archivos.

Compruebe si la alarma se borra 5 minutos más tarde.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 9**.

Recopilar información de fallas.

Paso 9 En FusionInsight Manager, seleccione **O&M**. En el panel de navegación de la izquierda, elija **Log** > **Download**.

Paso 10 Expanda la lista desplegable junto al campo **Service**. En el cuadro de diálogo **Services** que se muestra, seleccione **HDFS** para el clúster de destino.

Paso 11 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 12 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

Información relacionada

Ninguna

9.109 ALM-14029 Número de bloques en una réplica supera el umbral

Descripción

El sistema comprueba el número de bloques en una sola réplica cada cuatro horas y compara el número con el umbral. Existe un umbral para el número de bloques en una sola réplica. Esta alarma se genera cuando el número real de bloques en una única réplica excede el umbral.

Esta alarma se borra cuando el número de bloques a complementar es menor que el umbral.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
14029	Leves	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
NameServiceName	Especifica el NameService para el que se genera la alarma.
Trigger Condition	Especifica el umbral para activar la alarma.

Impacto en el sistema

Los datos de réplicas tienden a perderse cuando un nodo está defectuoso. Demasiados archivos de una sola réplica afectan a la seguridad del sistema de archivos HDFS.

Causas posibles

- El DataNode está defectuoso.
- El disco está defectuoso.

- Los archivos se escriben en una sola réplica.

Procedimiento

Paso 1 En FusionInsight Manager, seleccione **O&M**. En el panel de navegación de la izquierda, elija **Alarm** > **Alarms**. En la página que se muestra, compruebe si se genera la alarma **ALM-14003 El número de bloques HDFS perdidos supera el umbral**.

- En caso afirmativo, vaya a **Paso 2**.
- Si no, vaya a **Paso 3**.

Paso 2 Rectifique la falla de acuerdo con el procedimiento de manejo de **ALM-14003 El número de bloques HDFS perdidos supera el umbral**. En el siguiente periodo de detección, compruebe si la alarma está borrada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 3**.

Paso 3 Compruebe si los archivos de una sola réplica se han escrito en el servicio.

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 7**.

Paso 4 Inicie sesión en el cliente HDFS como usuario **root**. La contraseña de usuario la define el usuario antes de la instalación. Póngase en contacto con el administrador del clúster MRS para obtener la contraseña. Ejecute los siguientes comandos:

- Modo de seguridad:

  cd *Client installation directory*

  source bigdata_env

  kinit hdfs

- Modo normal:

  su - omm

  cd *Client installation directory*

  source bigdata_env

Paso 5 Ejecute el siguiente comando en el nodo cliente para aumentar el número de réplicas de un solo archivo de réplica:

hdfs dfs -setrep -w *file replica number file name or file path*

Paso 6 En el siguiente periodo de detección, compruebe si la alarma está borrada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 7**.

Recopilar información de fallas.

Paso 7 En FusionInsight Manager, seleccione **O&M**. En el panel de navegación de la izquierda, elija **Log** > **Download**.

Paso 8 Expanda la lista desplegable junto al campo **Service**. En el cuadro de diálogo **Services** que se muestra, seleccione **HDFS** para el clúster de destino.

Paso 9 Haga clic en  en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 10 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

Información relacionada

Ninguna

9.110 ALM-14030 HDFS permite la escritura de datos de una sola réplica

Descripción

Esta alarma se genera cuando **dfs.single.replication.enable** se establece en **true**, indicando que HDFS está configurado para permitir la escritura de datos de réplica única.

Esta alarma se borra cuando esta función está deshabilitada en HDFS.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
14030	Advertencia	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.

Impacto en el sistema

Si esta configuración está habilitada en el servidor y el número de réplicas HDFS configuradas en el cliente es 1, los datos de una sola réplica se pueden escribir en HDFS. Los datos de una única réplica pueden perderse. Por lo tanto, el sistema no permite la escritura de datos de réplica única de forma predeterminada. Si un servicio requiere escritura de datos de réplica única en un directorio, modifique el elemento de configuración de HDFS **dfs.single.replication.exclude.pattern**.

Causas posibles

El elemento de configuración HDFS **dfs.single.replication.enable** se establece en **true**.

Procedimiento

Paso 1 Inicie sesión en FusionInsight Manager y elija **Cluster** > **Services** > **HDFS**. En la página que se muestra, haga clic en la pestaña **Configurations** y luego en la subpestaña **All Configurations**.

Paso 2 Busque **dfs.single.replication.enable** en el cuadro de búsqueda, cambie el valor del elemento de configuración a **false** y haga clic en **Save**.

Paso 3 Espere unos 10 minutos y compruebe si la alarma está desactivada.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 4**.

Recopilar información de fallas.

Paso 4 En FusionInsight Manager, seleccione **O&M**. En el panel de navegación de la izquierda, elija **Log** > **Download**.

Paso 5 Expanda la lista desplegable junto al campo **Service**. En el cuadro de diálogo **Services** que se muestra, seleccione **HDFS** para el clúster de destino.

Paso 6 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 7 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

Información relacionada

Ninguna

9.111 ALM-16000 Porcentaje de sesiones conectadas al HiveServer al número máximo permitido supera el umbral

Descripción

El sistema detecta el porcentaje de sesiones conectadas al HiveServer hasta el número máximo de sesiones permitidas cada 30 segundos. Este indicador se puede ver en el nombre del **Cluster** > *Name of the desired cluster* > **Services** > **Hive > Instance** > *HiveServer instance***.** Esta alarma se genera cuando el porcentaje excede el valor predeterminado **90%**.

Para cambiar el umbral, elija **O&M > Alarm > Thresholds >** *Name of the desired cluster* > **Hive > Percentage of Sessions Connected to the HiveServer to Maximum Number of Sessions Allowed by the HiveServer**.

Cuando el **Trigger Count** es 1, esta alarma se borra cuando el porcentaje es menor o igual al umbral. Cuando el **Trigger Count** es mayor que 1, esta alarma se borra cuando el porcentaje es menor o igual al 90% del umbral.

Atributo

ID de alarma	Gravedad de la alarma	Borrado automáticamente
16000	Leves	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger Condition	Especifica el umbral que activa la alarma. Si el valor del indicador actual excede este umbral, se genera la alarma.

Impacto en el sistema

Si se genera una alarma de conexión, hay demasiadas sesiones conectadas a Hive y las nuevas conexiones no están disponibles.

Causas posibles

Hay demasiados clientes conectados a HiveServer.

Procedimiento

Aumentar el número máximo de conexiones a Hive.

Paso 1 En el portal del FusionInsight Manager, elija **Cluster** > *Name of the desired cluster* > **Services** > **Hive** > **Configurations >All Configurations**.

Paso 2 Busque **hive.server.session.control.maxconnections** y aumente el valor de este parámetro. Si el valor de este parámetro es **A**, el umbral es **B** y el número de sesiones conectadas al HiveServer es **C**, ajuste el valor de este parámetro de acuerdo con **A x B > C**. Para ver el número de sesiones conectadas al HiveServer, compruebe el valor de **Statistics for Sessions of the HiveServer** en la página de supervisión de Hive.

Paso 3 Verifique si la alarma se ha borrado.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 4**.

Recopilar información de fallas.

Paso 4 En el portal del FusionInsight Manager, elija **O&M** > **Log > Download**.

Paso 5 Seleccione **Hive** en el clúster requerido en el **Service**.

Paso 6 Haga clic en  en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 7 Póngase en contacto con el y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.112 ALM-16001 El uso del espacio en el almacén de Hive supera el umbral

Descripción

Esta alarma se genera cuando el uso del espacio del almacén de Hive supera el umbral especificado (85% de forma predeterminada). El sistema comprueba el uso del espacio del almacén de datos de Hive cada 30s. El indicador **Porcentaje de espacio de HDFS utilizado por Hive con respecto al espacio disponible** se puede ver en la página de supervisión del servicio Hive.

Para cambiar el umbral, elija **O&M > Alarm > Thresholds >** *Name of the desired cluster* > **Hive > Percentage of HDFS Space Used by Hive to the Available Space**.

Cuando el **Trigger Count** es 1, esta alarma se borra cuando el uso del espacio del almacén de Hive es menor o igual que el umbral. Cuando el **Trigger Count** es mayor que 1, esta alarma se borra cuando el uso del espacio del almacén de Hive es menor o igual al 90% del umbral.

NOTA

El administrador puede reducir el uso del espacio del almacén mediante la ampliación de la capacidad del almacén o la liberación del espacio utilizado.

Atributo

ID de alarma	Gravedad de la alarma	Borrado automáticamente
16001	Leves	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger Condition	Especifica el umbral que activa la alarma. Si el valor del indicador actual excede este umbral, se genera la alarma.

Impacto en el sistema

El sistema no puede escribir datos, lo que causa la pérdida de datos.

Causas posibles

- El límite superior de la capacidad HDFS disponible para Hive es demasiado pequeño.
- El espacio HDFS es insuficiente.
- Algunos nodos de datos se descomponen.

Procedimiento

Expandir la configuración del sistema.

Paso 1 Analice el uso de la capacidad HDFS del clúster y aumente el límite superior de la capacidad HDFS disponible para Hive.

Inicie sesión en el Administrador de FusionInsight, elija **Cluster** > *Name of the desired cluster* > **Services** > **Hive** > **Configurations > All Configurations**, find **hive.metastore.warehouse.size.percent**, y aumentar su valor para que una mayor capacidad de HDFS esté disponible para Hive. Supongamos que el valor del elemento de configuración es A, el espacio de almacenamiento de HDFS total es B, el umbral es C y el espacio de HDFS utilizado por Hive es D. La política de ajuste es A x B x C > D. El espacio total de almacenamiento de HDFS se puede ver en la página HDFS NameNode. El espacio HDFS utilizado por Hive se puede ver en la página de supervisión de Hive.

Paso 2 Verifique si la alarma se ha borrado.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 3**.

Expandir el sistema.

Paso 3 Expanda el sistema.

Paso 4 Verifique si la alarma se ha borrado.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 5**.

Comprobar si el nodo de datos es normal.

Paso 5 En el portal de Administrador de FusionInsight, haga clic en **O&M > Alarm > Alarms**.

Paso 6 Compruebe si existen "ALM-12006 error de nodo", "ALM-12007 error de proceso", o "ALM-14002 uso de disco de DataNode excede el umbral".

- En caso afirmativo, vaya a **Paso 7**.
- Si no, vaya a **Paso 9**.

Paso 7 Borre la alarma siguiendo los pasos proporcionados en "ALM-12006 error de nodo", "ALM-12007 error de proceso", y "ALM-14002 El uso del disco de DataNode supera el umbral".

Paso 8 Verifique si la alarma se ha borrado.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 9**.

Recopilar información de fallas.

Paso 9 En el portal del FusionInsight Manager, elija **O&M** > **Log > Download**.

Paso 10 Seleccione **Hive** en el clúster requerido en el **Service**.

Paso 11 Haga clic en  en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 12 Póngase en contacto con el y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.113 ALM-16002 Hive La Tasa de éxito de ejecución SQL es inferior al umbral

Descripción

El sistema comprueba el porcentaje de las sentencias HQL que se ejecutan correctamente cada 30 segundos. La fórmula es: Porcentaje de sentencias HQL que se ejecutan correctamente = Número de sentencias HQL que Hive ejecuta correctamente en un período especificado / Número total de sentencias HQL que Hive ejecuta. Este indicador se puede ver en el **Cluster > *Name of the desired cluster* > Services** > **Hive > Instance** > *HiveServer instance* **.** El umbral predeterminado del porcentaje de instrucciones HQL que se ejecutan correctamente es **90%**. Se informa de una alarma cuando el porcentaje es inferior al **90%**. Los usuarios pueden ver el nombre del host donde se genera una alarma en la información de ubicación de la alarma. La dirección IP del host es la dirección IP del nodo HiveServer.

Los usuarios pueden modificar el umbral eligiendo **O&M > Alarm > Thresholds >** *Name of the desired cluster* > **Hive** > **Percentage of HQL Statements That Are Executed Successfully by Hive**.

Esta alarma se borra cuando la tasa de éxito de ejecución es superior al 110% del umbral.

Atributo

ID de alarma	Gravedad de la alarma	Borrado automáticamente
16002	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger Condition	Especifica el umbral que activa la alarma. Si el valor del indicador actual excede este umbral, se genera la alarma.

Impacto en el sistema

La configuración y el rendimiento del sistema no pueden cumplir los requisitos de procesamiento del servicio.

Causas posibles

- Se produce un error de sintaxis en las sentencias HQL.
- El servicio HBase es anormal cuando se realiza una tarea Hive on HBase.
- El servicio Spark es anormal cuando se realiza una tarea Hive on Spark.
- Los servicios básicos dependientes, como HDFS, Yarn y ZooKeeper son anormales.

Procedimiento

Comprobar si las sentencias HQL cumplen con la sintaxis.

Paso 1 En la página Administrador de FusionInsight, seleccione **O&M** > **Alarm** para ver los detalles de la alarma y obtener el nodo donde se genera la alarma.

Paso 2 Utilice el cliente Hive para iniciar sesión en el nodo HiveServer donde se notifica una alarma. Consulte la sintaxis HQL proporcionada por Apache y compruebe si los comandos HQL son correctos. Para más detalles, consulte **https://cwiki.apache.org/confluence/display/hive/languagemanual**.

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 3**.

NOTA

Para ver al usuario que ejecuta una instrucción incorrecta, puede descargar el archivo de registro de auditoría HiveServer del nodo HiveServer donde se genera esta alarma. **Start Data** y **End Data** son 10 minutos antes y después del tiempo de generación de alarma, respectivamente. Abra el archivo de registro y busque la palabra clave **Result=FAIL** para filtrar la información de registro sobre la sentencia incorrecta y, a continuación, vea el usuario que ejecuta la sentencia incorrecta según **UserName** en la información de registro.

Paso 3 Introduzca las sentencias HQL correctas y compruebe si el comando se puede ejecutar correctamente.

- En caso afirmativo, vaya a **Paso 12**.
- Si no, vaya a **Paso 4**.

Comprobar si el servicio HBase es anormal.

Paso 4 Compruebe si se realiza una tarea Hive on HBase con el usuario que ejecuta el comando HQL.

- En caso afirmativo, vaya a **Paso 5**.
- Si no, vaya a **Paso 8**.

Paso 5 En la página Administrador de FusionInsight, haga clic en **Cluster** > *Name of the desired cluster* > **Services** y compruebe si el servicio HBase es normal en la lista de servicios.

- En caso afirmativo, vaya a **Paso 8**.
- Si no, vaya a **Paso 6**.

Paso 6 Elija **O&M** > **Alarm**, verifique las alarmas relacionadas que se muestran en la página de alarma y borre de acuerdo con la ayuda de alarma relacionada.

Paso 7 Introduzca las sentencias HQL correctas y compruebe si el comando se puede ejecutar correctamente.

- En caso afirmativo, vaya a **Paso 12**.
- Si no, vaya a **Paso 8**.

Compruebe si HDFS, Yarn y ZooKeeper son normales.

Paso 8 En el portal del FusionInsight Manager, haga clic en **Cluster** > *Name of the desired cluster* > **Services**.

Paso 9 En la lista de servicios, compruebe si los servicios, como HDFS, Yarn y ZooKeeper son normales.

- En caso afirmativo, vaya a **Paso 12**.
- Si no, vaya a **Paso 10**.

Paso 10 Compruebe las alarmas relacionadas que se muestran en la página de alarmas y bórrelas de acuerdo con la ayuda de alarma relacionada.

Paso 11 Introduzca las sentencias HQL correctas y compruebe si el comando se puede ejecutar correctamente.

- En caso afirmativo, vaya a **Paso 12**.
- Si no, vaya a **Paso 13**.

Paso 12 Después de 1 minuto, compruebe si la alarma está borrada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 13**.

Recopilar información de fallas.

Paso 13 En la página de inicio del Administrador FusionInsight, elija **O&M** > **Log > Download**.

Paso 14 Seleccione los siguientes nodos en el clúster requerido desde el **Service**:

- MapReduce
- Hive

Paso 15 Haga clic en  en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 16 Póngase en contacto con el y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.114 ALM-16003 El uso de subprocesos en segundo plano supera el umbral

Descripción

El sistema comprueba el uso de subprocesos en segundo plano cada 30 segundos. Esta alarma se genera cuando el uso del grupo de subprocesos en segundo plano de Hive excede el umbral, 90% de forma predeterminada.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
16003	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger condition	Especifica el umbral que activa la alarma. Si el valor del indicador actual excede este umbral, se genera la alarma.

Impacto en el sistema

Hay demasiados subprocesos en segundo plano, por lo que la tarea recién enviada no puede ejecutarse a tiempo.

Causas posibles

El uso del grupo de hilos de fondo de Hive es excesivamente alto cuando:

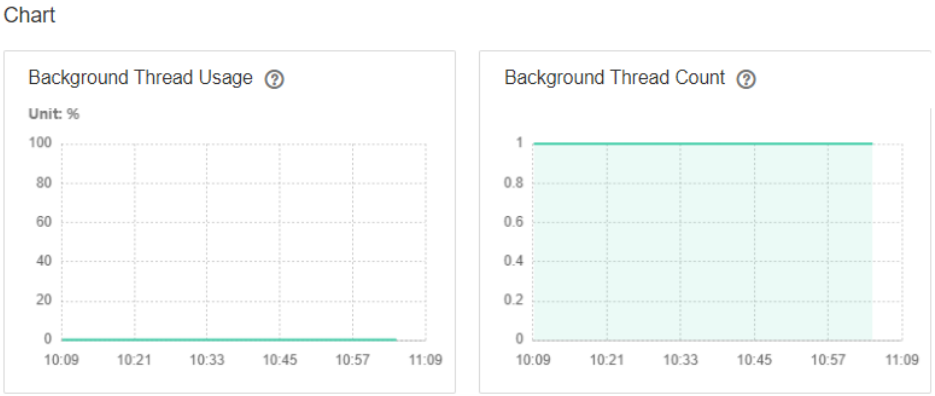
- Hay muchas tareas ejecutadas en el grupo de subprocesos de fondo de HiveServer.
- La capacidad del grupo de subproceso de fondo de HiveServer es demasiado pequeña.

Procedimiento

Verificar la cantidad de tareas ejecutadas en el grupo de subprocesos en segundo plano de HiveServer.

Paso 1 En el portal del FusionInsight Manager, seleccione **Cluster** > *Name of the desired cluster* > **Services** > **Hive**. En la página mostrada, haga clic en **HiveServer Instance** y compruebe los valores de **Background Thread Count** y **Background Thread Usage**.

Figura 9-27 Fondo



Paso 2 Compruebe si el número de subprocesos de fondo en la última media hora es excesivamente alto. (Por defecto, el número de cola es 100, y el número de subproceso se considera como alto si es 90 o más.)

- Si lo es, vaya a **Paso 3**.
- Si no es así, vaya a **Paso 5**.

Paso 3 Ajuste el número de tareas enviadas al grupo de subprocesos en segundo plano. (Por ejemplo, cancele algunas tareas que consumen mucho tiempo con bajo rendimiento.)

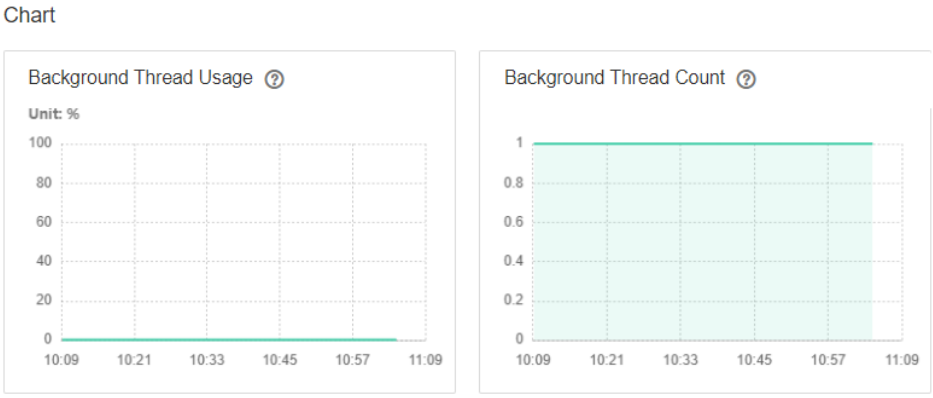
Paso 4 Compruebe si los valores de Recuento de subprocesos en segundo plano y Uso de subprocesos en segundo plano disminuyen.

- Si lo es, vaya a **Paso 7**.
- Si no es así, vaya a **Paso 5**.

Comprobar la capacidad del grupo de subprocesos de fondo de HiveServer.

Paso 5 En el portal del FusionInsight Manager, seleccione **Cluster** > *Name of the desired cluster* > **Services** > **Hive**. En la página mostrada, haga clic en **HiveServer Instance** y compruebe los valores de Background Thread Count y Background Thread Usage.

Figura 9-28 Fondo



Paso 6 Aumente el valor de **hive.server2.async.exec.threads** en el archivo **${BIGDATA_HOME}/FusionInsight_HD_/1_23_HiveServer/etc/hive-site.xml**. Por ejemplo, aumente el valor en un 20%.

Paso 7 Guarde la modificación.

Paso 8 Verifique si la alarma se ha borrado.

- Si lo es, no se requiere ninguna otra acción.
- Si no es así, vaya a **Paso 9**.

Recopilar información de fallas.

Paso 9 En el portal del FusionInsight Manager, elija **O&M** > **Log > Download**.

Paso 10 Seleccione **Hive** en el clúster requerido en el **Service**.

Paso 11 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 12 Póngase en contacto con el y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.115 ALM-16004 Servicio Hive no disponible

Descripción

Esta alarma se genera cuando el servicio HiveServer no está disponible. El sistema comprueba el estado del servicio HiveServer cada 60 segundos.

Esta alarma se borra cuando el servicio HiveServer es normal.

Atributo

ID de alarma	Gravedad de la alarma	Borrado automáticamente
16004	Crítica	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

El sistema no puede proporcionar servicios de carga, consulta y extracción de datos.

Causas posibles

- La falta de disponibilidad del servicio Hive puede estar relacionada con las fallas del proceso Hive, así como con servicios básicos, como ZooKeeper y el sistema de archivos distribuidos de Hadoop (HDFS), Yarn y DBService.
  - El servicio ZooKeeper es anormal.
  - El servicio HDFS es anormal.
  - El servicio Yarn es anormal.
  - El servicio DBService es anormal.
  - El proceso de servicio de Hive es anormal. Si la alarma es causada por una falla del proceso de Hive, el informe de alarma tiene un retraso de aproximadamente 5 minutos.
- La comunicación de red entre Hive y los servicios básicos se interrumpe.

Procedimiento

Comprobar el estado de proceso de HiveServer/MetaStore.

Paso 1 En el portal de FusionInsight Manager, haga clic en **Cluster >** *Name of the desired cluster* **> Services** > **Hive** > **Instance**. En la lista de instancias de Hive, compruebe si las instancias HiveServer o MetaStore están en el estado Unknown.

- En caso afirmativo, vaya a **Paso 2**.
- Si no, vaya a **Paso 4**.

Paso 2 En la lista de instancias de Hive, elija **More** > **Restart Instance** para reiniciar el proceso HiveServer/MetaStore.

Paso 3 En la lista de alarmas, compruebe si **Hive Service Unavailable** está borrado.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 4**.

Verificar el estado del servicio de ZooKeeper.

Paso 4 En el FusionInsight Manager, compruebe si la lista de alarmas contiene **Process Fault**.

- En caso afirmativo, vaya a **Paso 5**.
- Si no, vaya a **Paso 8**.

Paso 5 En el **Process Fault**, compruebe si **ServiceName** tiene un valor de tipo **ZooKeeper**.

- En caso afirmativo, vaya a **Paso 6**.
- Si no, vaya a **Paso 8**.

Paso 6 Rectifique la falla siguiendo los pasos proporcionados en "ALM-12007 Falla de proceso".

Paso 7 En la lista de alarmas, compruebe si **Hive Service Unavailable** está borrado.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 8**.

Comprobar el estado de servicio HDFS.

Paso 8 En el FusionInsight Manager, compruebe si la lista de alarmas contiene **HDFS Service Unavailable**.

- En caso afirmativo, vaya a **Paso 9**.
- Si no, vaya a **Paso 11**.

Paso 9 Rectifique el falla siguiendo los pasos proporcionados en "ALM-14000 Servicio HDFS no disponible".

Paso 10 En la lista de alarmas, compruebe si **Hive Service Unavailable** está borrado.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 11**.

Comprobar el estado de servicio Yarn.

Paso 11 En la lista de alarmas del FusionInsight Manager, compruebe si se ha generado **Servicio Yarn no disponible**.

- En caso afirmativo, vaya a **Paso 12**.
- Si no, vaya a **Paso 14**.

Paso 12 Rectifique la falla. Para obtener más información, consulte "ALM-18000 Servicio Yarn no disponible".

Paso 13 En la lista de alarmas, compruebe si **Hive Service Unavailable** está borrado.

- De ser así, no se requiere ninguna acción adicional.

- Si no, vaya a **Paso 14**.

Comprobar el estado del servicio DBService.

Paso 14 En la lista de alarmas del FusionInsight Manager, compruebe si se ha generado **Servicio DBService no disponible**.

- En caso afirmativo, vaya a **Paso 15**.
- Si no, vaya a **Paso 17**.

Paso 15 Rectifique la falla. Para obtener más información, consulte "ALM-27001 Servicio DBService no disponible".

Paso 16 En la lista de alarmas, compruebe si **Hive Service Unavailable** está borrado.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 17**.

Compruebe la conexión de red entre Hive y ZooKeeper, HDFS, Yarn y DBService.

Paso 17 En el FusionInsight Manager, elija **Cluster >** *Name of the desired cluster* **> Services** > **Hive**.

Paso 18 Haga clic en **Instance**.

Se muestra la lista de instancias HiveServer.

Paso 19 Haga clic en **Host Name** en la fila de **HiveServer**.

Se muestra la página de estado del host HiveServer activo.

Paso 20 Registre la dirección IP en **Basic Information**.

Paso 21 Utilice la dirección IP obtenida en **Paso 20** para iniciar sesión en el host donde se ejecuta el HiveServer activo como usuario **omm**.

Paso 22 Ejecute el comando **ping** para comprobar si la comunicación entre el host que ejecuta el HiveServer activo y los hosts que ejecutan los servicios ZooKeeper, HDFS, Yarn, y DBService es normal. (Obtenga las direcciones IP de los hosts que ejecutan los servicios ZooKeeper, HDFS, Yarn y DBService de la misma manera que para obtener la dirección IP del HiveServer activo.)

- En caso afirmativo, vaya a **Paso 25**.
- Si no, vaya a **Paso 23**.

Paso 23 Póngase en contacto con el administrador para restaurar la red.

Paso 24 En la lista de alarmas, compruebe si **Hive Service Unavailable** está borrado.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 25**.

Recopilar información de fallas.

Paso 25 En el FusionInsight Manager, elija **O&M** > **Log > Download**.

Paso 26 Seleccione los siguientes nodos en el clúster requerido desde el **Service**:

- ZooKeeper
- HDFS
- Yarn

- DBService
- Hive

Paso 27 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 28 Póngase en contacto con el y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.116 ALM-16005 El uso de memoria heap del proceso Hive supera el umbral

Descripción

El sistema comprueba el estado del servicio Hive cada 30 segundos. La alarma se genera cuando el uso de memoria heap de un servicio Hive supera el umbral (95% de la memoria máxima).

Los usuarios pueden elegir **O&M > Alarm > Thresholds >** *Name of the desired cluster* > **Hive** para cambiar el umbral.

La alarma se borra cuando el uso de memoria heap es menor o igual que el umbral.

Atributo

ID de alarma	Gravedad de la alarma	Borrado automáticamente
16005	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el nombre del servicio para el que se genera la alarma.

Nombre	Significado
RoleName	Especifica el nombre del rol para el que se genera la alarma.
HostName	Especifica el objeto (ID de host) para el que se genera la alarma.

Impacto en el sistema

Cuando el uso de memoria heap de Hive es excesivo, el rendimiento de la operación de tarea de Hive se ve afectado. Además, puede producirse un desbordamiento de memoria para que el servicio Hive no esté disponible.

Causas posibles

La memoria heap de la instancia de Hive en el nodo se utiliza en exceso o la memoria heap se asigna de forma inadecuada. Como resultado, el uso excede el umbral.

Procedimiento

Comprobar el uso de memoria heap.

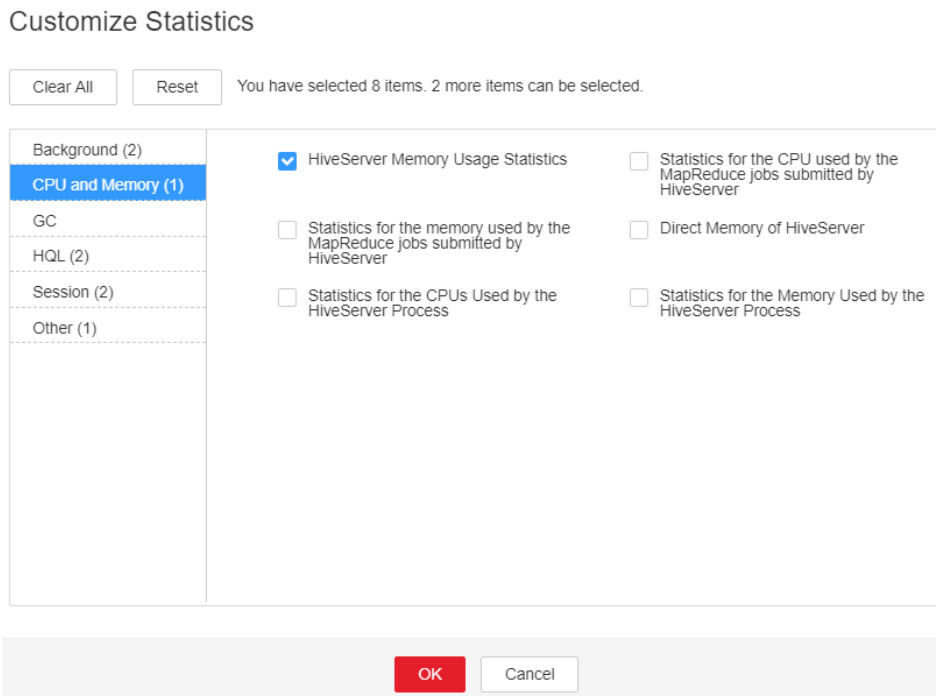
Paso 1 En el portal del Administrador FusionInsight, haga clic en **O&M > Alarm > Alarms** y seleccione la alarma cuyo **Alarm ID** es **16005**. A continuación, compruebe el nombre del rol de **Location** y confirme la dirección IP de la instancia.

- Si el rol para el que se genera la alarma es "HiveServer", vaya a **Paso 2**.
- Si el rol para el que se genera la alarma es MetaStore, vaya a **Paso 3**.

Paso 2 En el portal del FusionInsight Manager, elija **Cluster** > *Name of the desired cluster* > **Services** > **Hive** > **Instance** y haga clic en el HiveServer para el que se genera la alarma para ir a la página **Dashboard**. Haga clic en el menú desplegable en el área **Chart** y elija **Customize** > **CPU and Memory** y seleccione **HiveServer Memory Usage Statistics** y haga clic en **OK** y compruebe si la memoria heap usada del servicio HiveServer alcanza el umbral(valor predeterminado: 95%) de la memoria heap máxima especificada para HiveServer.

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 7**.

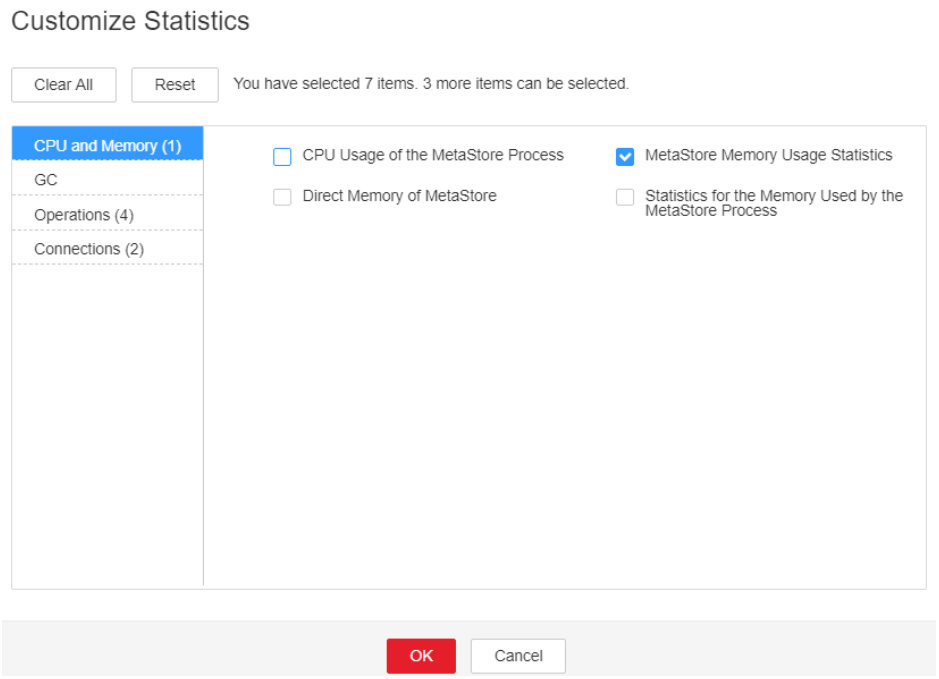
Figura 9-29 Estadísticas de uso de memoria de HiveServer



Paso 3 En el portal del FusionInsight Manager, elija **Cluster** > *Name of the desired cluster* > **Services** > **Hive** > **Instance** y haga clic en el MetaStore para el que se genera la alarma para ir a la página **Dashboard**. Haga clic en el menú desplegable en el área **Chart** y elija **Customize** > **CPU and Memory** y seleccione **MetaStore Memory Usage Statistics** y haga clic en **OK** y compruebe si la memoria heap usada del servicio MetaStore alcanza el umbral(valor predeterminado: 95%) de la memoria heap máxima especificada para MetaStore.

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 7**.

Figura 9-30 Estadísticas de uso de memoria de MetaStore



Paso 4 En el portal del FusionInsight Manager, seleccione **Cluster** > *Name of the desired cluster* > **Services** > **Hive** > **Configurations > All Configurations**. Seleccione **HiveServer/MetaStore** > **JVM**. Ajuste el valor de **-Xmx** en **HIVE_GC_OPTS/METASTORE_GC_OPTS** como las siguientes reglas. Haga clic en **Save**.

NOTA

Sugerencias para la configuración de los parámetros de GC para el HiveServer:

- Cuando la memoria heap utilizada por el proceso HiveServer alcanza el umbral (valor predeterminado: 95%) de la memoria heap máxima establecida por el proceso HiveServer, cambie el valor de **-Xmx** al doble del valor predeterminado. Por ejemplo, si **-Xmx** está establecido en 2GB de forma predeterminada, cambie el valor de **-Xmx** a 4GB. Se recomienda cambiar el valor de **-Xms** para establecer la relación de **-Xms** y **-Xmx** a 1:2 para evitar problemas de rendimiento cuando JVM es dinámica. En la página de inicio de FusionInsight Manager, elija **O&M**> **Alarm**> **Thresholds** > *Name of the desired cluster* **> Hive** > **CPU and Memory** > **HiveServer Heap Memory Usage Statistics (HiveServer)** para ve **Threshold**.

Sugerencias para la configuración de los parámetros de GC para el MetaServer:

- Cuando la memoria heap utilizada por el proceso MetaStore alcanza el umbral (valor predeterminado: 95%) de la memoria heap máxima establecida por el proceso MetaStore, cambie el valor de **-Xmx** al doble del valor predeterminado. Por ejemplo, si **-Xmx** está establecido en 2GB de forma predeterminada, cambie el valor de **-Xmx** a 4GB. En la página de inicio de FusionInsight Manager, elija **O&M**> **Alarm**> **Thresholds** > *Name of the desired cluster* **> Hive** > **CPU and Memory** > **MetaStore Heap Memory Usage Statistics (MetaStore)** para ver **Threshold**.
- Se recomienda cambiar el valor de **-Xms** para establecer la relación de **-Xms** y **-Xmx** a 1:2 para evitar problemas de rendimiento cuando JVM es dinámica.

Paso 5 Haga clic en **More > Restart Service** para reiniciar el servicio.

Paso 6 Verifique si la alarma se ha borrado.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 7**.

Recopilar información de fallas.

Paso 7 En el portal del FusionInsight Manager, elija **O&M** > **Log > Download**.

Paso 8 Seleccione **Hive** en el clúster requerido en el **Service**.

Paso 9 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 10 Póngase en contacto con el y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.117 ALM-16006 El uso de la memoria directa del proceso Hive supera el umbral

Descripción

El sistema comprueba el estado del servicio Hive cada 30 segundos. La alarma se genera cuando el uso de memoria directa de un servicio Hive supera el umbral (95% de la memoria máxima).

Los usuarios pueden elegir **O&M > Alarm > Thresholds >** *Name of the desired cluster* **> Hive** para cambiar el umbral.

La alarma se borra cuando el uso directo de memoria es menor o igual que el umbral.

Atributo

ID de alarma	Gravedad de la alarma	Borrado automáticamente
16006	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el nombre del servicio para el que se genera la alarma.

Nombre	Significado
RoleName	Especifica el nombre del rol para el que se genera la alarma.
HostName	Especifica el objeto (ID de host) para el que se genera la alarma.
Trigger Condition	Especifica el umbral que activa la alarma. Si el valor del indicador actual excede este umbral, se genera la alarma.

Impacto en el sistema

Cuando el uso de memoria directa de Hive es excesivo, el rendimiento de la operación de tarea Hive se ve afectado. Además, puede producirse un desbordamiento de memoria para que el servicio Hive no esté disponible.

Causas posibles

La memoria directa de la instancia de Hive en el nodo se utiliza en exceso o la memoria directa se asigna de forma inapropiada. Como resultado, el uso excede el umbral.

Procedimiento

Comprobar el uso de memoria directa.

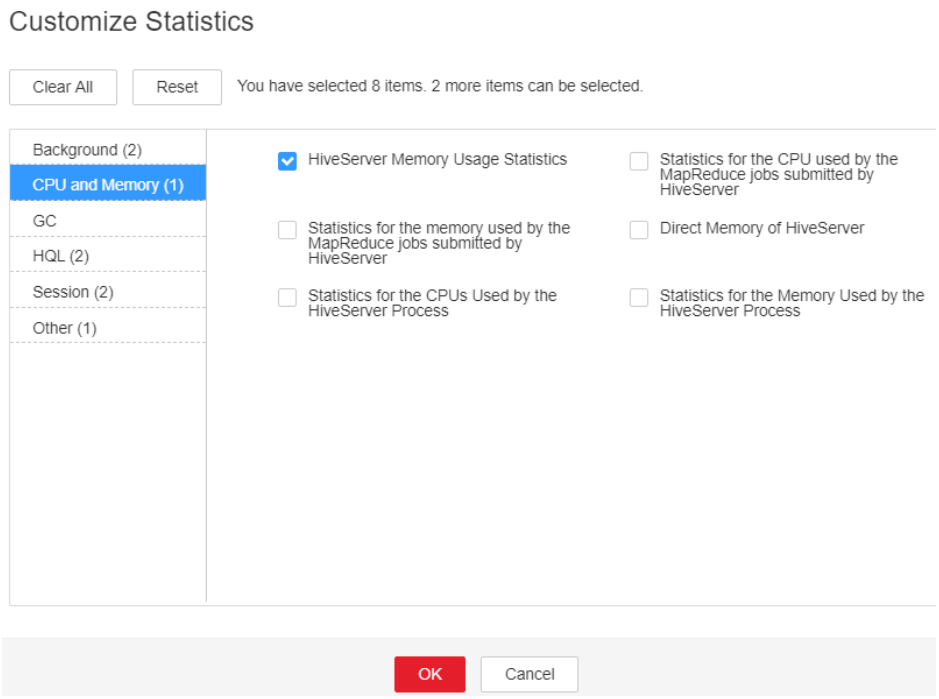
Paso 1 En el portal del Administrador FusionInsight, haga clic en **O&M > Alarm > Alarms** y seleccione la alarma cuyo **Alarm ID** es **16006**. A continuación, compruebe el nombre del rol de **Location** y confirme la dirección IP de la instancia.

- Si el rol para el que se genera la alarma es HiveServer, vaya a **Paso 2**.
- Si el rol para el que se genera la alarma es MetaStore, vaya a **Paso 3**.

Paso 2 En el portal del FusionInsight Manager, elija **Cluster** > *Name of the desired cluster* > **Services > Hive > Instance** y haga clic en el HiveServer para el que se genera la alarma para ir a la página **Dashboard**. Haga clic en el menú desplegable en el área **Chart** y elija **Customize** > **CPU and Memory** y seleccione **HiveServer Memory Usage Statistics** y haga clic en **OK** y compruebe si la memoria directa utilizada del servicio HiveServer alcanza el umbral (valor predeterminado: 95%) de la memoria directa máxima especificada para HiveServer.

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 7**.

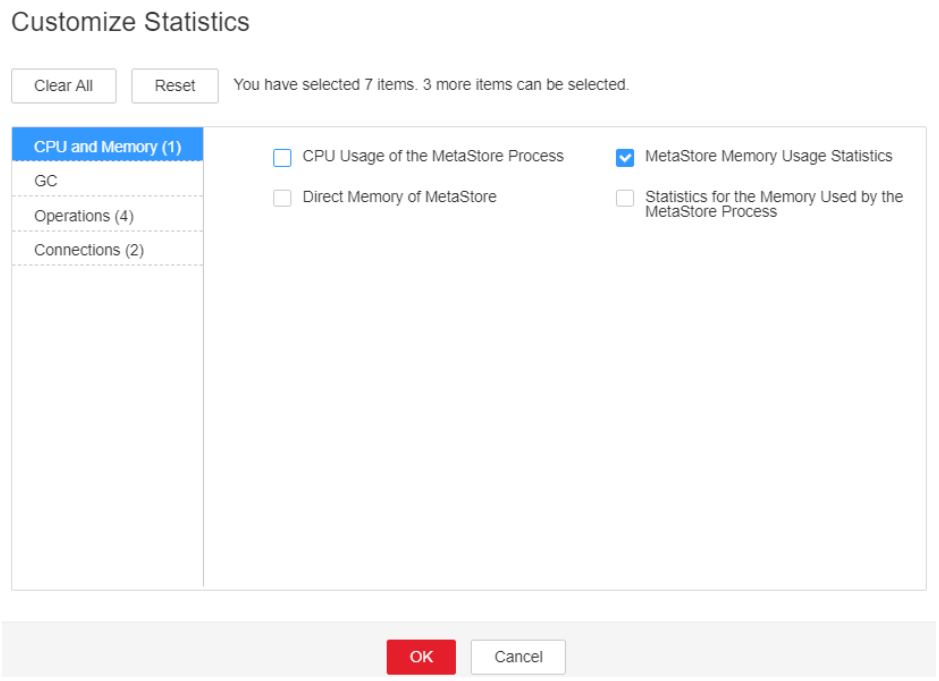
Figura 9-31 Estadísticas de uso de memoria de HiveServer



Paso 3 En el portal del FusionInsight Manager, elija **Cluster** > *Name of the desired cluster* > **Services** > **Hive** > **Instance** y haga clic en el MetaStore para el que se genera la alarma para ir a la página **Dashboard**. Haga clic en el menú desplegable en el área **Chart** y elija **Customize** > **CPU and Memory** y seleccione **MetaStore Memory Usage Statistics** y haga clic en **OK** y compruebe si la memoria directa utilizada del servicio MetaStore alcanza el umbral (valor predeterminado: 95%) de la memoria directa máxima especificada para MetaStore.

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 7**.

Figura 9-32 Estadísticas de uso de memoria de MetaStore



Paso 4 En el portal del FusionInsight Manager, seleccione **Cluster** >*Name of the desired cluster* > **Services** > **Hive** > **Configurations > All Configurations**. Elija **HiveServer/MetaStore** > **JVM**. Ajuste el valor de **-XX:MaxDirectMemorySize** en **HIVE_GC_OPTS/ METASTORE_GC_OPTS** como las siguientes reglas. Haga clic en **Save**.

NOTA

Sugerencias para la configuración de los parámetros de GC para el HiveServer:

- Se recomienda establecer el valor de **-XX:MaxDirectMemorySize** en 1/8 del valor de **-Xmx**. Por ejemplo, si **-Xmx** se establece en 8 GB, **-XX:MaxDirectMemorySize** se establece en 1024 MB. Si **-Xmx** se establece en 4 GB, **-XX:MaxDirectMemorySize** se establece en 512 MB. Se recomienda que el valor de **-XX:MaxDirectMemorySize** sea mayor o igual a 512 MB.

Sugerencias para la configuración de los parámetros de GC para el MetaServer:

- Se recomienda establecer el valor de **-XX:MaxDirectMemorySize** en 1/8 del valor de **-Xmx**. Por ejemplo, si **-Xmx** se establece en 8 GB, **-XX:MaxDirectMemorySize** se establece en 1024 MB. Si **-Xmx** se establece en 4 GB, **-XX:MaxDirectMemorySize** se establece en 512 MB. Se recomienda que el valor de **-XX:MaxDirectMemorySize** sea mayor o igual a 512 MB.

Paso 5 Haga clic en **More > Restart Service** para reiniciar el servicio.

Paso 6 Verifique si la alarma se ha borrado.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 7**.

Recopilar información de fallas.

Paso 7 En el portal del FusionInsight Manager, elija **O&M** > **Log > Download**.

Paso 8 Seleccione **Hive** en el clúster requerido en el **Service**.

Paso 9 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 10 Póngase en contacto con el y envíe los registros de fallas recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.118 ALM-16007 El tiempo de Hive GC supera el umbral

Descripción

El sistema comprueba el tiempo de recolección de basura (GC) del servicio Hive cada 60 segundos. Esta alarma se genera cuando el tiempo GC detectado excede el umbral (excede 12 segundos durante tres comprobaciones consecutivas). Para cambiar el umbral, elija **O&M > Alarm > Thresholds >** *Name of the desired cluster* > **Hive**. Esta alarma se borra cuando el tiempo de GC de Hive es menor o igual que el umbral.

Atributo

ID de alarma	Gravedad de la alarma	Borrado automáticamente
16007	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el nombre del servicio para el que se genera la alarma.
RoleName	Especifica el nombre del rol para el que se genera la alarma.
HostName	Especifica el objeto (ID de host) para el que se genera la alarma.
Trigger Condition	Especifica el umbral que activa la alarma. Si el valor del indicador actual excede este umbral, se genera la alarma.

Impacto en el sistema

Si el tiempo de GC excede el umbral, la lectura y escritura de los datos de Hive se verán afectados.

Causas posibles

La memoria de las instancias de Hive se utiliza en exceso, la memoria heap se asigna de forma inadecuada. Como resultado, los GC ocurren con frecuencia.

Procedimiento

Comprobar el tiempo de GC.

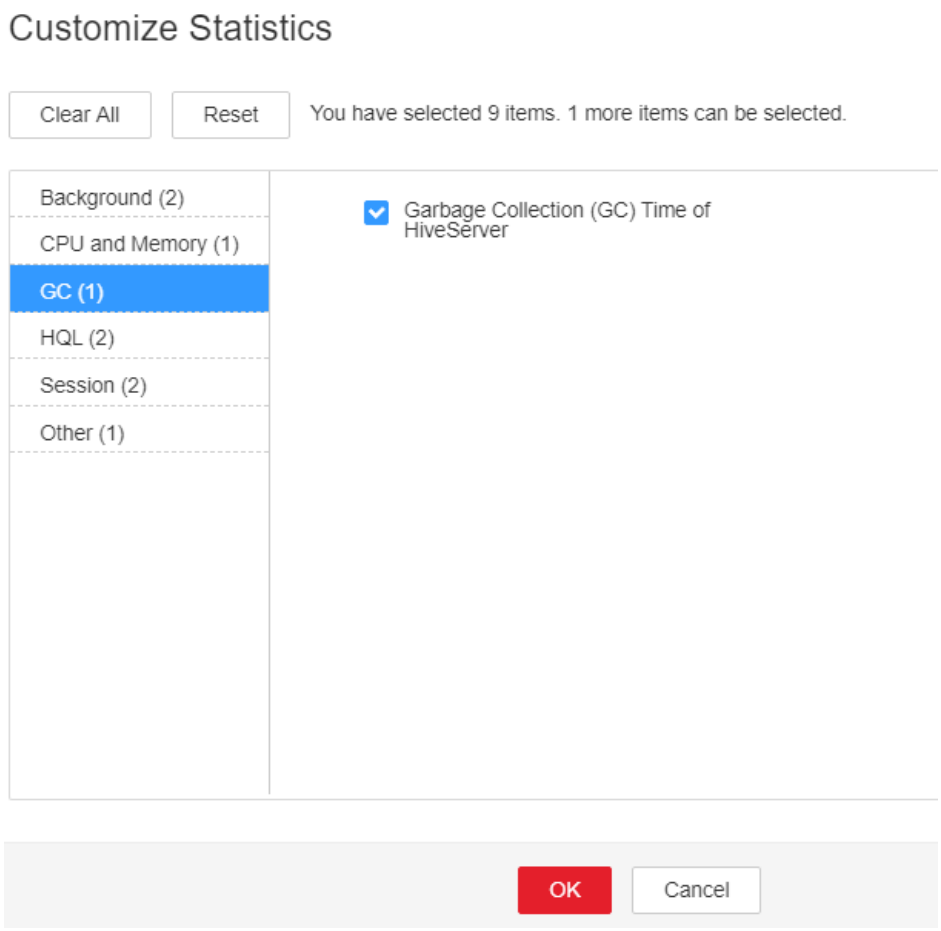
Paso 1 En el portal del FusionInsight Manager, haga clic en **O&M > Alarm > Alarms** y seleccione la alarma cuyo **Alarm ID** es **16007**. A continuación, compruebe el nombre del rol de **Location** y confirme la dirección IP de la instancia.

- Si el rol para el que se genera la alarma es HiveServer, vaya a **Paso 2**.
- Si el rol para el que se genera la alarma es MetaStore, vaya a **Paso 3**.

Paso 2 En el portal del FusionInsight Manager, elija **Cluster** >*Name of the desired cluster* > **Services** > **Hive** > **Instance** y haga clic en el HiveServer para el que se genera la alarma para ir a la página **Dashboard**. Haga clic en el menú desplegable en el área **Chart** y elija **Customize** > **GC** y seleccione **Garbage Collection (GC) Time of HiveServer** y haga clic en **OK** para comprobar si el tiempo de GC es más de 12 segundos.

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 7**.

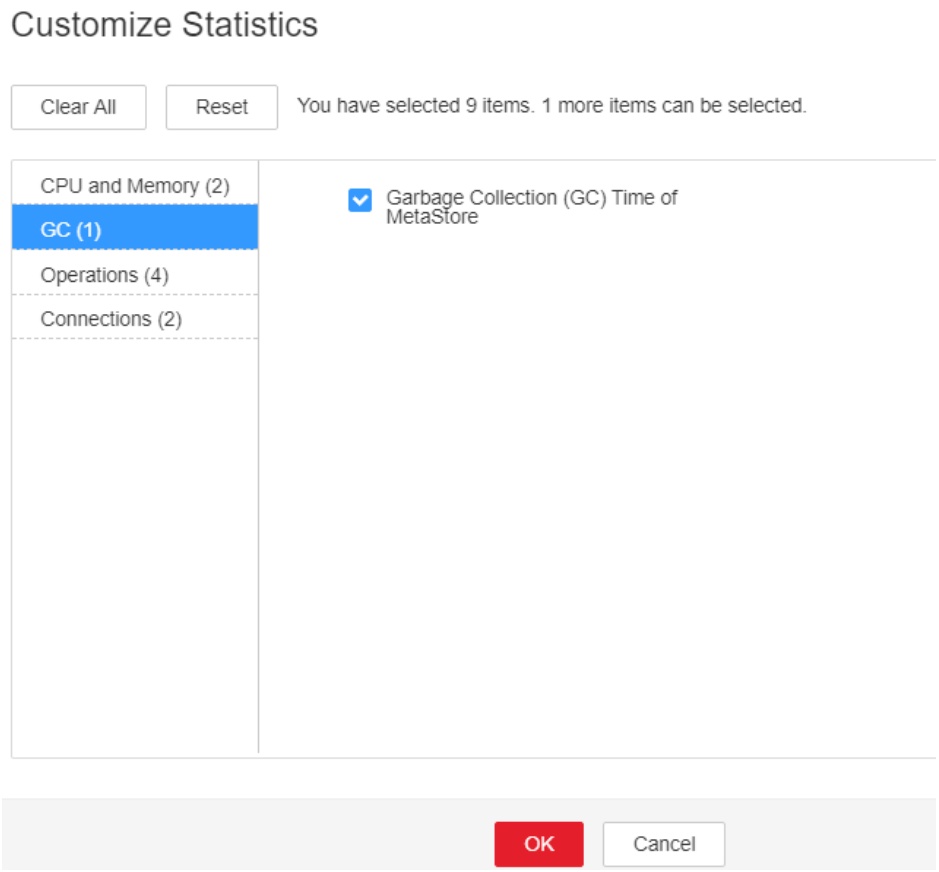
Figura 9-33 Tiempo de Recolección de basura (GC) de HiveServer



Paso 3 En el portal del FusionInsight Manager, elija **Cluster** >*Name of the desired cluster* > **Services** > **Hive** > **Instance** y haga clic en el MetaStore para el que se genera la alarma para ir a la página **Dashboard** . Haga clic en el menú desplegable en el área **Chart** y elija **Customize** > **GC** y seleccione **Garbage Collection (GC) Time of MetaStore** y haga clic en **OK** para comprobar si el tiempo de GC es más de 12 segundos.

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 7**.

Figura 9-34 Tiempo de Recolección de basura (GC) de MetaStore



Comprobar la configuración de JVM actual.

Paso 4 En el portal del FusionInsight Manager, seleccione **Cluster** >*Name of the desired cluster* > **Services > Hive > Configurations > All Configurations**. Seleccione **HiveServer/MetaStore** > **JVM**. Ajuste el valor de **-Xmx** en **HIVE_GC_OPTS/METASTORE_GC_OPTS** como las siguientes reglas. Haga clic en **Save**.

NOTA

Sugerencias para la configuración de los parámetros de GC para el HiveServer:

- Cuando el tiempo de GC de Hive exceda el umbral, cambie el valor de **-Xmx** al doble del valor predeterminado. Por ejemplo, si **-Xmx** está establecido en 2 GB de forma predeterminada, cambie el valor de **-Xmx** a 4 GB.
- Se recomienda cambiar el valor de **-Xms** para establecer la relación de **-Xms** y **-Xmx** a 1:2 para evitar problemas de rendimiento cuando JVM es dinámica.

Sugerencias para la configuración de los parámetros de GC para el MetaServer:

- Cuando el tiempo de Meta GC excede el umbral, cambie el valor de **-Xmx** al doble del valor predeterminado. Por ejemplo, si **-Xmx** está establecido en 2 GB de forma predeterminada, cambie el valor de **-Xmx** a 4 GB.
- Se recomienda cambiar el valor de **-Xms** para establecer la relación de **-Xms** y **-Xmx** a 1:2 para evitar problemas de rendimiento cuando JVM es dinámica.

Paso 5 Haga clic en **More > Restart Service** para reiniciar el servicio.

Paso 6 Verifique si la alarma se ha borrado.

- De ser así, no se requiere ninguna acción adicional.

- Si no, vaya a **Paso 7**.

Recopilar información de fallas.

Paso 7 En el portal del FusionInsight Manager de clústeres activos y en espera, seleccione **O&M** > **Log > Download**.

Paso 8 En el **Service**, seleccione **Hive** en el clúster requerido.

Paso 9 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 10 Póngase en contacto con el y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.119 ALM-16008 El uso de memoria no heap del proceso Hive supera el umbral

Descripción

El sistema comprueba el estado del servicio Hive cada 30 segundos. La alarma se genera cuando el uso de memoria no heap de un servicio Hive excede el umbral (95% de la memoria máxima).

Los usuarios pueden elegir **O&M > Alarm > Thresholds >** *Name of the desired cluster* > **Hive** para cambiar el umbral.

La alarma se borra cuando el uso de memoria no heap es menor o igual que el umbral.

Atributo

ID de alarma	Gravedad de la alarma	Borrado automáticamente
16008	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el nombre del servicio para el que se genera la alarma.
RoleName	Especifica el nombre del rol para el que se genera la alarma.
HostName	Especifica el objeto (ID de host) para el que se genera la alarma.

Impacto en el sistema

Cuando el uso de memoria no heap de Hive es excesivo, el rendimiento de la operación de tarea Hive se ve afectado. Además, puede producirse un desbordamiento de memoria para que el servicio Hive no esté disponible.

Causas posibles

La memoria no heap de la instancia de Hive en el nodo se utiliza en exceso o la memoria no heap se asigna de forma inadecuada. Como resultado, el uso excede el umbral.

Procedimiento

Verificar el uso de memoria no heap.

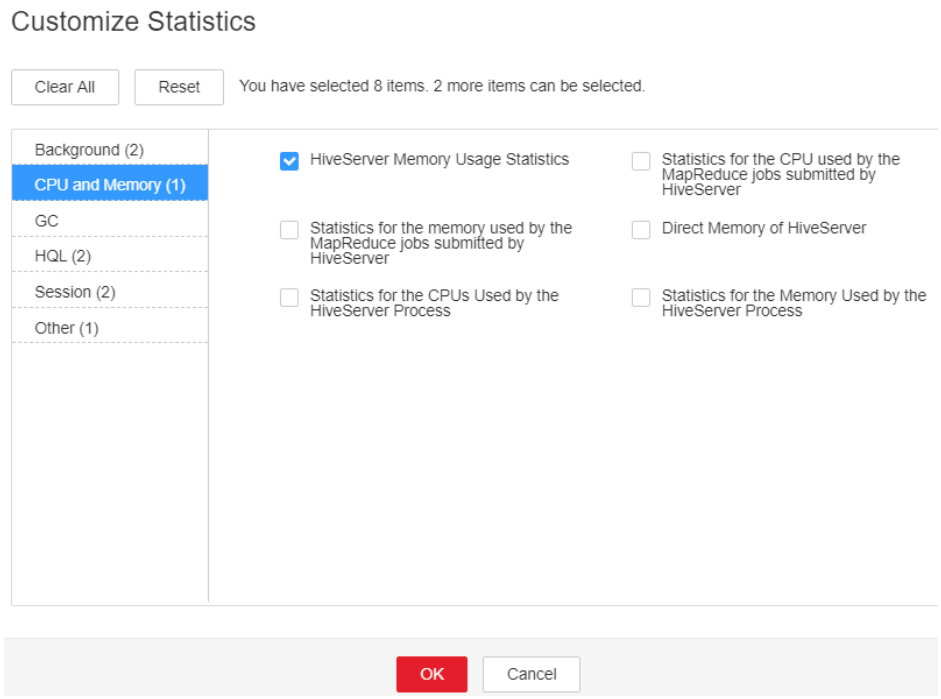
Paso 1 En el portal del FusionInsight Manager, haga clic en **O&M > Alarm > Alarms** y seleccione la alarma cuyo **Alarm ID** is **16008**. A continuación, compruebe el nombre del rol de **Location** y confirme la dirección IP de la instancia.

- Si el rol para el que se genera la alarma es HiveServer, vaya a **Paso 2**.
- Si el rol para el que se genera la alarma es MetaStore, vaya a **Paso 3**.

Paso 2 En el portal del FusionInsight Manager, elija **Cluster** > *Name of the desired cluster* > **Services** > **Hive** > **Instance** y haga clic en el HiveServer para el que se genera la alarma para ir a la página **Dashboard**. Haga clic en el menú desplegable en el área **Chart** y elija **Customize** > **CPU and Memory** y seleccione **HiveServer Memory Usage Statistics** y haga clic en **OK** y compruebe si la memoria no heap utilizada del servicio HiveServer alcanza el umbral (valor predeterminado: 95%) de la memoria no heap máxima especificada para HiveServer.

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 7**.

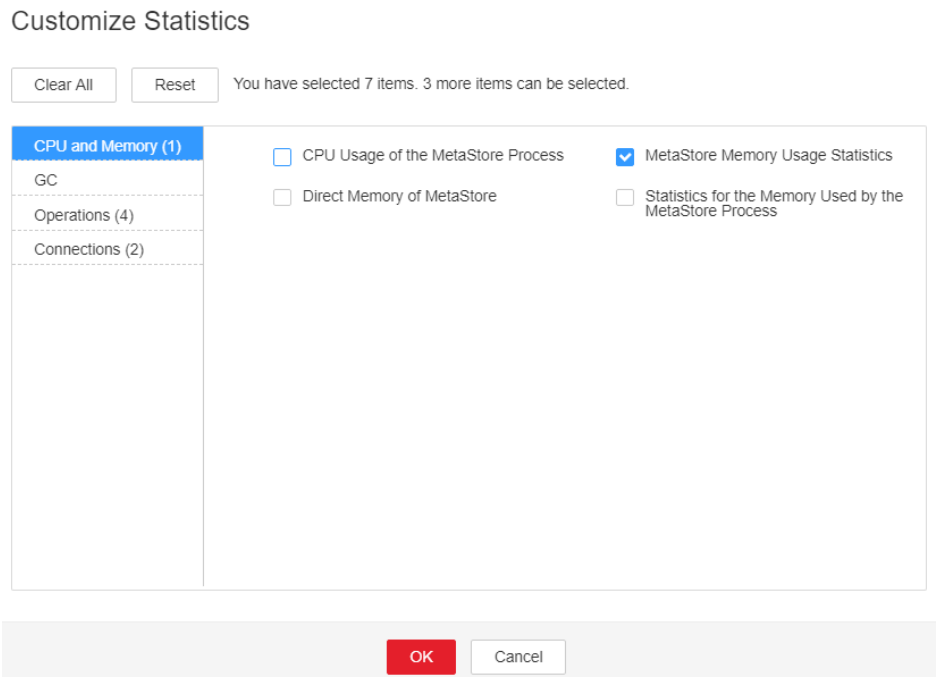
Figura 9-35 Estadísticas de uso de memoria de HiveServer



Paso 3 En el portal del FusionInsight Manager, elija **Cluster** > *Name of the desired cluster* > **Services** > **Hive** > **Instance** y haga clic en el MetaStore para el que se genera la alarma para ir a la página **Dashboard**. Haga clic en el menú desplegable en el área **Chart** y elija **Customize** > **CPU and Memory** y seleccione **MetaStore Memory Usage Statistics** y haga clic en **OK** y compruebe si la memoria no heap utilizada del servicio MetaStore alcanza el umbral (valor predeterminado: 95%) de la memoria no heap máxima especificada para MetaStore.

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 7**.

Figura 9-36 Estadísticas de uso de memoria de MetaStore



Paso 4 En el portal del FusionInsight Manager, seleccione **Cluster >** *Name of the desired cluster* > **Services** > **Hive** > **Configurations > All Configurations**. Elija **HiveServer/MetaStore** > **JVM**. Ajuste el valor de **-XX:MaxMetaspaceSize** en **HIVE_GC_OPTS/ METASTORE_GC_OPTS** como las siguientes reglas. Haga clic en **Save**.

NOTA

Sugerencias para la configuración de los parámetros de GC para el HiveServer:

- Se recomienda establecer el valor de **-XX:MaxMetaspaceSize** en 1/8 del valor de **-Xmx**. Por ejemplo, si **-Xmx** se establece en 2 GB, **-XX:**

  MaxMetaspaceSize está establecido en 256 MB. Si **-Xmx** se establece en 4 GB, **-XX:MaxMetaspaceSize** se establece en 512 MB.

Sugerencias para la configuración de los parámetros de GC para el MetaServer:

- Se recomienda establecer el valor de **-XX:MaxMetaspaceSize** en 1/8 del valor de **-Xmx**. Por ejemplo, si **-Xmx** se establece en 2 GB, **-XX:**

  MaxMetaspaceSize está establecido en 256 MB. Si **-Xmx** se establece en 4 GB, **-XX:MaxMetaspaceSize** se establece en 512 MB.

Paso 5 Haga clic en **More > Restart Service** para reiniciar el servicio.

Paso 6 Verifique si la alarma se ha borrado.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 7**.

Recopilar información de fallas.

Paso 7 En el portal del FusionInsight Manager, elija **O&M** > **Log > Download**.

Paso 8 Seleccione **Hive** en el clúster requerido en el **Service**.

Paso 9 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 10 Póngase en contacto con el y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.120 ALM-16009 El número de Map supera el umbral

Descripción

El sistema comprueba el número de Map de HQL cada 30 segundos. Esta alarma se genera si el número excede el umbral. De forma predeterminada, el valor de **Trigger Count** es **3** y el umbral es 5000.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
16009	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger Condition	Especifica el umbral que activa la alarma. Si el valor del indicador actual excede este umbral, se genera la alarma.

Impacto en el sistema

Si el número de maps de HQL ejecutados en Hive es excesivamente grande, la velocidad de ejecución de HQL es lenta y se ocupa un gran número de recursos.

Causas posibles

Las sentencias HQL no son las óptimas.

Procedimiento

Comprobar el número de map de HQL.

Paso 1 En el portal del FusionInsight Manager, elija **Cluster** >*Name of the desired cluster* > **Services** > **Hive** > **Resource**. Comprueba las sentencias HQL con el número excesivamente grande (5000 o más) de map de **HQL Map Count**.

Paso 2 Localice las sentencias HQL correspondientes, optimícelas y vuelva a ejecutarlas.

Paso 3 Verifique si la alarma se ha borrado.

- Si lo es, no se requiere ninguna otra acción.
- Si no es así, vaya a **Paso 4**.

Recopilar información de fallas.

Paso 4 En el FusionInsight Manager, elija **O&M** > **Log > Download**.

Paso 5 Seleccione **Hive** en el clúster requerido en el **Service**.

Paso 6 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 7 Póngase en contacto con el y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.121 ALM-16045 Se elimina el almacén de datos de Hive

Descripción

El sistema comprueba el almacén de datos de Hive cada 60 segundos. Esta alarma se genera cuando se elimina el almacén de datos de Hive.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
16045	Crítica	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

Se elimina el almacén de datos de Hive predeterminado. Como resultado, la creación de bases de datos o tablas en el almacén de datos predeterminado falla y los servicios se ven afectados.

Causas posibles

Hive comprueba periódicamente el estado del almacén de datos predeterminado y encuentra que se elimina el almacén de datos predeterminado.

Procedimiento

Comprobar el almacén de datos predeterminado de Hive.

Paso 1 Inicie sesión en el nodo donde se encuentra el cliente como usuario **root**.

Paso 2 Ejecute el siguiente comando para comprobar si el directorio **warehouse** existe en **hdfs://hacluster/user/**<*username*>**/.Trash/Current/**.

hdfs dfs -ls hdfs://hacluster/user/<*username*>**/.Trash/Current/**

Por ejemplo, si existe **user/hive/warehouse**:

```
host01 # hdfs dfs -ls hdfs://hacluster/user/test/.Trash/Current/
Found 1 items
drwx------   - test hadoop          0 2019-06-17 19:53 hdfs://hacluster/user/
test/.Trash/Current/user
```

- En caso afirmativo, vaya a **Paso 3**.
- Si no, vaya a **Paso 5**.

Paso 3 De forma predeterminada, existe un mecanismo de recuperación automática para el almacén de datos. Puede esperar 5 ~10s para comprobar si se restaura el almacén de datos predeterminado. Si el almacén de datos no se recupera, ejecute manualmente el siguiente comando para restaurar el almacén de datos.

hdfs dfs -mv hdfs://hacluster/user/<*username*>**/.Trash/Current/user/hive/warehouse / user/hive/warehouse**

Paso 4 Verifique si la alarma se ha borrado.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 5**.

Recopilar información de fallas.

Paso 5 Recopilar información relacionada en el directorio **.Trash/Current/** en el fondo del cliente.

Paso 6 Póngase en contacto con el y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.122 ALM-16046 Se modifica el permiso de almacén de datos de Hive

Descripción

El sistema comprueba el permiso del almacén de datos de Hive cada 60 segundos. Esta alarma se genera si se modifica el permiso.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
16046	Crítica	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

Si se modifica el permiso del almacén de datos predeterminado de Hive, se modifica el permiso para que los usuarios o grupos de usuarios creen bases de datos o tablas en el almacén de datos predeterminado.

Causas posibles

Hive comprueba periódicamente el estado del almacén de datos predeterminado y encuentra que se ha cambiado el permiso del almacén de datos predeterminado.

Procedimiento

Comprobar el permiso de almacén de datos predeterminado de Hive.

Paso 1 Inicie sesión en el nodo donde se encuentra el cliente como usuario **root**.

Paso 2 Ejecute el siguiente comando para ir al directorio de instalación del cliente HDFS:

cd *Client installation directory*

source bigdata_env

kinit *User who has the supergroup permission* (Omita este paso para un clúster común.)

Paso 3 Ejecute el siguiente comando para restaurar el permiso de almacén de datos predeterminado:

- Modo de seguridad: **hdfs dfs -chmod 770 hdfs://hacluster/user/hive/warehouse**
- Modo sin seguridad: **hdfs dfs -chmod 777 hdfs://hacluster/user/hive/warehouse**

Paso 4 Verifique si la alarma se ha borrado.

- Si lo es, no se requiere ninguna otra acción.
- Si no es así, vaya a **Paso 5**.

Recopilar información de fallas.

Paso 5 Recopilar información relacionada en el directorio **hdfs://hacluster/user/hive/warehouse** en el fondo del cliente.

Paso 6 Póngase en contacto con el y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.123 ALM-16047 HiveServer se ha dado de baja de ZooKeeper

Descripción

El sistema comprueba el servicio Hive cada 60 segundos. Esta alarma se genera cuando la información de registro de Hive en el ZooKeeper se pierde o Hive no puede conectarse a ZooKeeper.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
16047	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

Si no se puede leer la configuración de Hive desde ZooKeeper, HiveServer no estará disponible.

Causas posibles

- La red está desconectada.
- La instancia ZooKeeper es anormal.

Procedimiento

Reinicie las instancias relacionadas.

Paso 1 Inicie sesión en FusionInsight Manager. Elija **O&M** > **Alarm** > **Alarms**, haga clic en la lista desplegable de la fila que contiene la alarma y vea el rol y la dirección IP del nodo para el que se genera la alarma en **Location**.

Paso 2 Elija **Cluster** > *Name of the desired cluster* > **Services** > **Hive** > **Instance**, seleccione la instancia en la dirección IP para la que se genera la alarma y elija **More** > **Restart Instance**.

Paso 3 Espere 5 minutos y compruebe si la alarma está desactivada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 4**.

Recopilar información de fallas.

Paso 4 En FusionInsight Manager, seleccione **O&M**. En el panel de navegación de la izquierda, elija **Log** > **Download**.

Paso 5 Expanda la lista desplegable **Service** y seleccione **Hive** para el clúster de destino.

Paso 6 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 7 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

Información relacionada

Ninguna

9.124 ALM-16048 Ruta de biblioteca de Tez o Spark no existe

Descripción

El sistema comprueba las rutas de las bibliotecas Tez y Spark cada 180 segundos. Esta alarma se genera cuando la ruta de la biblioteca Tez o Spark no existe.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
16048	Grave	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.

Nombre	Significado
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

Las funciones de Hive on Tez y Hive on Spark se ven afectadas.

Causas posibles

La ruta de acceso de la biblioteca Tez o Spark se elimina del HDFS.

Procedimiento

Comprobar el almacén de datos predeterminado de Hive.

Paso 1 Inicie sesión en el nodo donde se encuentra el cliente como usuario **root**.

Paso 2 Ejecute el siguiente comando para comprobar si el directorio **tezlib** o **sparklib** existe en el director **hdfs://hacluster/user/{User name}/.Trash/Current/**:

hdfs dfs -ls hdfs://hacluster/user/<*username*>**/.Trash/Current/**

Por ejemplo, la siguiente información muestra que **/user/hive/tezlib//** y **/user/hive/sparklib//** existen.

```
host01 # hdfs dfs -ls hdfs://hacluster/user/test/.Trash/Current/
Found 1 items
drwx------   - test hadoop          0 2019-06-17 19:53 hdfs://hacluster/user/
test/.Trash/Current/user
```

- En caso afirmativo, vaya a **Paso 3**.
- Si no, vaya a **Paso 5**.

Paso 3 Ejecute el siguiente comando para restaurar **tezlib** y **sparklib**.

hdfs dfs -mv hdfs://hacluster/user/<*username*>**/.Trash/Current/user/hive/tezlib// tez.tar.gz /user/hive/tezlib//tez.tar.gz**

Paso 4 Verifique si la alarma se ha borrado.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 5**.

Recopilar información de fallas.

Paso 5 Recopile información relacionada en el directorio **.Trash/Current/** en el fondo del cliente.

Paso 6 Póngase en contacto con el y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.125 ALM-17003 Servicio Oozie no disponible

Descripción

El sistema comprueba el estado del servicio de Oozie cada 5 segundos. Esta alarma se genera cuando Oozie o un componente del que depende Oozie no puede proporcionar servicios correctamente.

Esta alarma se borra automáticamente cuando el servicio Oozie se recupera.

Atributo

ID de alarma	Gravedad de la alarma	Borrado automáticamente
17003	Crítica	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

Oozie no se puede utilizar para enviar trabajos.

Causas posibles

- El servicio DBService es anormal o los datos de Oozie almacenados en DBService están dañados.

- El servicio HDFS es anormal o los datos de Oozie almacenados en HDFS están dañados.
- El servicio Yarn es anormal.
- El proceso Nodeagent es anormal.

Procedimiento

Consultar el código de estado de salud de servicio Oozie.

Paso 1 En el portal del FusionInsight Manager, seleccione **Cluster** > *Name of the desired cluster* >**Services** > **Oozie**. Haga clic en **oozie** (cualquiera de ellos está bien) en el **oozie WebUI**. para ir a la WebUI de Oozie.

NOTA

De forma predeterminada, el usuario **admin** no tiene los permisos para gestionar otros componentes. Si la página no se puede abrir o el contenido mostrado está incompleto al acceder a la interfaz de usuario nativa de un componente debido a la falta de permisos, puede crear manualmente un usuario con los permisos para gestionar ese componente.

Paso 2 Agregue **/servicehealth** a la URL en el cuadro de direcciones del navegador y vuelva a acceder. El valor de **statusCode** es el código de estado de servicio actual de Oozie.

Por ejemplo, visite **https://10.10.0.117:20026/Oozie/oozie/130/oozie/servicehealth**. El resultado es el siguiente:

```
{"beans":[{"name":"serviceStatus","statusCode":0}]}
```

Si el código de estado de salud no se puede mostrar o el navegador no responde, el servicio puede no estar disponible debido a una falla en el proceso de Oozie. Vea **Paso 13** para rectificar la falla.

Paso 3 Realice las operaciones basadas en el código de error. Para obtener más información, consulte **Tabla 9-4**.

Tabla 9-4 Código de estado de salud del servicio Oozie

Código de estado	Descripción	Causa del error	Solución
0	El servicio está funcionando correctamente.	Ninguna	Ninguna
18002	El servicio DBService es anormal.	Oozie no puede conectarse a DBService o los datos almacenados en DBService están dañados.	Consulte **Paso 4**.
18003	El servicio HDFS es anormal.	Oozie no puede conectarse a HDFS o los datos almacenados en HDFS están dañados.	Consulte **Paso 7**.

Código de estado	Descripción	Causa del error	Solución
18005	El MapReduce service es anormal.	El servicio Yarn es anormal.	Consulte **Paso 11**.

Comprobar el servicio DBService.

Paso 4 En el portal FusionInsight Manager, elija **Cluster** > *Name of the desired cluster* > **Services** y compruebe si el servicio DBService se está ejecutando correctamente.

- En caso afirmativo, vaya a **Paso 6**.
- Si no, vaya a **Paso 5**.

Paso 5 Resuelva el problema de DBService basándose en la ayuda de alarma y compruebe si la alarma de Oozie está borrada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 18**.

Paso 6 Inicie sesión en la base de datos de Oozie para comprobar si los datos están completos.

1. Inicie sesión en el nodo DBService activo como usuario **root**.

   En la página FusionInsight Manager, elija **Cluster** > *Name of the desired cluster* > **Services** > **DBService > Instance** para ver la dirección IP del nodo DBservice activo.
2. Ejecute el siguiente comando para iniciar sesión en la base de datos de Oozie:

   su - omm

   source ${BIGDATA_HOME}/FusionInsight_BASE_/install/FusionInsight-dbservice-2.7.0/.dbservice_profile

   gsql -U *Username* **-W** *Oozie database password* **-p 20051 -d** *Database name*
3. Una vez que el inicio de sesión se haya realizado correctamente, introduzca **\d** para comprobar si hay 15 tablas de datos.

   El servicio Oozie tiene 15 tablas de datos por defecto. Si se eliminan estas tablas de datos o se modifica la estructura de la tabla, es posible que el servicio Oozie no esté disponible. Póngase en contacto con el para realizar una copia de respaldo de los datos y realizar la restauración.

Comprobar el servicio HDFS.

Paso 7 En el portal del FusionInsight Manager, elija **Cluster** > *Name of the desired cluster* > **Services** y compruebe si el servicio HDFS se está ejecutando correctamente.

- En caso afirmativo, vaya a **Paso 9**.
- Si no, vaya a **Paso 8**.

Paso 8 Resuelva el problema de HDFS basándose en la ayuda de alarma y compruebe si la alarma Oozie está borrada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 18**.

Paso 9 Inicie sesión en HDFS para comprobar si la estructura de directorios de archivos Oozie está completa.

1. Descargue e instale un cliente HDFS..

2. Inicie sesión en el nodo cliente como usuario **root** y ejecute los siguientes comandos para comprobar si **/user/oozie/share** existe.

   Si el clúster utiliza el modo de seguridad, realice la autenticación de seguridad.

   kinit admin

   hdfs dfs -ls /user/oozie/share

- En caso afirmativo, vaya a **Paso 18**.
- Si no, vaya a **Paso 10**.

Paso 10 En el directorio de instalación del cliente Oozie, cargue manualmente el directorio compartido a **/user/oozie** en HDFS y compruebe si la alarma está borrada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 18**.

Comprobar el servicio Yarn y MapReduce.

Paso 11 En el portal del FusionInsight Manager, elija **Cluster >** *Name of the desired cluster* > **Services** y compruebe si los servicios de Yarn y MapReduce se están ejecutando correctamente.

- En caso afirmativo, vaya a **Paso 18**.
- Si no, vaya a **Paso 12**.

Paso 12 Resuelva el problema de Yarn y MapReduce basándose en la ayuda de alarma y compruebe si la alarma Oozie está borrada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 18**.

Comprobar el proceso Oozie.

Paso 13 Inicie sesión en cada nodo de Oozie como usuario **root**.

Paso 14 Ejecute el comando **ps -ef | grep oozie** para comprobar si el proceso Oozie existe.

- En caso afirmativo, vaya a **Paso 15**.
- Si no, vaya a **Paso 18**.

Paso 15 Recopilar información de fallas en **prestartDetail.log**, **oozie.log**, y **catalina.out** en el directorio de registro de Oozie **/var/log/Bigdata/oozie**. Si la alarma no es causada por un mal funcionamiento manual, vaya a **Paso 16**.

Comprobar el proceso Nodeagent.

Paso 16 Inicie sesión en cada nodo de Oozie como usuario **root**. Ejecute el comando **ps -ef | grep nodeagent** para comprobar si existe el proceso Nodeagent.

- En caso afirmativo, vaya a **Paso 17**.
- Si no, vaya a **Paso 18**.

Paso 17 Ejecute el comando **kill -9** *The process ID of nodeagent*, espere 10 minutos y compruebe si la alarma está desactivada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 18**.

Paso 18 Póngase en contacto con el y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.126 ALM-17004 El uso de memoria heap de Oozie supera el umbral

Descripción

El sistema comprueba el uso de memoria heap del servicio Oozie cada 60 segundos. La alarma se genera cuando el uso de memoria heap de una instancia de metadatos supera el umbral (95% de la memoria máxima). La alarma se borra cuando el uso de memoria heap es menor que el umbral.

Atributo

ID de alarma	Gravedad de la alarma	Borrado automáticamente
17004	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger Condition	Especifica el umbral que activa la alarma. Si el valor del indicador actual excede este umbral, se genera la alarma.

Impacto en el sistema

El desbordamiento de la memoria heap puede provocar una avería del servicio.

Causas posibles

La memoria heap de la instancia de Oozie está sobreutilizada o la memoria heap se asigna de forma inapropiada.

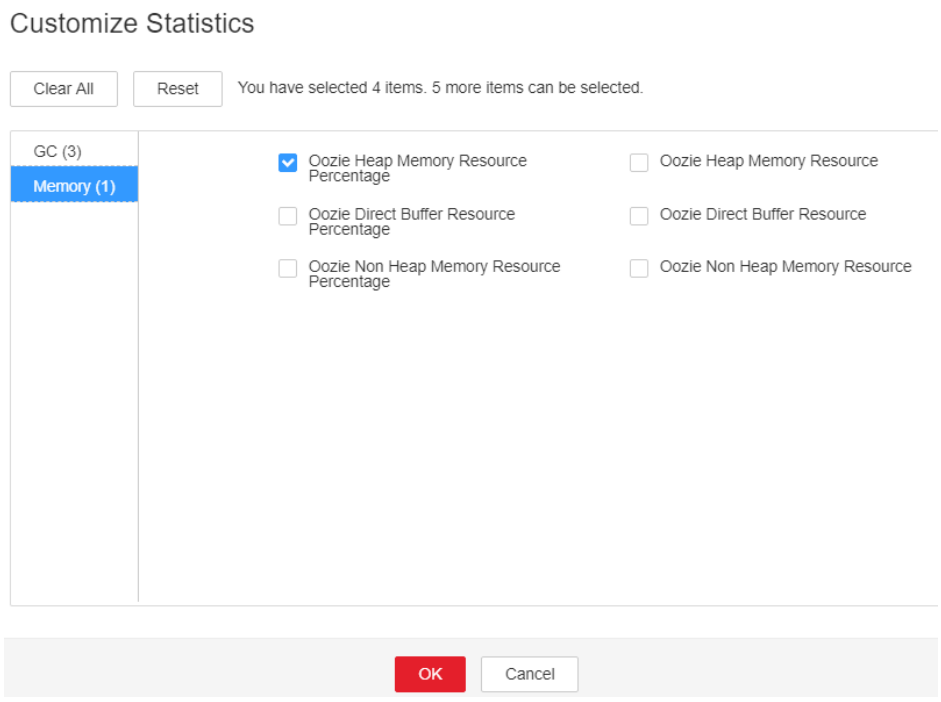
Procedimiento

Comprobar el uso de memoria heap.

Paso 1 En el portal del FusionInsight Manager, elija **O&M > Alarm > Alarms** > **Oozie Heap Memory Usage Exceeds the Threshold** > **Location**. Compruebe la dirección IP de la instancia involucrada en esta alarma.

Paso 2 En el portal del FusionInsight Manager, seleccione **Cluster >** *Name of the desired cluster* > **Services** > **Oozie** > **Instance**. Haga clic en la instancia para la que se genera la alarma para ir a la página de la instancia. Haga clic en el menú desplegable en el área del gráfico y elija **Customize** > **Memory** > **Oozie Heap Memory Resource Percentage**. Haga clic en **OK**.

Figura 9-37 Porcentaje de recursos de memoria heap de Oozie



Paso 3 Comprobar si la memoria heap usada de Oozie alcanza el umbral (el valor predeterminado es el 95% de la memoria heap máxima) especificado para Oozie.

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 6**.

Paso 4 En el portal del FusionInsight Manager, seleccione **Cluster >** *Name of the desired cluster* > **Services** > **Oozie** > **Configurations > All Configurations**. Establezca Buscar **GC_OPTS** en el cuadro de búsqueda. Aumente el valor de **-Xmx** según sea necesario y haga clic en **Save** > **OK**.

NOTA

Sugerencias sobre la configuración de parámetros de GC para Oozie:

Se recomienda establecer **-Xms** y **-Xmx** en el mismo valor para evitar un impacto adverso en el rendimiento cuando JVM ajusta dinámicamente el tamaño de la memoria heap.

Paso 5 Reinicie los servicios o instancias afectados y compruebe si la alarma está desactivada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 6**.

Recopilar información de fallas.

Paso 6 En el portal del FusionInsight Manager, seleccione **O&M** > **Log** > **Download**.

Paso 7 Seleccione **Oozie** en el clúster requerido en el **Service**.

Paso 8 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 9 Póngase en contacto con el y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.127 ALM-17005 El uso de memoria no heap de Oozie supera el umbral

Descripción

El sistema comprueba el uso de memoria no heap de Oozie cada 30 segundos. Esta alarma se notifica si el uso de memoria no heap de Oozie excede el umbral (80%). Esta alarma se borra si el uso de memoria no heap es menor que el umbral.

Atributo

ID de alarma	Gravedad de la alarma	Borrado automático
17005	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger Condition	Especifica el umbral para activar la alarma.

Impacto en el sistema

El desbordamiento de la memoria no heap puede provocar una falla en el servicio.

Causas posibles

La memoria no heap de la instancia de Oozie es sobreutilizada o la memoria no heap es asignada inapropiadamente.

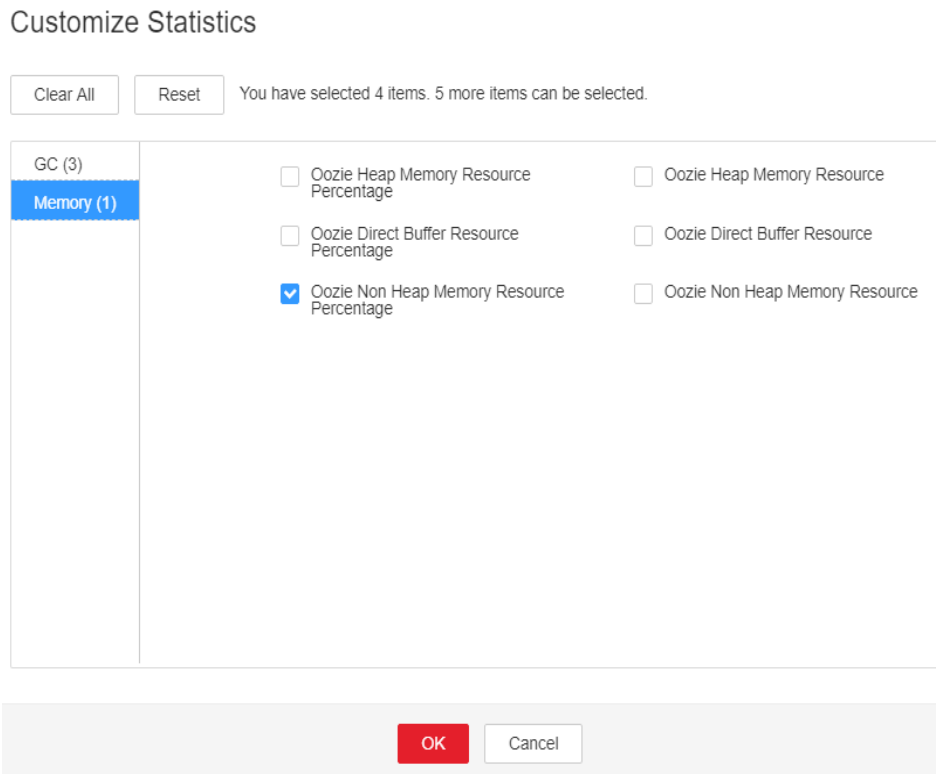
Procedimiento

Verifique el uso de memoria no heap.

Paso 1 En FusionInsight Manager, elija **O&M** > **Alarm** > **Alarms** > **Oozie Non Heap Memory Usage Exceeds the Threshold**. En la página mostrada, compruebe la información de ubicación de la alarma. Compruebe el nombre del host de instancia para el que se genera la alarma.

Paso 2 En el Administrador de FusionInsight, elija **Cluster** > *Name of the target cluster* > **Services** > **Oozie** y haga clic en la pestaña **Instance**. En la página mostrada, seleccione el rol correspondiente al nombre de host para el que se genera la alarma y seleccione **Customize** en la lista desplegable en la esquina superior derecha del área del gráfico. Elija **Memory** y seleccione **Oozie Non Heap Memory Resource Percentage**. Haga clic en **OK**.

Figura 9-38 Uso de memoria no heap de Oozie



Paso 3 Compruebe si la memoria no heap utilizada por Oozie alcanza el umbral (80% de la memoria no heap máxima por defecto).

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 6**.

Paso 4 En el Administrador de FusionInsight, elija **Cluster** > *Name of the target cluster* > **Services** > **Oozie** y haga clic en **Configurations** y, a continuación, en **All Configurations**. En la página mostrada, busque el parámetro **GC_OPTS** en el cuadro de búsqueda y compruebe si contiene **-XX: MaxMetaspaceSize**. En caso afirmativo, aumente el valor de **-XX: MaxMetaspaceSize** según los requisitos del sitio. Si no, agregue manualmente **-XX: MaxMetaspaceSize** y establezca su valor en 1/8 del valor de **-Xmx**. Haga clic en **Save** y, a continuación, haga clic en **OK**

NOTA

JDK1.8 no admite el parámetro **MaxPermSize**.

Sugerencias sobre la configuración de parámetros de GC para Oozie:

Establezca el valor de **-XX:MaxMetaspaceSize** en 1/8 del valor de **-Xmx**. Por ejemplo, si **-Xmx** se establece en 2 GB, **-XX:MaxMetaspaceSize** se establece en 256 MB. Si **-Xmx** se establece en 4 GB, **-XX:MaxMetaspaceSize** se establece en 512 MB.

Paso 5 Reinicie los servicios o instancias afectados y compruebe si la alarma está desactivada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 6**.

Recopilar información de fallas.

Paso 6 En FusionInsight Manager, seleccione **O&M**. En el panel de navegación de la izquierda, elija **Log** > **Download**.

Paso 7 Expanda la lista desplegable **Service** y seleccione **Oozie** para el clúster de destino.

Paso 8 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 9 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

Información relacionada

Ninguna

9.128 ALM-17006 El uso de memoria directa de Oozie supera el umbral

Descripción

El sistema comprueba el uso memoria directa del servicio Oozie cada 30 segundos. La alarma se genera cuando el uso de memoria directa de una instancia de Oozie excede el umbral (80% de la memoria máxima). La alarma se borra cuando el uso directo de memoria de Oozie es menor o igual que el umbral.

Atributo

ID de alarma	Gravedad de la alarma	Borrado automáticamente
17006	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Nombre	Significado
Trigger Condition	Especifica el umbral que activa la alarma. Si el valor del indicador actual excede este umbral, se genera la alarma.

Impacto en el sistema

El desbordamiento de la memoria directa puede provocar una avería del servicio.

Causas posibles

La memoria directa de la instancia de Oozie es sobreutilizada o la memoria directa es asignada inapropiadamente.

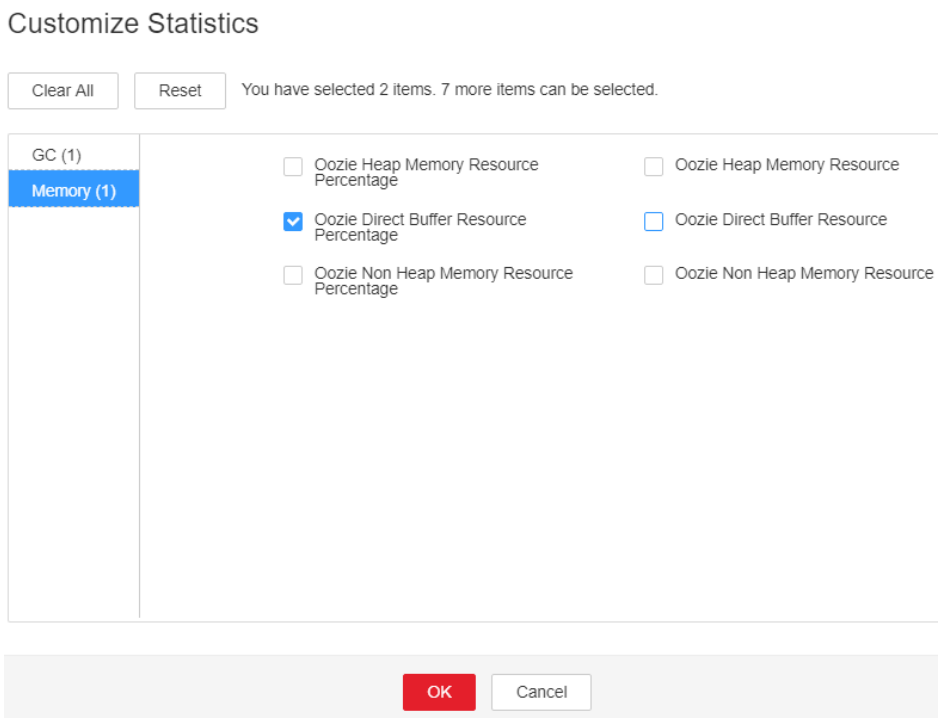
Procedimiento

Comprobar el uso de memoria directa.

Paso 1 En el portal del FusionInsight Manager, elija **O&M** > **Alarm** > **Alarms** > **Oozie Direct Memory Usage Exceeds the Threshold** > **Location**. Compruebe la dirección IP de la instancia involucrada en esta alarma.

Paso 2 En el portal del FusionInsight Manager, seleccione **Cluster >** *Name of the desired cluster* > **Services** > **Oozie** > **Instance**. Haga clic en la instancia para la que se genera la alarma para ir a la página de la instancia. Haga clic en el menú desplegable en el área del gráfico y elija **Customize** > **Memory** > **Oozie Direct Buffer Resource Percentage**. Haga clic en **OK**.

Figura 9-39 Porcentaje de recursos de búfer directo de Oozie



Paso 3 Comprobar si la memoria directa utilizada de Oozie alcanza el umbral (el valor predeterminado es 80% de la memoria directa máxima) especificado para Oozie.

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 6**.

Paso 4 En el portal del FusionInsight Manager, seleccione **Cluster >** *Name of the desired cluster* > **Services** > **Oozie** > **Configurations**. Haga clic en **All Configurations**. Busque **GC_OPTS** en el cuadro de búsqueda. Aumente el valor de **-XX:MaxDirectMemorySize** según sea necesario y haga clic en **Save**. Haga clic en **OK**.

NOTA

Sugerencias sobre la configuración de parámetros de GC para Oozie:

Se recomienda establecer el valor de **-XX:MaxDirectMemorySize** en 1/4 del valor de **-Xmx**. Por ejemplo, si **-Xmx** se establece en 4 GB, **-XX:MaxDirectMemorySize** se establece en 1024 MB. Si **-Xmx** se establece en 2 GB, **-XX:MaxDirectMemorySize** se establece en 512 MB. Se recomienda que el valor de **-XX:MaxDirectMemorySize** sea mayor o igual a 512 MB.

Paso 5 Reinicie los servicios o instancias afectados y compruebe si la alarma está desactivada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 6**.

Recopilar información de fallas.

Paso 6 En el portal del FusionInsight Manager, seleccione **O&M** > **Log** > **Download**.

Paso 7 Seleccione **Oozie** en el clúster requerido en la lista desplegable **Service**.

Paso 8 Haga clic en  en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 9 Póngase en contacto con el y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.129 ALM-17007 El tiempo de recolección de basura (GC) del proceso Oozie supera el umbral

Descripción

El sistema comprueba el tiempo de GC del proceso Oozie cada 60 segundos. La alarma se genera cuando el tiempo de GC del proceso Oozie supera el umbral (valor predeterminado **12 seconds**). La alarma se borra cuando el tiempo GC es menor que el umbral.

Atributo

ID de alarma	Gravedad de la alarma	Borrado automáticamente
17007	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger Condition	Especifica el umbral que activa la alarma. Si el valor del indicador actual excede este umbral, se genera la alarma.

Impacto en el sistema

Oozie responde lentamente cuando se utiliza para enviar tareas.

Causas posibles

La memoria heap de la instancia de Oozie está sobreutilizada o la memoria heap se asigna de forma inapropiada.

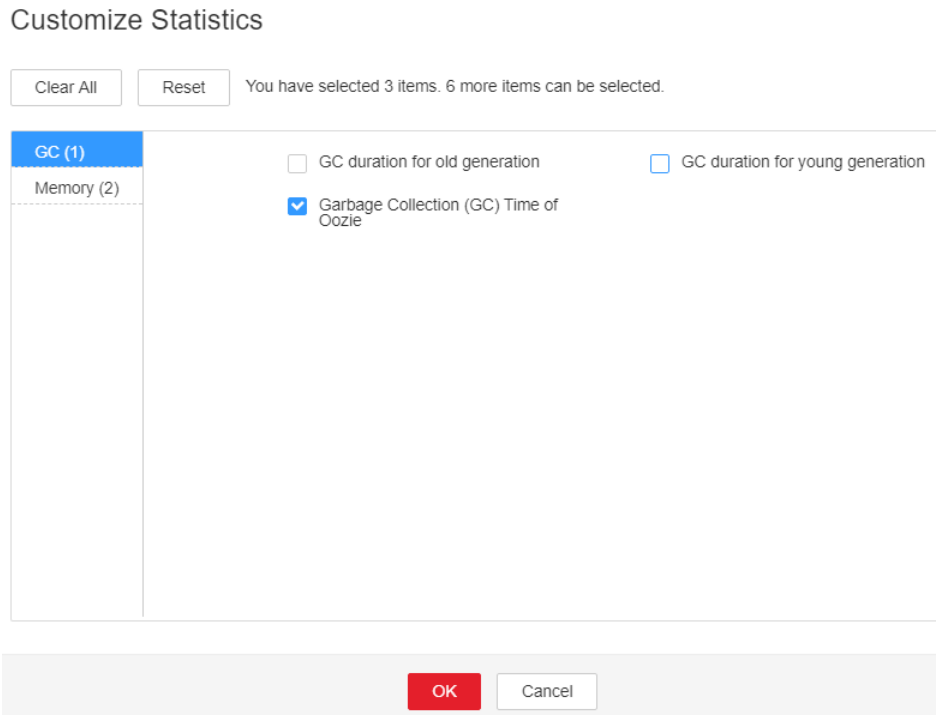
Procedimiento

Comprobar el tiempo de GC.

Paso 1 En el portal del administrador FusionInsight, elija **O&M** > **Alarm** > **Alarms** > **Garbage Collection (GC) Time of the Oozie Process Exceeds the Threshold** > **Location**. Compruebe la dirección IP de la instancia involucrada en esta alarma.

Paso 2 En el portal del FusionInsight Manager, seleccione **Cluster >** *Name of the desired cluster* > **Services** > **Oozie** > **Instance**. Haga clic en la instancia para la que se genera la alarma para ir a la página de la instancia. Haga clic en el menú desplegable en el área del gráfico y elija **Customize** > **GC** > **Garbage Collection (GC) Time of Oozie**. Haga clic en **OK**.

Figura 9-40 Tiempo de recolección de basura (GC) de Oozie



Paso 3 Compruebe si el tiempo GC del proceso Oozie excede cada segundo el umbral (valor predeterminado **12 seconds**).

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 6**.

Paso 4 En el portal del FusionInsight Manager, seleccione **Cluster >** *Name of the desired cluster* > **Services** > **Oozie** > **Configurations**. Haga clic en **All Configurations**. Busque **GC_OPTS** en el cuadro de búsqueda. Aumente el valor de **-Xmx** según sea necesario y haga clic en **Save**. Haga clic en **OK**.

NOTA

Sugerencias sobre la configuración de parámetros de GC para Oozie:

Se recomienda establecer **-Xms** y **-Xmx** en el mismo valor para evitar un impacto adverso en el rendimiento cuando JVM ajusta dinámicamente el tamaño de la memoria heap.

Paso 5 Reinicie los servicios o instancias afectados y compruebe si la alarma está desactivada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 6**.

Recopilar información de fallas.

Paso 6 En el portal del FusionInsight Manager, seleccione **O&M** > **Log** > **Download**.

Paso 7 Seleccione **Oozie** en el clúster requerido en la lista desplegable **Service**.

Paso 8 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 9 Póngase en contacto con el y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.130 ALM-18000 Servicio de Yarn no disponible

Descripción

Esta alarma se genera cuando el servicio Yarn no está disponible. El módulo de alarma comprueba el estado del servicio de Yarn cada 60 segundos.

La alarma se borra cuando se recupera el servicio Yarn.

Atributo

ID de alarma	Gravedad de la alarma	Borrado automáticamente
18000	Crítica	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceNam	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

El clúster no puede proporcionar servicios de Yarn. Los usuarios no pueden ejecutar aplicaciones nuevas. Las aplicaciones enviadas no se pueden ejecutar.

Causas posibles

- El servicio ZooKeeper es anormal.
- El servicio HDFS es anormal.
- No hay ninguna instancia de ResourceManager activa en el clúster de Yarn.
- Todos los NodeManagers en el clúster de Yarn son anormales.

Procedimiento

Verificar el estado del servicio de ZooKeeper.

Paso 1 En el FusionInsight Manager, compruebe si la lista de alarmas contiene **ALM-13000 Servicio ZooKeeper no disponible**.

- En caso afirmativo, vaya a **Paso 2**.
- Si no, vaya a **Paso 3**.

Paso 2 Rectifique la falla siguiendo los pasos en **ALM-13000 Servicio ZooKeeper Service no disponible** y compruebe si la alarma está borrada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 3**.

Comprobar el estado de servicio HDFS.

Paso 3 En el FusionInsight Manager, compruebe si la lista de alarmas contiene las alarmas HDFS.

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 5**.

Paso 4 Elija **O&M > Alarm > Alarms** y maneje las alarmas HDFS en función de la ayuda de alarma y compruebe si la alarma de Yarn está desactivada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 5**.

Verificar el estado de ResourceManager en el clúster de Yarn.

Paso 5 En el portal del FusionInsight Manager, elija **Cluster >** *Name of the desired cluster* **> Services** > **Yarn**.

Paso 6 En **Dashboard**, compruebe si hay una instancia de ResourceManager activa en el clúster de Yarn.

- En caso afirmativo, vaya a **Paso 7**.
- Si no, vaya a **Paso 10**.

Comprobar el estado del nodo NodeManager en el clúster de Yarn.

Paso 7 En el portal del FusionInsight Manager, elija **Cluster >** *Name of the desired cluster* **> Services** > **Yarn** > **Instance**.

Paso 8 Consulte el **Running Status** de NodeManager y compruebe si hay nodos en mal estado.

- En caso afirmativo, vaya a **Paso 9**.
- Si no, vaya a **Paso 10**.

Paso 9 Rectifique la falla siguiendo los pasos de **ALM-18002 El latido de corazón de NodeManager perdido** y **ALM-18003 NodeManager en mal estado**. Después de rectificar la falla, compruebe si la alarma de Yarn está desactivada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 10**.

Recopilar información de fallas.

Paso 10 En el portal del FusionInsight Manager del clúster activo, seleccione **O&M** > **Log** > **Download**.

Paso 11 Seleccione **Yarn** en el clúster requerido en el **Service**.

Paso 12 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 13 Póngase en contacto con el y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.131 ALM-18002 Latidos del corazón de NodeManager perdidos

Descripción

El sistema comprueba el número de nodos de NodeManager perdidos cada 30 segundos, y compara el número con el umbral. El indicador Número de nodos perdidos tiene un umbral predeterminado. La alarma se genera cuando el valor de Número de Nodos Perdidos excede el umbral.

Para cambiar el umbral, en FusionInsight Manager, elija **Cluster** > *Name of the desired cluster* > **Services** > **Yarn**. En la página mostrada, elija **Configurations** > **All Configurations** y cambie el valor de **yarn.nodemanager.lost.alarm.threshold**. No es necesario reiniciar Yarn para que el cambio surta efecto.

El umbral predeterminado es 0. La alarma se genera cuando el número de nodos perdidos excede el umbral, y se borra cuando el número de nodos perdidos es menor que el umbral.

Atributo

ID de alarma	Gravedad de la alarma	Borrado automáticamente
18002	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Lost Host	Especifica la lista de hosts con nodos perdidos.

Impacto en el sistema

- El nodo NodeManager perdido no puede proporcionar el servicio Yarn.
- El número de contenedores disminuye, por lo que el rendimiento del clúster se deteriora.

Causas posibles

- NodeManager se elimina por la fuerza sin darse de baja.
- Todas las instancias NodeManager se detienen o el proceso NodeManager es defectuoso.
- El host donde reside el nodo NodeManager es defectuoso.
- La red entre el NodeManager y el ResourceManager está desconectada u ocupada.

Procedimiento

Comprobar el estado de NodeManager.

Paso 1 En el FusionInsight Manager, elija **O&M** >**Alarm > Alarms**. Haga clic en ⌄ antes de la alarma y obtenga los nodos perdidos de **Additional Information**.

Paso 2 Compruebe si los nodos perdidos son hosts que se han eliminado manualmente sin darse de baja.

- En caso afirmativo, vaya a **Paso 3**.
- Si no, vaya a **Paso 5**.

Paso 3 Después de la configuración, elija **Cluster** > *Name of the desired cluster* > **Services** > **Yarn**. En la página mostrada, elija **Configurations** > **All Configurations**. Busque **yarn.nodemanager.lost.alarm.threshold** y cambie su valor por el número de hosts que no están fuera de servicio y que se eliminan de forma proactiva. Después de la configuración, compruebe si la alarma está desactivada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 4**.

Paso 4 Borre la alarma manualmente. Tenga en cuenta que el desmantelamiento debe realizarse antes de eliminar los hosts.

Paso 5 En el portal de FusionInsight Manager, elija **Cluster > Hosts** y compruebe si los nodos obtenidos en **Paso 1** están sanos.

- En caso afirmativo, vaya a **Paso 7**.
- Si no, vaya a **Paso 6**.

Paso 6 Rectifique la falla del nodo basado en el **ALM-12006 Falla de nodo** y verifique si la alarma está borrada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 7**.

Comprobar el estado de proceso.

Paso 7 En el FusionInsight Manager, seleccione **Cluster** > *Name of the desired cluster* **> Services** > **Yarn** > **Instance** y compruebe si NodeManager hay instancias cuyo estado no es **Good**.

- En caso afirmativo, vaya a **Paso 10**.
- Si no, vaya a **Paso 8**.

Paso 8 Compruebe si se ha eliminado la instancia NodeManager.

- En caso afirmativo, vaya a **Paso 9**.
- Si no, vaya a **Paso 11**.

Paso 9 Reinicie las instancias de ResourceManager activa y en espera y compruebe si la alarma está desactivada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 13**.

Comprobar el estado de instancia.

Paso 10 Seleccione instancias de NodeManager cuyo estado de ejecución no sea **Normal** y reinícielas. Verifique si la alarma se ha borrado.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 11**.

Comprobar el estado de red.

Paso 11 Inicie sesión en el nodo de gestión, **haga ping** a la dirección IP del nodo de NodeManager perdido para comprobar si la red está desconectada u ocupada.

- En caso afirmativo, vaya a **Paso 12**.
- Si no, vaya a **Paso 13**.

Paso 12 Rectifique la red y compruebe si la alarma está borrada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 13**.

Recopilar información de fallas.

Paso 13 En el FusionInsight Manager del clúster activo, elija **O&M** > **Log > Download**.

Paso 14 Seleccione **Yarn** en el clúster requerido en el **Service**.

Paso 15 Haga clic en  en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 16 Póngase en contacto con el y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.132 ALM-18003 NodeManager en mal estado

Descripción

El sistema comprueba el número de nodos de NodeManager no saludables cada 30 segundos y compara el número con el umbral. El indicador de nodos no saludables tiene un umbral predeterminado. Esta alarma se genera cuando el valor del indicador de nodos no saludables excede el umbral.

Para cambiar el umbral, en FusionInsight Manager, elija **Cluster** > *Name of the desired cluster* > **Services** > **Yarn**. En la página mostrada, elija **Configurations** > **All Configurations**, y cambie el valor de **yarn.nodemanager.unhealthy.alarm.threshold**. No es necesario reiniciar Yarn para que el cambio surta efecto.

El umbral predeterminado es 0. La alarma se genera cuando el número de nodos no sanos excede el umbral, y se borra cuando el número de nodos no sanos es menor que el umbral.

Atributo

ID de alarma	Gravedad de la alarma	Borrado automáticamente
18003	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Unhealthy Host	Especifica la lista de hosts con nodos no saludables.

Impacto en el sistema

- El nodo NodeManager defectuoso no puede proporcionar el servicio Yarn.
- El número de contenedores disminuye, por lo que el rendimiento del clúster se deteriora.

Causas posibles

- El espacio en disco duro del host donde reside el nodo de NodeManager es insuficiente.
- El usuario **omm** no tiene permiso para acceder a un directorio local en el nodo NodeManager.

Procedimiento

Comprobar el espacio en el disco duro del host.

Paso 1 En el FusionInsight Manager, elija **O&M** >**Alarm > Alarms**. Haga clic en antes de la alarma y obtenga nodos no saludables de **Additional Information**.

Paso 2 Elija **Cluster** > *Name of the desired cluster* **> Services > Yarn** > **Instance**, seleccione la instancia de NodeManager correspondiente al host, elija **Instance Configurations > All Configurations** y vea los discos correspondientes al **yarn.nodemanager.local-dirs** y **yarn.nodemanager.log-dirs**.

Paso 3 Elija **O&M > Alarm > Alarms**. En la lista de alarmas, compruebe si el disco relacionado tiene la alarma **ALM-12017 Capacidad de disco insuficiente**.

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 5**.

Paso 4 Rectifique la falla del disco basado en **ALM-12017 Capacidad de disco insuficiente** y compruebe si la alarma está borrada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 7**.

Paso 5 Elija **Hosts** > *Name of the desired host.* En la página **Dashboard**, compruebe el uso del disco de la partición correspondiente. Compruebe si el porcentaje del espacio usado del disco montado excede el valor de **yarn.nodemanager.disk-health-checker.max-disk-utilization-per-disk-percentage**

- En caso afirmativo, vaya a **Paso 6**.
- Si no, vaya a **Paso 7**.

Paso 6 Reduzca el uso del disco a menos que el valor de **yarn.nodemanager.disk-health-checker.max-disk-utilization-per-disk-percentage**, espere de 10 a 20 minutos y compruebe si la alarma está borrada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 7**.

Verificar el permiso de acceso del directorio local en cada nodo de NodeManager.

Paso 7 Obtenga el directorio NodeManager visto en **Paso 2**, inicie sesión en cada nodo de NodeManager como usuario **root** y vaya al directorio obtenido.

Paso 8 Ejecute el comando **ll** para comprobar si el permiso de las carpetas **localdir** y **containerlogs** es **755** y si **User:Group** es **omm:ficommon**.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 9**.

Paso 9 Ejecute el siguiente comando para establecer el permiso para **755** y **User:Group** para **omm:ficommon**:

chmod 755 <*folder_name*>

chown omm:ficommon <*folder_name*>

Paso 10 Espere de 10 a 20 minutos y compruebe si la alarma está desactivada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 11**.

Recopilar información de fallas.

Paso 11 En el FusionInsight Manager del clúster activo, elija **O&M** > **Log > Download**.

Paso 12 Seleccione **Yarn** en el clúster requerido en el **Service**.

Paso 13 Haga clic en  en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 14 Póngase en contacto con el y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.133 ALM-18008 El uso de memoria heap de ResourceManager supera el umbral

Descripción

El sistema comprueba el uso de memoria heap de ResourceManager de Yarn cada 30 segundos y compara el uso real con el umbral. La alarma se genera cuando el uso de memoria de heap de Yarn ResourceManager excede el umbral (95% de la memoria máxima por defecto).

Los usuarios pueden elegir **O&M > Alarm > Thresholds** > *Name of the desired cluster* > **Yarn** para cambiar el umbral.

Cuando el **Trigger Count** es 1, esta alarma se borra cuando el uso de memoria heap de Yarn de ResourceManager es menor o igual que el umbral. Cuando el **Trigger Count** es mayor que 1, esta alarma se borra cuando el uso de memoria heap de Yarn ResourceManager es menor o igual al 95% del umbral.

Atributo

ID de alarma	Gravedad de la alarma	Borrado automáticamente
18008	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el nombre del servicio para el que se genera la alarma.
RoleName	Especifica el nombre del rol para el que se genera la alarma.
HostName	Especifica el objeto (ID de host) para el que se genera la alarma.
Trigger Condition	Especifica el umbral que activa la alarma. Si el valor del indicador actual excede este umbral, se genera la alarma.

Impacto en el sistema

Cuando el uso de memoria heap de Yarn ResourceManager es demasiado alto, el rendimiento del envío y la operación de la tarea de Yarn se ve afectado. Además, puede producirse un desbordamiento de memoria para que el servicio Yarn no esté disponible.

Causas posibles

La memoria heap de la instancia de Yarn ResourceManager en el nodo se utiliza en exceso o la memoria heap se asigna de forma inapropiada. Como resultado, el uso excede el umbral.

Procedimiento

Comprobar el uso de la memoria heap.

Paso 1 En el portal del FusionInsight Manager, elija **O&M > Alarm > Alarms** > **Heap Memory Usage of Yarn ResourceManager Exceeds the Threshold** > **Location**. Compruebe el HostName de la instancia para la que se genera la alarma.

Paso 2 En el portal de FusionInsight Manager, elija **Cluster** > *Name of the desired cluster* **> Services** > **Yarn** > **Instance** > **ResourceManager** (Indica el nombre de host de la instancia para la que se genera la alarma)**.** Haz clic en el menú desplegable en la esquina superior derecha de **Chart** y elige **Customize** > **ResourceManager > Percentage of Used Memory of the ResourceManager**. Compruebe el uso de la memoria heap.

Figura 9-41 Porcentaje de memoria usada del ResourceManager

Paso 3 Compruebe si la memoria heap utilizada de ResourceManager alcanza el 95% de la memoria de pila máxima especificada para ResourceManager.

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 6**.

Paso 4 En el portal del FusionInsight Manager, seleccione **Cluster** > *Name of the desired cluster* **> Services** > **Yarn** > **Configurations** > **All Configurations** > **ResourceManager** > **System**. Aumente el valor del parámetro **GC_OPTS** según sea necesario, haga clic en **Save**. Reinicie la instancia de rol.

NOTA

La asignación entre el número de instancias de NodeManager en un clúster y el tamaño de memoria de ResourceManager es la siguiente:

- Si el número de instancias NodeManager en el clúster alcanza 100, los parámetros JVM recomendados de la instancia de ResourceManager son los siguientes: -Xms4G -Xmx4G -XX:NewSize=512M -XX:MaxNewSize=1G
- Si el número de instancias de NodeManager en el clúster alcanza 200, los parámetros JVM recomendados de la instancia de ResourceManager son los siguientes: -Xms6G -Xmx6G -XX:NewSize=512M -XX:MaxNewSize=1G
- Si el número de instancias de NodeManager en el clúster alcanza 500, los parámetros JVM recomendados de la instancia de ResourceManager son los siguientes: -Xms10G -Xmx10G -XX:NewSize=1G -XX:MaxNewSize=2G
- Si el número de instancias de NodeManager en el clúster alcanza 1000, los parámetros JVM recomendados de la instancia de ResourceManager son los siguientes: -Xms20G -Xmx20G -XX:NewSize=1G -XX:MaxNewSize=2G
- Si el número de instancias de NodeManager en el clúster alcanza 2000, los parámetros JVM recomendados de la instancia de ResourceManager son los siguientes: -Xms40G -Xmx40G -XX:NewSize=2G -XX:MaxNewSize=4G
- Si el número de instancias de NodeManager en el clúster alcanza 3000, los parámetros JVM recomendados de la instancia de ResourceManager son los siguientes: -Xms60G -Xmx60G -XX:NewSize=2G -XX:MaxNewSize=4G
- Si el número de instancias de NodeManager en el clúster alcanza las 4000, los parámetros JVM recomendados de la instancia de ResourceManager son los siguientes: -Xms80G -Xmx80G -XX:NewSize=2G -XX:MaxNewSize=4G
- Si el número de instancias de NodeManager en el clúster alcanza 5000, los parámetros JVM recomendados de la instancia de ResourceManager son los siguientes: -Xms100G -Xmx100G -XX:NewSize=3G -XX:MaxNewSize=6G

Paso 5 Verifique si la alarma se ha borrado.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 6**.

Recopilar información de fallas.

Paso 6 En el portal del FusionInsight Manager, elija **O&M** > **Log > Download**.

Paso 7 Seleccione el nodo siguiente en el clúster requerido desde el **Service**.

- NodeAgent
- Yarn

Paso 8 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 9 Póngase en contacto con el y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.134 ALM-18009 El uso de memoria heap de JobHistoryServer supera el umbral

Descripción

El sistema comprueba el uso de memoria heap de Mapreduce JobHistoryServer cada 30 segundos y compara el uso real con el umbral. La alarma se genera cuando el uso de memoria heap de Mapreduce JobHistoryServer excede el umbral (95% de la memoria máxima de forma predeterminada).

Los usuarios pueden elegir **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster* > **Mapreduce** para cambiar el umbral.

Cuando el **Trigger Count** es 1, esta alarma se borra cuando el uso de memoria heap de MapReduce JobHistoryServer es menor o igual que el umbral. Cuando el **Trigger Count** es mayor que 1, esta alarma se borra cuando el uso de memoria heap de MapReduce JobHistoryServer es menor o igual al 95% del umbral.

Atributo

ID de alarma	Gravedad de la alarma	Borrado automáticamente
18009	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el nombre del servicio para el que se genera la alarma.
RoleName	Especifica el nombre del rol para el que se genera la alarma.
HostName	Especifica el objeto (ID de host) para el que se genera la alarma.

Nombre	Significado
Trigger Condition	Especifica el umbral que activa la alarma. Si el valor del indicador actual excede este umbral, se genera la alarma.

Impacto en el sistema

Cuando el uso de memoria heap de JobHistoryServer de Mapreduce es excesivo, el rendimiento del archivo de registros de Mapreduce se ve afectado. Además, puede producirse un desbordamiento de memoria para que el servicio Yarn no esté disponible.

Causas posibles

La memoria heap de la instancia de JobHistoryServer de Mapreduce en el nodo se utiliza en exceso o la memoria heap se asigna de forma inadecuada. Como resultado, el uso excede el umbral.

Procedimiento

Comprobar el uso de memoria.

Paso 1 En el portal FusionInsight Manager, elija **O&M > Alarm > Alarms** > **ALM-18009 Heap Memory Usage of MapReduce JobHistoryServer Exceeds the Threshold** > **Location**. Compruebe el HostName de la instancia para la que se genera la alarma.

Paso 2 En el portal del FusionInsight Manager, elija **Cluster** > *Name of the desired cluster* **> Services** > **Mapreduce** > **Instance** > **JobHistoryServer.** Haga clic en el menú desplegable en la esquina superior derecha de **Chart**, elija **Customize** > **JobHistoryServer heap memory usage statistics**. JobHistoryServer indica el HostName correspondiente de la instancia para la que se genera la alarma. Compruebe el uso de la memoria heap.

Paso 3 Compruebe si la memoria heap utilizada de JobHistoryServer alcanza el 95% de la memoria heap máxima especificada para JobHistoryServer.

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 6**.

Paso 4 En el portal del FusionInsight Manager, seleccione **Cluster** > *Name of the desired cluster* **> Services** > **Mapreduce** > **Configurations** > **All Configurations** > **JobHistoryServer** > **System**. Aumente el valor del parámetro **GC_OPTS** según sea necesario, haga clic en **Save**. Haga clic en **OK** y reinicie la instancia de rol.

NOTA

El mapeo entre el número de tareas históricas (10000) y la memoria de JobHistoryServer es el siguiente:

-Xms30G -Xmx30G -XX:NewSize=1G -XX:MaxNewSize=2G

Paso 5 Verifique si la alarma se ha borrado.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 6**.

Recopilar información de fallas.

Paso 6 En el portal del FusionInsight Manager, elija **O&M** > **Log > Download**.

Paso 7 Seleccione el nodo siguiente en el clúster requerido desde el **Service**.

- NodeAgent
- Mapreduce

Paso 8 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 9 Póngase en contacto con el y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.135 ALM-18010 El tiempo de GC de ResourceManager supera el umbral

Descripción

El sistema comprueba la duración de la recolección de basura (GC) del proceso ResourceManager cada 60 segundos. Esta alarma se genera cuando la duración de GC excede el umbral (12 segundos por defecto).

Esta alarma se borra cuando la duración de GC es menor que el umbral.

Atributo

ID de alarma	Gravedad de la alarma	Borrado automáticamente
18010	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.

Nombre	Significado
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger Condition	Especifica el umbral que activa la alarma. Si el valor del indicador actual excede este umbral, se genera la alarma.

Impacto en el sistema

Una larga duración de GC del proceso de ResourceManager puede interrumpir los servicios.

Causas posibles

La memoria heap de la instancia ResourceManager se utiliza en exceso o la memoria heap se asigna de forma inadecuada. Como resultado, los GC ocurren con frecuencia.

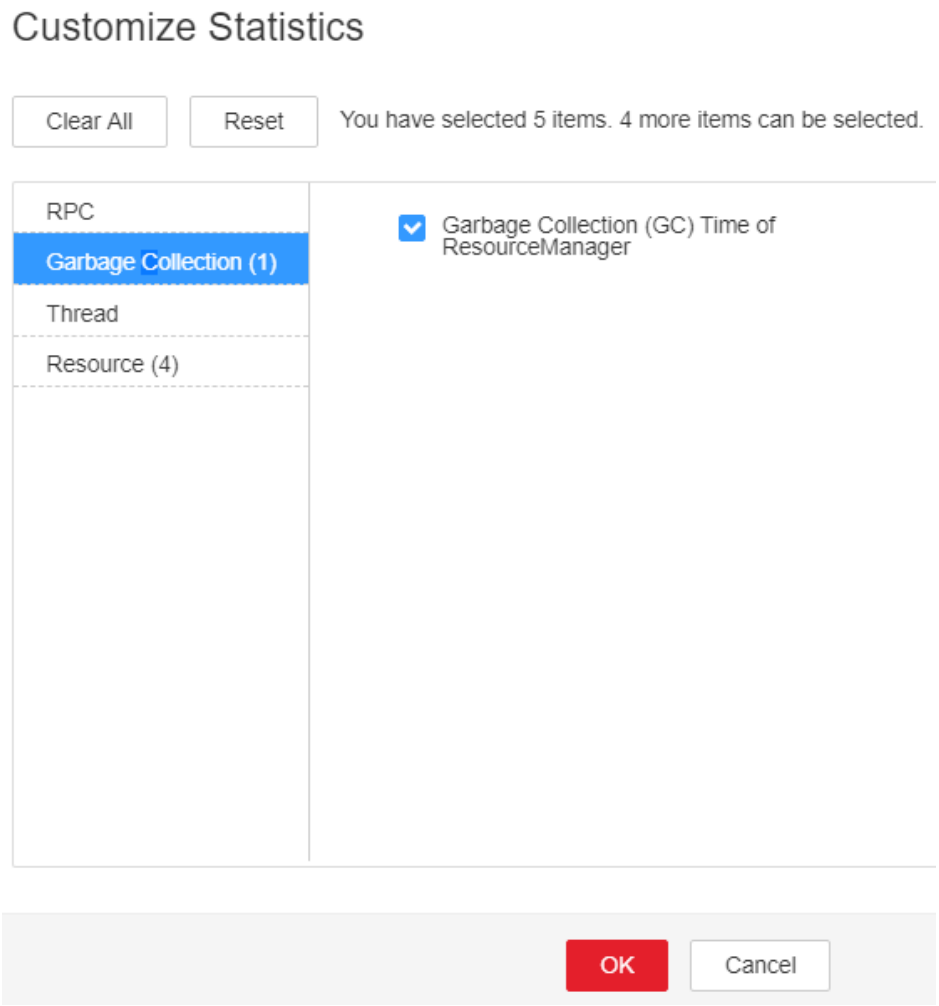
Procedimiento

Comprobar la duración del GC.

Paso 1 En el portal de FusionInsight Manager, elija **O&M > Alarm > Alarms** > **ALM-18010 ResourceManager GC Time Exceeds the Threshold** > **Location** para comprobar la dirección IP del ejemplo para el que se genera la alarma.

Paso 2 En el portal del FusionInsight Manager, seleccione **Cluster** > *Name of the desired cluster* **> Services** > **Yarn** > **Instance** > **ResourceManager (IP address for which the alarm is generated)**. Haga clic en el menú desplegable en la esquina superior derecha de **Chart** y elija **Customize** > **Garbage Collection (GC) Time of ResourceManager** para comprobar las estadísticas de duración de GC del proceso de Broker recopiladas cada minuto.

Figura 9-42 Tiempo de Recopilación de basura (GC) de ResourceManager



Paso 3 Compruebe si la duración GC del proceso de ResourceManager recopilado cada minuto supera el umbral (12 segundos por defecto).

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 7**.

Paso 4 En el portal del FusionInsight Manager, elija **Cluster** > *Name of the desired cluster* > **Services** > **Yarn** > **Configurations** > **All Configurations** > **ResourceManager** > **System** para aumentar el valor del parámetro **GC_OPTS** según sea necesario.

NOTA

La asignación entre el número de instancias de NodeManager en un clúster y el tamaño de memoria de ResourceManager es la siguiente:

- Si el número de instancias NodeManager en el clúster alcanza 100, los parámetros JVM recomendados de la instancia de ResourceManager son los siguientes: -Xms4G -Xmx4G -XX:NewSize=512M -XX:MaxNewSize=1G
- Si el número de instancias de NodeManager en el clúster alcanza 200, los parámetros JVM recomendados de la instancia de ResourceManager son los siguientes: -Xms6G -Xmx6G -XX:NewSize=512M -XX:MaxNewSize=1G
- Si el número de instancias de NodeManager en el clúster alcanza 500, los parámetros JVM recomendados de la instancia de ResourceManager son los siguientes: -Xms10G -Xmx10G -XX:NewSize=1G -XX:MaxNewSize=2G
- Si el número de instancias de NodeManager en el clúster alcanza 1000, los parámetros JVM recomendados de la instancia de ResourceManager son los siguientes: -Xms20G -Xmx20G -XX:NewSize=1G -XX:MaxNewSize=2G
- Si el número de instancias de NodeManager en el clúster alcanza 2000, los parámetros JVM recomendados de la instancia de ResourceManager son los siguientes: -Xms40G -Xmx40G -XX:NewSize=2G -XX:MaxNewSize=4G
- Si el número de instancias de NodeManager en el clúster alcanza 3000, los parámetros JVM recomendados de la instancia de ResourceManager son los siguientes: -Xms60G -Xmx60G -XX:NewSize=2G -XX:MaxNewSize=4G
- Si el número de instancias de NodeManager en el clúster alcanza las 4000, los parámetros JVM recomendados de la instancia de ResourceManager son los siguientes: -Xms80G -Xmx80G -XX:NewSize=2G -XX:MaxNewSize=4G
- Si el número de instancias de NodeManager en el clúster alcanza 5000, los parámetros JVM recomendados de la instancia de ResourceManager son los siguientes: -Xms100G -Xmx100G -XX:NewSize=3G -XX:MaxNewSize=6G

Paso 5 Guarde la configuración y reinicie la instancia ResourceManager.

Paso 6 Verifique si la alarma se ha borrado.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 7**.

Recopilar información de fallas.

Paso 7 En el portal del FusionInsight Manager, elija **O&M** > **Log > Download**.

Paso 8 Seleccione **ResourceManager** en el clúster requerido en el **Service**.

Paso 9 Haga clic en  en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 10 Póngase en contacto con el y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.136 ALM-18011 El tiempo de GC de NodeManager supera el umbral

Descripción

El sistema comprueba la duración de la recolección de basura (GC) del proceso NodeManager cada 60 segundos. Esta alarma se genera cuando la duración de GC excede el umbral (12 segundos por defecto).

Esta alarma se borra cuando la duración de GC es menor que el umbral.

Atributo

ID de alarma	Gravedad de la alarma	Borrado automáticamente
18011	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger Condition	Especifica el umbral que activa la alarma. Si el valor del indicador actual excede este umbral, se genera la alarma.

Impacto en el sistema

Una larga duración GC del proceso NodeManager puede interrumpir los servicios.

Causas posibles

La memoria heap de la instancia NodeManager se utiliza en exceso o la memoria heap se asigna de forma inadecuada. Como resultado, los GC ocurren con frecuencia.

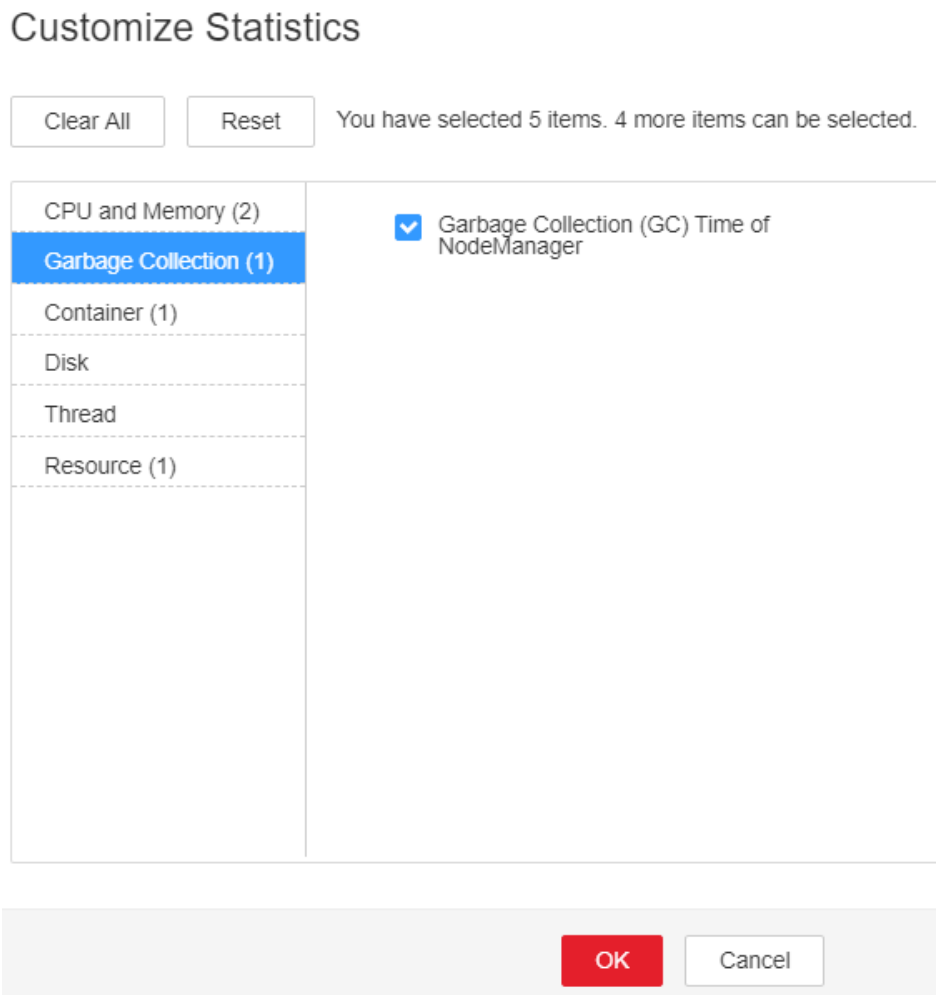
Procedimiento

Comprobar la duración del GC.

Paso 1 En el portal del FusionInsight Manager, elija **O&M > Alarm > Alarms** > **ALM-18011 NodeManager GC Time Exceeds the Threshold** > **Location** para comprobar la dirección IP de el ejemplo para el que se genera la alarma.

Paso 2 En el portal del FusionInsight Manager, seleccione **Cluster >** *Name of the desired cluster* **> Services** > **Yarn** > **Instance** > **NodeManager (IP address for which the alarm is generated)**. Haga clic en el menú desplegable en la esquina superior derecha de **Chart** y elija **Customize** > **Garbage Collection (GC) Time of NodeManager** para comprobar las estadísticas de duración de GC del proceso de Broker recopiladas cada minuto.

Figura 9-43 Tiempo de recolección de basura (GC) de NodeManager



Paso 3 Compruebe si la duración GC del proceso NodeManager recopilado cada minuto supera el umbral (12 segundos por defecto).

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 7**.

Paso 4 En el portal FusionInsight Manager, elija **Cluster >** *Name of the desired cluster* **> Services** > **Yarn** > **Configurations** > **All Configurations** > **NodeManager** > **System** para aumentar el valor del parámetro **GC_OPTS** según sea necesario.

NOTA

La asignación entre el número de instancias de NodeManager en un clúster y el tamaño de memoria de NodeManager es la siguiente:

- Si el número de instancias de NodeManager en el clúster alcanza 100, los parámetros de JVM recomendados para las instancias de NodeManager son los siguientes: -Xms2G -Xmx4G -XX:NewSize=512M -XX:MaxNewSize=1G
- Si el número de instancias de NodeManager en el clúster alcanza 200, los parámetros de JVM recomendados para las instancias de NodeManager son los siguientes: -Xms4G -Xmx4G -XX:NewSize=512M -XX:MaxNewSize=1G
- Si el número de instancias de NodeManager en el clúster alcanza 500, los parámetros JVM recomendados para las instancias de NodeManager son los siguientes: -Xms8G -Xmx8G -XX:NewSize=1G -XX:MaxNewSize=2G

Paso 5 Guarde la configuración y reinicie la instancia NodeManager.

Paso 6 Verifique si la alarma se ha borrado.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 7**.

Recopilar información de fallas.

Paso 7 En el portal del FusionInsight Manager, elija **O&M** > **Log > Download**.

Paso 8 Seleccione **NodeManager** en el clúster requerido en el **Service**.

Paso 9 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 10 Póngase en contacto con el y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.137 ALM-18012 El tiempo de GC de JobHistoryServer supera el umbral

Descripción

El sistema comprueba la duración de la recolección de basura (GC) del proceso JobHistoryServer cada 60 segundos. Esta alarma se genera cuando la duración de GC excede el umbral (12 segundos por defecto).

Esta alarma se borra cuando la duración de GC es menor que el umbral.

Atributo

ID de alarma	Gravedad de la alarma	Borrado automáticamente
18012	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger Condition	Especifica el umbral que activa la alarma. Si el valor del indicador actual excede este umbral, se genera la alarma.

Impacto en el sistema

Una larga duración GC del proceso de JobHistoryServer puede interrumpir los servicios.

Causas posibles

La memoria heap de la instancia de JobHistoryServer se utiliza en exceso o la memoria heap se asigna de forma inadecuada. Como resultado, los GC ocurren con frecuencia.

Procedimiento

Comprobar la duración del GC.

Paso 1 En el portal del administrador FusionInsight, elija **O&M > Alarm > Alarms** > **ALM-18012 JobHistoryServer GC Time Exceeds the Threshold** > **Location** para comprobar la dirección IP de el ejemplo para el que se genera la alarma.

Paso 2 En el portal FusionInsight Manager, elija **Cluster >** *Name of the desired cluster* **> Services** > **MapReduce** > **Instance** > **JobHistoryServer (IP address for which the alarm is generated)**. Haga clic en el menú desplegable en la esquina superior derecha de **Chart**, seleccione **Customize** > **Garbage Collection (GC) Time of the JobHistoryServer** para comprobar las estadísticas de duración de GC del proceso de Broker recopiladas cada minuto.

Paso 3 Compruebe si la duración GC del proceso de JobHistoryServer recopilado cada minuto supera el umbral (12 segundos por defecto).

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 7**.

Paso 4 En el portal Administrador de FusionInsight, elija **Cluster >** *Name of the desired cluster* **> Services** > **MapReduce** > **Configurations** > **All Configurations** > **JobHistoryServer** > **System** para aumentar el valor del parámetro **GC_OPTS** según sea necesario.

NOTA

El mapeo entre el número de tareas históricas (10000) y la memoria del JobHistoryServer es el siguiente:

-Xms30G -Xmx30G -XX:NewSize=1G -XX:MaxNewSize=2G

Paso 5 Guarde la configuración y reinicie la instancia de JobHistoryServer.

Paso 6 Verifique si la alarma se ha borrado.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 7**.

Recopilar información de fallas.

Paso 7 En el portal del FusionInsight Manager, elija **O&M** > **Log > Download**.

Paso 8 Seleccione **JobHistoryServer** en el clúster requerido en el **Service**.

Paso 9 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 10 Póngase en contacto con el y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.138 ALM-18013 El uso de memoria directa de ResourceManager supera el umbral

Descripción

El sistema comprueba el uso de la memoria directa del servicio Yarn cada 30 segundos. Esta alarma se genera cuando el uso de memoria directa de una instancia de ResourceManager excede el umbral (90% de la memoria máxima).

La alarma se borra cuando el uso directo de memoria es menor que el umbral.

Atributo

ID de alarma	Gravedad de la alarma	Borrado automáticamente
18013	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger Condition	Especifica el umbral que activa la alarma. Si el valor del indicador actual excede este umbral, se genera la alarma.

Impacto en el sistema

Si la memoria directa disponible del servicio Yarn es insuficiente, se produce un desbordamiento de memoria y el servicio se interrumpe.

Causas posibles

La memoria directa de la instancia de ResourceManager se utiliza en exceso o la memoria directa se asigna de forma inapropiada.

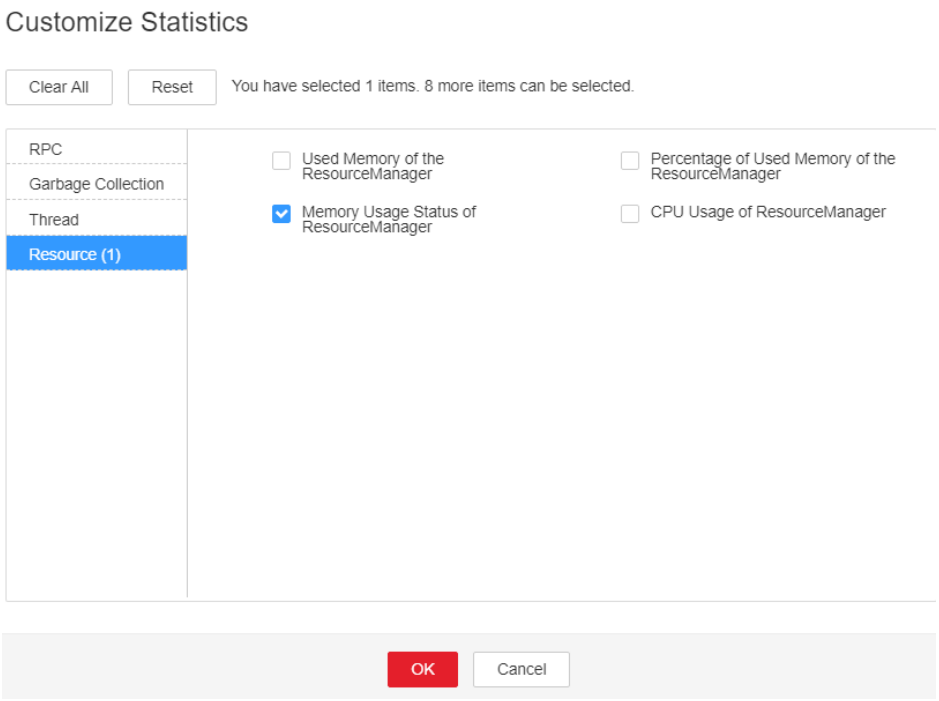
Procedimiento

Comprobar el uso de la memoria directa.

Paso 1 En el portal del FusionInsight Manager, elija **O&M > Alarm > Alarms** > **ALM-18013 ResourceManager Direct Memory Usage Exceeds the Threshold** > **Location** para comprobar la dirección IP del ejemplo para el que se genera la alarma.

Paso 2 En el portal del FusionInsight Manager, seleccione **Cluster >** *Name of the desired cluster* **> Services** > **Yarn** > **Instance** > **ResourceManager (IP address for which the alarm is generated)**. Haga clic en el menú desplegable en la esquina superior derecha de **Chart** y elija **Customize** > **Memory Usage Status of ResourceManager** para comprobar el uso de la memoria directa.

Figura 9-44 Estado de uso de memoria de ResourceManager



Paso 3 Compruebe si la memoria directa utilizada de ResourceManager alcanza el 90% de la memoria directa máxima especificada para ResourceManager de forma predeterminada.

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 9**.

Paso 4 En el portal de FusionInsight Manager, elija **Cluster >** *Name of the desired cluster* **> Services** > **Yarn** > **Configurations** > **All Configurations** > **ResourceManager** > **System** para aumentar el valor de comprobar si **-XX:MaxDirectMemorySize** existe en el parámetro **GC_OPTS**.

- En caso afirmativo, vaya a **Paso 5**.
- Si no, vaya a **Paso 7**.

Paso 5 En el parámetro **GC_OPTS**, elimine **-XX:MaxDirectMemorySize**.

Paso 6 Guarde la configuración y reinicie la instancia ResourceManager.

Paso 7 Compruebe si **ALM-18008 El uso de memoria heap de ResourceManager supera el umbral** existe.

- En caso afirmativo, maneje la alarma haciendo referencia a **ALM-18008 El uso de memoria heap de ResourceManager supera el umbral**.
- Si no, vaya a **Paso 8**.

Paso 8 Verifique si la alarma se ha borrado.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 9**.

Recopilar información de fallas.

Paso 9 En el portal del FusionInsight Manager, elija **O&M** > **Log > Download**.

Paso 10 Seleccione **ResourceManager** en el clúster requerido en el **Service**.

Paso 11 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 12 Póngase en contacto con el y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.139 ALM-18014 El uso de memoria directa de NodeManager supera el umbral

Descripción

El sistema comprueba el uso de la memoria directa del servicio Yarn cada 30 segundos. Esta alarma se genera cuando el uso de memoria directa de una instancia de NodeManager excede el umbral (90% de la memoria máxima).

La alarma se borra cuando el uso directo de memoria es menor que el umbral.

Atributo

ID de alarma	Gravedad de la alarma	Borrado automáticamente
18014	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.

Nombre	Significado
HostName	Especifica el host para el que se genera la alarma.
Trigger Condition	Especifica el umbral que activa la alarma. Si el valor del indicador actual excede este umbral, se genera la alarma.

Impacto en el sistema

Si la memoria directa disponible del servicio Yarn es insuficiente, se produce un desbordamiento de memoria y el servicio se interrumpe.

Causas posibles

La memoria directa de la instancia NodeManager se utiliza en exceso o la memoria directa se asigna de forma inapropiada.

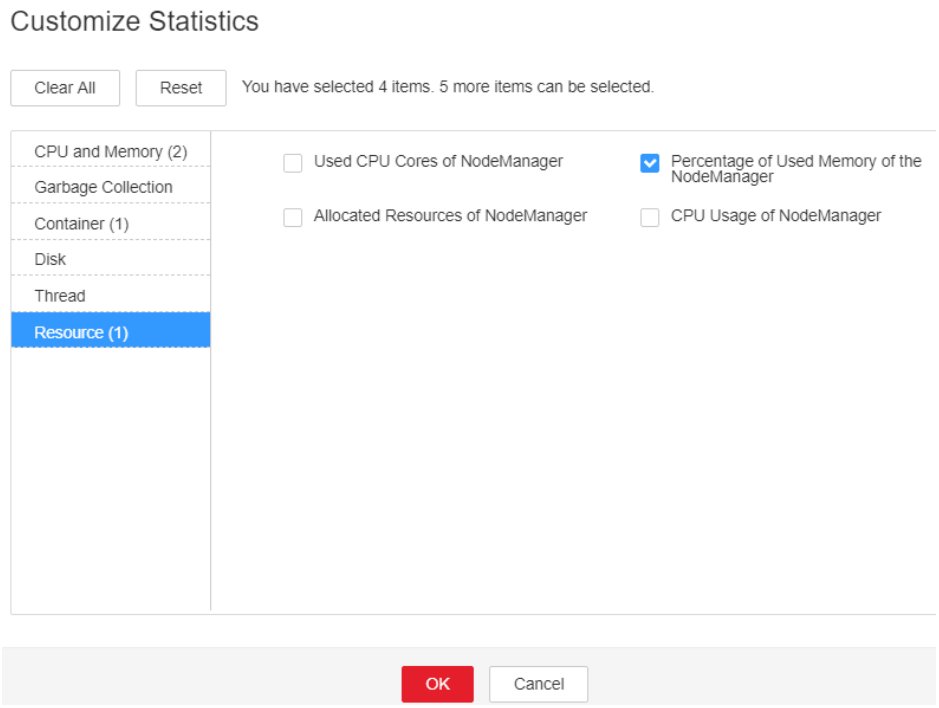
Procedimiento

Comprobar el uso de la memoria directa.

Paso 1 En el portal del FusionInsight Manager, elija **O&M** > **Alarm > Alarms** > **ALM-18014 NodeManager Direct Memory Usage Exceeds the Threshold** > **Location** para comprobar la dirección IP de el ejemplo para el que se genera la alarma.

Paso 2 En el portal del FusionInsight Manager, seleccione **Cluster >** *Name of the desired cluster* **> Services** > **Yarn** > **Instance** > **NodeManager (IP address for which the alarm is generated)**. Haga clic en el menú desplegable en la esquina superior derecha de **Chart** y elija **Customize** > **Resource** > **Percentage of Used Memory of the NodeManager** para comprobar el uso de la memoria directa.

Figura 9-45 Porcentaje de memoria usada del NodeManager



Paso 3 Compruebe si la memoria directa utilizada de NodeManager alcanza el 90% de la memoria directa máxima especificada para NodeManager de forma predeterminada.

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 9**.

Paso 4 En el portal del FusionInsight Manager, seleccione **Cluster** > *Name of the desired cluster* > **Services** > **Yarn** > **Configurations** > **All Configurations**> **NodeManager** > **System** para comprobar si existe "-XX:MaxDirectMemorySize" en el parámetro **GC_OPTS**.

- En caso afirmativo, vaya a **Paso 5**.
- Si no, vaya a **Paso 7**.

Paso 5 En el parámetro **GC_OPTS**, elimine "-XX:MaxDirectMemorySize".

Paso 6 Guarde la configuración y reinicie la instancia NodeManager.

Paso 7 Check whether the **ALM-18018 NodeManager Heap Memory Usage Exceeds the Threshold** exists.

- En caso afirmativo, maneje la alarma haciendo referencia a **ALM-18018 El uso de memoria heap de NodeManager supera el umbral**.
- Si no, vaya a **Paso 8**.

Paso 8 Verifique si la alarma se ha borrado.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 9**.

Recopilar información de fallas.

Paso 9 En el portal del FusionInsight Manager, elija **O&M** > **Log** > **Download**.

Paso 10 Seleccione **NodeManager** en el clúster requerido en el **Service**.

Paso 11 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 12 Póngase en contacto con el y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.140 ALM-18015 El uso de memoria directa de JobHistoryServer supera el umbral

Descripción

El sistema comprueba el uso de memoria directa del servicio MapReduce cada 30 segundos. Esta alarma se genera cuando el uso de memoria directa de una instancia de JobHistoryServer excede el umbral (90% de la memoria máxima).

La alarma se borra cuando el uso directo de memoria es menor que el umbral.

Atributo

ID de alarma	Gravedad de la alarma	Borrado automáticamente
18015	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Nombre	Significado
Trigger Condition	Especifica el umbral que activa la alarma. Si el valor del indicador actual excede este umbral, se genera la alarma.

Impacto en el sistema

Si la memoria directa disponible del servicio MapReduce es insuficiente, se produce un desbordamiento de memoria y el servicio se interrumpe.

Causas posibles

La memoria directa de la instancia de JobHistoryServer se utiliza en exceso o la memoria directa se asigna de forma inapropiada.

Procedimiento

Comprobar el uso de la memoria directa.

Paso 1 En el portal del FusionInsight Manager, elija **O&M > Alarm > Alarms** > **ALM-18015 JobHistoryServer Direct Memory Usage Exceeds the Threshold** > **Location** para comprobar la dirección IP del ejemplo para el que se genera la alarma.

Paso 2 En el portal FusionInsight Manager, elija **Cluster >** *Name of the desired cluster* **> Services** > **MapReduce** > **Instance** > **JobHistoryServer (IP address for which the alarm is generated).** Haga clic en el menú desplegable en la esquina superior derecha del **Chart**, seleccione **Customize** > **Memory Usage Status of JobHistoryServer** para comprobar el uso de la memoria directa.

Paso 3 Compruebe si la memoria directa utilizada de JobHistoryServer alcanza el 90% de la memoria directa máxima especificada para JobHistoryServer de forma predeterminada.

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 9**.

Paso 4 En el portal del FusionInsight Manager, seleccione **Cluster >** *Name of the desired cluster* **> Services** > **MapReduce** > **Configurations** > **All Configurations** > **JobHistoryServer** > **System** para comprobar si existe "-XX:MaxDirectMemorySize" en el parámetro **GC_OPTS**.

- En caso afirmativo, vaya a **Paso 5**.
- Si no, vaya a **Paso 7**.

Paso 5 En el parámetro **GC_OPTS**, elimine "-XX:MaxDirectMemorySize".

Paso 6 Guarde la configuración y reinicie la instancia de JobHistoryServer.

Paso 7 Compruebe si el **ALM-18009 El uso de memoria heap de JobHistoryServer supera el umbral** existe.

- En caso afirmativo, maneje la alarma haciendo referencia a **ALM-18009 El uso de memoria heap de JobHistoryServer supera el umbral**.
- Si no, vaya a **Paso 8**.

Paso 8 Verifique si la alarma se ha borrado.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 9**.

Recopilar información de fallas.

Paso 9 En el portal del FusionInsight Manager, elija **O&M** > **Log > Download**.

Paso 10 Seleccione **JobHistoryServer** en el clúster requerido en el **Service**.

Paso 11 Haga clic en  en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 12 Póngase en contacto con el y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.141 ALM-18016 El uso de memoria no heap de ResourceManager supera el umbral

Descripción

El sistema comprueba el uso de memoria no heap de ResourceManager de Yarn cada 30 segundos y compara el uso real con el umbral. La alarma se genera cuando el uso de memoria no heap de ResourceManager de Yarn excede el umbral (90% de la memoria máxima por defecto).

Los usuarios pueden elegir **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster* > **Yarn** para cambiar el umbral.

La alarma se borra cuando el uso de memoria no heap es menor o igual que el umbral.

Atributo

ID de alarma	Gravedad de la alarma	Borrado automáticamente
18016	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el nombre del servicio para el que se genera la alarma.
RoleName	Especifica el nombre del rol para el que se genera la alarma.
HostName	Especifica el objeto (ID de host) para el que se genera la alarma.
Trigger Condition	Especifica el umbral que activa la alarma. Si el valor del indicador actual excede este umbral, se genera la alarma.

Impacto en el sistema

Cuando el uso de memoria no heap de ResourceManager de Yarn es demasiado alto, el rendimiento del envío de tareas de Yarn y la operación se ve afectado. Además, puede producirse un desbordamiento de memoria para que el servicio Yarn no esté disponible.

Causas posibles

La memoria no heap de la instancia de ResourceManager de Yarn en el nodo se utiliza en exceso o la memoria no heap se asigna de forma inadecuada. Como resultado, el uso excede el umbral.

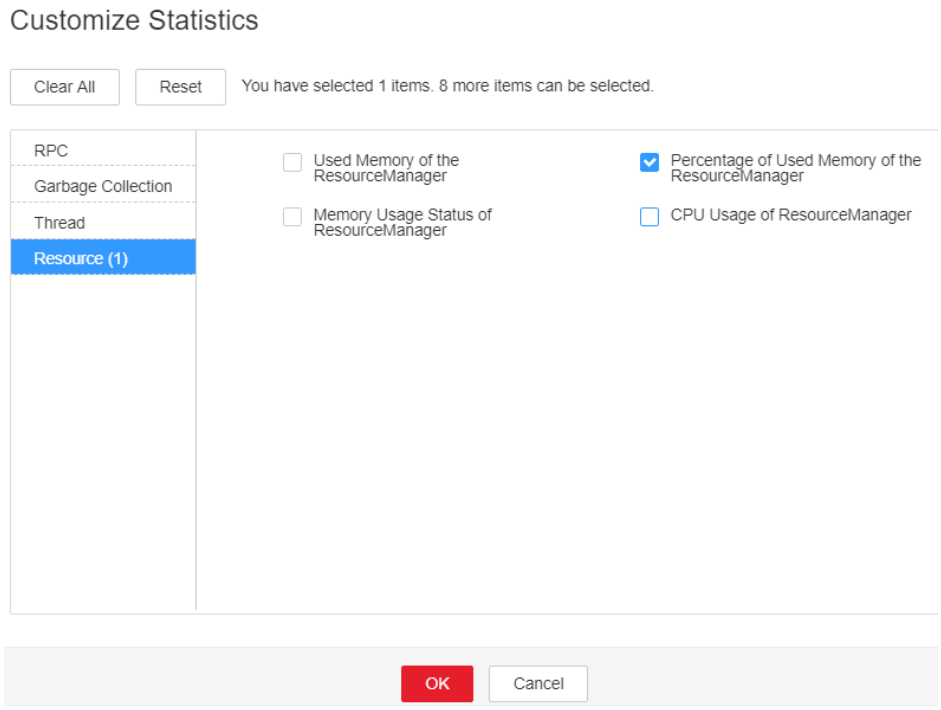
Procedimiento

Verificar el uso de la memoria no heap.

Paso 1 En el portal del FusionInsight Manager, elija **O&M > Alarm > Alarms** > **ALM-18016 Non Heap Memory Usage of Yarn ResourceManager Exceeds the Threshold** > **Location**. Compruebe el HostName de la instancia para la que se genera la alarma.

Paso 2 En el portal del FusionInsight Manager, seleccione **Cluster >** *Name of the desired cluster* **> Services** > **Yarn** > **Instance** > **ResourceManager**. Haga clic en el menú desplegable en la esquina superior derecha de **Chart** y elige **Customize** > **Percentage of Used Memory of the ResourceManager**. ResourceManager indica el HostName correspondiente de la instancia para la que se genera la alarma. Compruebe el uso de la memoria no heap.

Figura 9-46 Porcentaje de memoria usada del ResourceManager



Paso 3 Compruebe si la memoria no heap utilizada de ResourceManager alcanza el 90% del máximo de memoria no heap especificado para ResourceManager de forma predeterminada.

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 6**.

Paso 4 En el portal del FusionInsight Manager, seleccione **Cluster** > *Name of the desired cluster* > **Services** > **Yarn** > **Configurations** > **All Configurations** > **ResourceManager** > **System**. Ajuste el parámetro de memoria **GC_OPTS** de ResourceManager. Guarde la configuración y reinicie la instancia ResourceManager.

NOTA

La asignación entre el número de instancias de NodeManager en un clúster y el tamaño de memoria de ResourceManager es la siguiente:

- Si el número de instancias NodeManager en el clúster alcanza 100, los parámetros JVM recomendados de la instancia de ResourceManager son los siguientes: -Xms4G -Xmx4G -XX:NewSize=512M -XX:MaxNewSize=1G
- Si el número de instancias de NodeManager en el clúster alcanza 200, los parámetros JVM recomendados de la instancia de ResourceManager son los siguientes: -Xms6G -Xmx6G -XX:NewSize=512M -XX:MaxNewSize=1G
- Si el número de instancias de NodeManager en el clúster alcanza 500, los parámetros JVM recomendados de la instancia de ResourceManager son los siguientes: -Xms10G -Xmx10G -XX:NewSize=1G -XX:MaxNewSize=2G
- Si el número de instancias de NodeManager en el clúster alcanza 1000, los parámetros JVM recomendados de la instancia de ResourceManager son los siguientes: -Xms20G -Xmx20G -XX:NewSize=1G -XX:MaxNewSize=2G
- Si el número de instancias de NodeManager en el clúster alcanza 2000, los parámetros JVM recomendados de la instancia de ResourceManager son los siguientes: -Xms40G -Xmx40G -XX:NewSize=2G -XX:MaxNewSize=4G
- Si el número de instancias de NodeManager en el clúster alcanza 3000, los parámetros JVM recomendados de la instancia de ResourceManager son los siguientes: -Xms60G -Xmx60G -XX:NewSize=2G -XX:MaxNewSize=4G
- Si el número de instancias de NodeManager en el clúster alcanza las 4000, los parámetros JVM recomendados de la instancia de ResourceManager son los siguientes: -Xms80G -Xmx80G -XX:NewSize=2G -XX:MaxNewSize=4G
- Si el número de instancias de NodeManager en el clúster alcanza 5000, los parámetros JVM recomendados de la instancia de ResourceManager son los siguientes: -Xms100G -Xmx100G -XX:NewSize=3G -XX:MaxNewSize=6G

Paso 5 Verifique si la alarma se ha borrado.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 6**.

Recopilar información de fallas.

Paso 6 En el portal del FusionInsight Manager, elija **O&M** > **Log > Download**.

Paso 7 Seleccione el nodo siguiente en el clúster requerido desde el **Service**.

- NodeAgent
- Yarn

Paso 8 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 9 Póngase en contacto con el y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.142 ALM-18017 El uso de memoria no heap de NodeManager supera el umbral

Descripción

El sistema comprueba el uso de memoria no heap de Yarn NodeManager cada 30 segundos y compara el uso real con el umbral. La alarma se genera cuando el uso de memoria no heap de Yarn NodeManager excede el umbral (90% de la memoria máxima por defecto).

Los usuarios pueden elegir **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster* > **Yarn** para cambiar el umbral.

La alarma se borra cuando el uso de memoria no heap es menor o igual que el umbral.

Atributo

ID de alarma	Gravedad de la alarma	Borrado automáticamente
18017	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el nombre del servicio para el que se genera la alarma.
RoleName	Especifica el nombre del rol para el que se genera la alarma.
HostName	Especifica el objeto (ID de host) para el que se genera la alarma.
Trigger Condition	Especifica el umbral que activa la alarma. Si el valor del indicador actual excede este umbral, se genera la alarma.

Impacto en el sistema

Cuando el uso de memoria no heap de Yarn NodeManager es demasiado alto, el rendimiento del envío de tareas de Yarn y la operación se ve afectado. Además, puede producirse un desbordamiento de memoria para que el servicio Yarn no esté disponible.

Causas posibles

La memoria no heap de la instancia de NodeManager de Yarn en el nodo se utiliza en exceso o la memoria no heap se asigna de forma inadecuada. Como resultado, el uso excede el umbral.

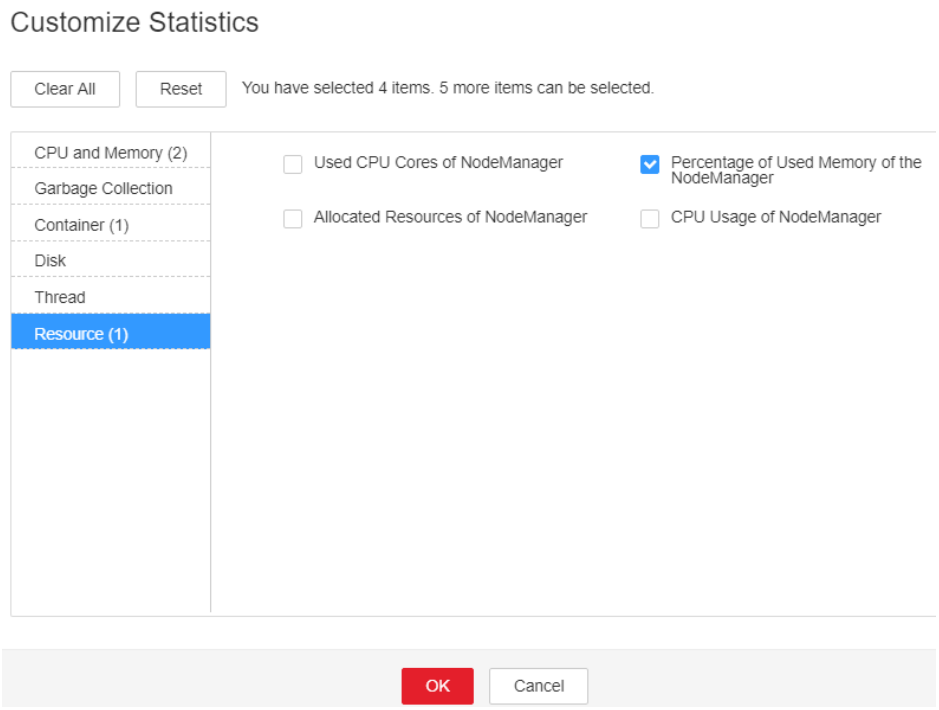
Procedimiento

Verificar el uso de la memoria no heap.

Paso 1 En el portal del administrador FusionInsight, elija **O&M > Alarm > Alarms** > **ALM-18017 Non Heap Memory Usage of Yarn NodeManager Exceeds the Threshold** > **Location**. Compruebe el HostName de la instancia para la que se genera la alarma.

Paso 2 En el portal del administrador de FusionInsight, seleccione **Cluster >** *Name of the desired cluster* **> Services** > **Yarn** > **Instance** > **NodeManager**. Haga clic en el menú desplegable en la esquina superior derecha de **Chart** y elige **Customize** > **Resource** > **Percentage of Used Memory of the NodeManager**. NodeManager indica el HostName correspondiente de la instancia para la que se genera la alarma. Compruebe el uso de la memoria no heap.

Figura 9-47 Porcentaje de memoria usada del NodeManager



Paso 3 Compruebe si la memoria No Heap utilizada de NodeManager alcanza el 90% del máximo de memoria No Heap especificado para NodeManager de forma predeterminada.

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 6**.

Paso 4 En el portal del administrador de FusionInsight, seleccione **Cluster >** *Name of the desired cluster* **> Services** > **Yarn** > **Configurations** > **All Configurations** > **NodeManager** > **System**. Ajuste el parámetro de memoria **GC_OPTS** de NodeManager, haga clic en **Save**, haga clic en **OK,** y reinicie la instancia de rol.

NOTA

La asignación entre el número de instancias de NodeManager en un clúster y el tamaño de memoria de NodeManager es la siguiente:

- Si el número de instancias de NodeManager en el clúster alcanza 100, los parámetros de JVM recomendados para las instancias de NodeManager son los siguientes: -Xms2G -Xmx4G -XX:NewSize=512M -XX:MaxNewSize=1G
- Si el número de instancias de NodeManager en el clúster alcanza 200, los parámetros de JVM recomendados para las instancias de NodeManager son los siguientes: -Xms4G -Xmx4G -XX:NewSize=512M -XX:MaxNewSize=1G
- Si el número de instancias de NodeManager en el clúster alcanza 500, los parámetros JVM recomendados para las instancias de NodeManager son los siguientes: -Xms8G -Xmx8G -XX:NewSize=1G -XX:MaxNewSize=2G

Paso 5 Verifique si la alarma se ha borrado.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 6**.

Recopilar información de fallas.

Paso 6 En el portal del FusionInsight Manager, elija **O&M** > **Log > Download**.

Paso 7 Seleccione el nodo siguiente en el clúster requerido desde el **Service**.

- NodeAgent
- Yarn

Paso 8 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 9 Póngase en contacto con el y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.143 ALM-18018 El uso de memoria heap de NodeManager supera el umbral

Descripción

El sistema comprueba el uso de memoria heap de NodeManager de Yarn cada 30 segundos y compara el uso real con el umbral. La alarma se genera cuando el uso de memoria heap de Yarn NodeManager excede el umbral (95% de la memoria máxima por defecto).

La alarma se borra cuando el uso de memoria heap es menor o igual que el umbral.

Atributo

ID de alarma	Gravedad de la alarma	Borrado automáticamente
18018	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el nombre del servicio para el que se genera la alarma.
RoleName	Especifica el nombre del rol para el que se genera la alarma.
HostName	Especifica el objeto (ID de host) para el que se genera la alarma.
Trigger Condition	Especifica el umbral que activa la alarma. Si el valor del indicador actual excede este umbral, se genera la alarma.

Impacto en el sistema

Cuando el uso de memoria heap de Yarn NodeManager es demasiado alto, el rendimiento del envío y la operación de la tarea de Yarn se ve afectado. Además, puede producirse un desbordamiento de memoria para que el servicio Yarn no esté disponible.

Causas posibles

La memoria heap de la instancia de NodeManager de Yarn en el nodo se utiliza en exceso o la memoria heap se asigna de forma inapropiada. Como resultado, el uso excede el umbral.

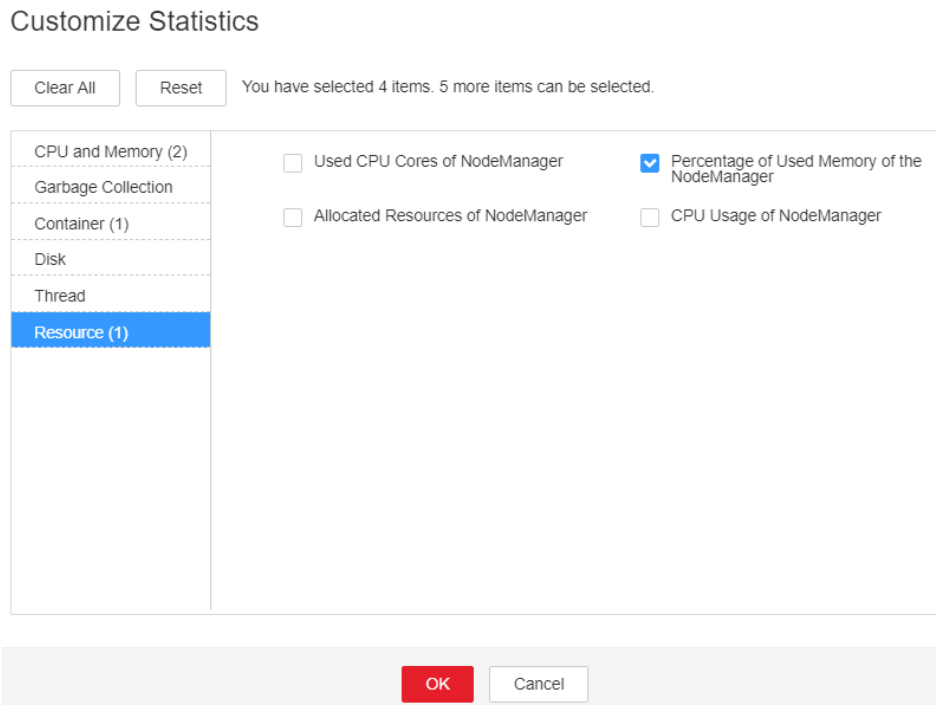
Procedimiento

Comprobar el uso de la memoria heap.

Paso 1 En el portal del FusionInsight Manager, elija **O&M > Alarm > Alarms** > **ALM-18018 NodeManager Heap Memory Usage Exceeds the Threshold** > **Location**. Compruebe el HostName de la instancia para la que se genera la alarma.

Paso 2 En el portal del FusionInsight Manager, seleccione **Cluster >** *Name of the desired cluster* **> Services** > **Yarn** > **Instance** > **NodeManager**. Haga clic en el menú desplegable en la esquina superior derecha de **Chart** y seleccione **Customize** > **Resource** > **Percentage of Used Memory of the NodeManager** para comprobar el uso de memoria heap.

Figura 9-48 Porcentaje de memoria usada del NodeManager



Paso 3 Compruebe si la memoria heap utilizada de NodeManager alcanza el 95% de la memoria heap máxima especificada para NodeManager.

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 6**.

Paso 4 En el portal del FusionInsight Manager, seleccione **Cluster** > *Name of the desired cluster* > **Services** > **Yarn** > **Configurations** > **All Configurations** > **NodeManager** > **System**. Aumente el valor del parámetro **GC_OPTS** según sea necesario, haga clic en **Save** y haga clic en **OK** y reinicie la instancia de rol.

NOTA

La asignación entre el número de instancias de NodeManager en un clúster y el tamaño de memoria de NodeManager es la siguiente:

- Si el número de instancias de NodeManager en el clúster alcanza 100, los parámetros de JVM recomendados para las instancias de NodeManager son los siguientes: -Xms2G -Xmx4G -XX:NewSize=512M -XX:MaxNewSize=1G
- Si el número de instancias de NodeManager en el clúster alcanza 200, los parámetros de JVM recomendados para las instancias de NodeManager son los siguientes: -Xms4G -Xmx4G -XX:NewSize=512M -XX:MaxNewSize=1G
- Si el número de instancias de NodeManager en el clúster alcanza 500, los parámetros JVM recomendados para las instancias de NodeManager son los siguientes: -Xms8G -Xmx8G -XX:NewSize=1G -XX:MaxNewSize=2G

Paso 5 Verifique si la alarma se ha borrado.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 6**.

Recopilar información de fallas.

Paso 6 En el portal del FusionInsight Manager, elija **O&M** > **Log** > **Download**.

Paso 7 Seleccione el nodo siguiente en el clúster requerido desde el **Service**.

- NodeAgent
- Yarn

Paso 8 Haga clic en  en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 9 Póngase en contacto con el y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.144 ALM-18019 El uso de memoria no heap de JobHistoryServer supera el umbral

Descripción

El sistema comprueba el uso de memoria no heap de MapReduce JobHistoryServer cada 30 segundos y compara el uso real con el umbral. La alarma se genera cuando el uso de memoria no heap de MapReduce JobHistoryServer excede el umbral (90% de la memoria máxima por defecto).

Los usuarios pueden elegir **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster* > **MapReduce** para cambiar el umbral.

La alarma se borra cuando el uso de memoria no heap es menor o igual que el umbral.

Atributo

ID de alarma	Gravedad de la alarma	Borrado automáticamente
18019	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.

Nombre	Significado
ServiceName	Especifica el nombre del servicio para el que se genera la alarma.
RoleName	Especifica el nombre del rol para el que se genera la alarma.
HostName	Especifica el objeto (ID de host) para el que se genera la alarma.
Trigger Condition	Especifica el umbral que activa la alarma. Si el valor del indicador actual excede este umbral, se genera la alarma.

Impacto en el sistema

Cuando el uso de memoria no acumulable de MapReduce JobHistoryServer es excesivo, el rendimiento del envío y la operación de tareas de MapReduce se ve afectado. Además, puede producirse un desbordamiento de memoria para que el servicio MapReduce no esté disponible.

Causas posibles

La memoria no heap de la instancia de MapReduce JobHistoryServer en el nodo se utiliza en exceso o la memoria no heap se asigna de forma inadecuada. Como resultado, el uso excede el umbral.

Procedimiento

Verificar el uso de la memoria no heap.

Paso 1 En el portal FusionInsight Manager, elija **O&M > Alarm > Alarms** > **ALM-18019 Non Heap Memory Usage of MapReduce JobHistoryServer Exceeds the Threshold** > **Location**. Compruebe el HostName de la instancia para la que se genera la alarma.

Paso 2 En el portal FusionInsight Manager, elija **Cluster >** *Name of the desired cluster* **> Services** > **MapReduce** > **Instance** > **JobHistoryServer.** Haga clic en el menú desplegable en la esquina superior derecha de **Chart**, elija **Customize** > **JobHistoryServer Non Heap memory usage statistics**. JobHistoryServer indica el HostName correspondiente de la instancia para la que se genera la alarma. Compruebe el uso de la memoria no heap.

Paso 3 Compruebe si la memoria no heap utilizada de JobHistoryServer alcanza el 90% del máximo de memoria no heap especificado para JobHistoryServer.

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 6**.

Paso 4 En el portal del FusionInsight Manager, seleccione **Cluster >** *Name of the desired cluster* **> Services** > **MapReduce** > **Configurations** > **All Configurations** > **JobHistoryServer** > **System**. Ajuste el parámetro de memoria **GC_OPTS** del NodeManager, haga clic en **Save**, haga clic en **OK,** y reinicie la instancia de rol.

NOTA

El mapeo entre el número de tareas históricas (10000) y la memoria del JobHistoryServer es el siguiente:

-Xms30G -Xmx30G -XX:NewSize=1G -XX:MaxNewSize=2G

Paso 5 Verifique si la alarma se ha borrado.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 6**.

Recopilar información de fallas.

Paso 6 En el portal del FusionInsight Manager, elija **O&M** > **Log > Download**.

Paso 7 Seleccione el nodo siguiente en el clúster requerido desde el **Service**.

- NodeAgent
- MapReduce

Paso 8 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 9 Póngase en contacto con el y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.145 ALM-18020 Tiempo de espera de ejecución de tareas de Yarn

Descripción

El sistema comprueba las tareas de MapReduce y Spark (excepto las tareas permanentes de JDBC) enviadas a Yarn cada 15 minutos. Esta alarma se genera cuando el tiempo de ejecución de la tarea excede el tiempo de espera especificado por el usuario. Sin embargo, la tarea se puede ejecutar correctamente. El parámetro de tiempo de espera del cliente de MapReduce es: MapReduce.application.timeout.alarm y el de Spark es Spark.application.timeout.alarm. La unidad es ms.

Esta alarma se borra cuando finaliza la tarea.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
18020	Leves	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
ApplicationName	Especifica el objeto (ID de aplicación) para el que se genera la alarma.
Trigger Condition	Especifica el umbral para activar la alarma.

Impacto en el sistema

La alarma persiste después de que se agote el tiempo de ejecución de la tarea. Sin embargo, la tarea todavía se puede ejecutar correctamente, por lo que esta alarma no ejerce ningún impacto en el sistema.

Causas posibles

- El tiempo de espera especificado es más corto que el tiempo de ejecución requerido.
- Los recursos de cola para la tarea en ejecución son insuficientes.
- Se produce un sesgo de los datos de la tarea. Como resultado, algunas tareas procesan una gran cantidad de datos y tardan mucho en ejecutarse.

Procedimiento

Comprobar si el intervalo de tiempo de espera está configurado correctamente.

Paso 1 En FusionInsight Manager, seleccione **O&M**. En el panel de navegación de la izquierda, elija **Alarm** > **Alarms**. Se muestra la página **Alarms**.

Paso 2 Seleccione la alarma cuyo ID sea **18020**. En los detalles de la alarma, vea **Location** para obtener el nombre de la tarea de tiempo de espera y la duración del tiempo de espera.

Paso 3 En función del nombre de la tarea y del intervalo de tiempo de espera, elija **Cluster** > *Name of the desired cluster* > **Services** > **Yarn** > **ResourceManager (Active)** para iniciar sesión en la página de Yarn nativa. A continuación, busque la tarea en la página nativa, compruebe su **StartTime** y calcule el tiempo de ejecución de la tarea en función de la hora actual del sistema. Compruebe si el tiempo de ejecución de la tarea excede el tiempo de espera.

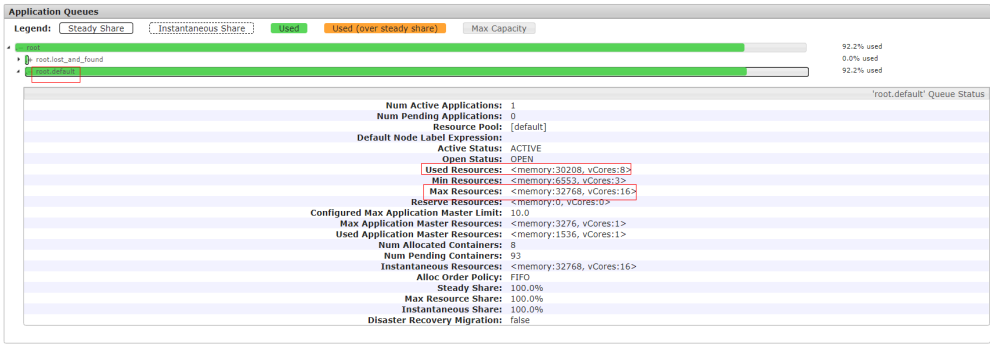
- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 10**.

Paso 4 Evalúe el tiempo de ejecución de la tarea esperado en función del servicio y compárelo con el intervalo de tiempo de espera de la tarea. Si el intervalo de tiempo de espera es demasiado corto, establezca el intervalo de tiempo de espera (**mapreduce.application.timeout.alarm** o **spark.application.timeout.alarm**) del cliente en el tiempo de ejecución esperado de la tarea. Vuelva a ejecutar la tarea y compruebe si la alarma está borrada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 5**.

Comprobar si los recursos de la cola son suficientes.

Paso 5 Busque la tarea en la página nativa y vea el nombre de la cola de la tarea. Haga clic en **Scheduler** a la izquierda de la página nativa. En la página **Applications Queues**, busque el nombre de la cola correspondiente y expanda los detalles de la cola, como se muestra en la siguiente figura.

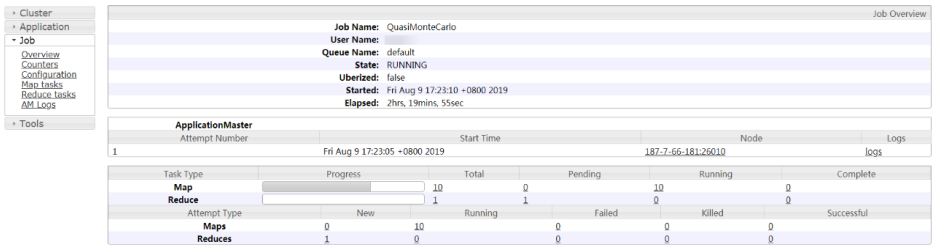


Paso 6 Compruebe si el valor de **Used Resources** en los detalles de la cola es aproximadamente igual al valor de **Max Resources** que indica que los recursos de la cola enviada por la tarea se han agotado. Si los recursos de la cola son insuficientes, elija **Tenant Resources** > **Dynamic Resource Plan** > **Resource Distribution Policy** en FusionInsight Manager y aumente el valor de **Max Resources** para la cola. Vuelva a ejecutar la tarea y compruebe si la alarma está borrada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 7**.

Comprobar si se produce un sesgo de datos.

Paso 7 En la página de Yarn nativa, haga clic en *task ID* (por ejemplo, en **application_1565337919723_0002**) > **Tracking URL:ApplicationMaster** > **job_1565337919723_0002**. Aparecerá en la pantalla la página siguiente.



Paso 8 Seleccione **Job** > **Map tasks** o **Job** > **Reduce tasks** a la izquierda y compruebe si el tiempo de ejecución de cada tarea de Map o Reduce difiere mucho. Si es así, se produce un sesgo de los datos de la tarea. En este caso, debe equilibrar los datos de la tarea.

Paso 9 Rectifique la falla basada en las causas anteriores y realice las tareas de nuevo. A continuación, compruebe si la alarma persiste.

- En caso afirmativo, vaya a **Paso 10**.
- En caso negativo, no se requiere ninguna otra acción.

Recopilar información de fallas.

Paso 10 En FusionInsight Manager, seleccione **O&M**. En el panel de navegación de la izquierda, elija **Log** > **Download**.

Paso 11 Expanda la lista desplegable **Service** y seleccione **Yarn** para el clúster de destino.

Paso 12 Haga clic en  en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 13 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

Información relacionada

Ninguna

9.146 ALM-18021 El servicio Mapreduce no está disponible

Descripción

El módulo de alarma comprueba el estado del servicio MapReduce cada 60 segundos. Esta alarma se genera cuando el sistema detecta que el servicio MapReduce no está disponible.

La alarma se borra cuando se recupera el servicio MapReduce.

Atributo

ID de alarma	Gravedad de la alarma	Borrado automáticamente
18021	Crítica	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

El clúster no puede proporcionar el servicio MapReduce. Por ejemplo, no se puede utilizar MapReduce para ver los registros de tareas o la función de archivo de registros no está disponible.

Causas posibles

- La instancia JobHistoryServer es anormal.
- El servicio KrbServer es anormal.
- El servicio ZooKeeper es anormal.
- El servicio HDFS anormal.
- El servicio Yarn es anormal.

Procedimiento

Comprobar el estado de instancia JobHistoryServer de servicio MapReduce.

Paso 1 En la página principal del Administrador FusionInsight, elija **Cluster** > *Name of the desired cluster* > **Services** > **MapReduce** > **Instance**.

Paso 2 Comprueba si el estado de ejecución de JobHistoryServer es de tipo **Normal**.

- En caso afirmativo, vaya a **Paso 11**.
- Si no, vaya a **Paso 3**.

Comprobar el estado de servicio KrbServer.

Paso 3 En la lista de alarmas del FusionInsight Manager, compruebe si existe **ALM-25500 Servicio KrbServer no disponible**.

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 5**.

Paso 4 Rectifique la falla siguiendo los pasos de **ALM-25500 Servicio KrbServer no disponible** y compruebe si la alarma está borrada.

- De ser así, no se requiere ninguna acción adicional.

- Si no, vaya a **Paso 5**.

Comprobar el servicio ZooKeeper.

Paso 5 En la lista de alarmas del FusionInsight Manager, compruebe si existe **ALM-13000 Servicio ZooKeeper Service no disponible**.

- En caso afirmativo, vaya a **Paso 6**.
- Si no, vaya a **Paso 7**.

Paso 6 Rectifique la falla siguiendo los pasos en **ALM-13000 Servicio ZooKeeper Service no disponible** y compruebe si la alarma está borrada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 7**.

Comprobar el estado de servicio HDFS.

Paso 7 En la lista de alarmas del Administrador de FusionInsight, compruebe si existe **ALM-14000 Servicio HDFS no disponible**.

- En caso afirmativo, vaya a **Paso 8**.
- Si no, vaya a **Paso 9**.

Paso 8 Rectifique el fallo siguiendo los pasos en **ALM-14000 Servicio HDFS no disponible** y compruebe si la alarma está borrada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 9**.

Comprobar el estado de servicio Yarn.

Paso 9 En la lista de alarmas del FusionInsight Manager, compruebe si existe **ALM-18000 Servicio Yarn no disponible**.

- En caso afirmativo, vaya a **Paso 10**.
- Si no, vaya a **Paso 11**.

Paso 10 Rectifique la falla siguiendo los pasos en **ALM-18000 Servicio Yarn no disponible** y compruebe si la alarma está borrada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 11**.

Recopilar información de fallas.

Paso 11 En la página de inicio del FusionInsight Manager del clúster activo, elija **O&M Log > Download.**

Paso 12 Seleccione **MapReduce** en el clúster requerido en **Service.**

Paso 13 Haga clic en  en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 14 Póngase en contacto con el y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.147 ALM-18022 Recursos de cola de Yarn insuficientes

Descripción

El módulo de alarma comprueba los recursos de cola de Yarn cada 60 segundos. Esta alarma se genera cuando los recursos disponibles o los recursos de ApplicationMaster (AM) de una cola son insuficientes.

Esta alarma se borra cuando los recursos disponibles son suficientes.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
18022	Leves	Sí

Parámetros

Nombre del parámetro	Descripción
Source	Especifica el clúster para el que se genera la alarma.
QueueName	Especifica la cola para la que se genera la alarma.
QueueMetric	Especifica la métrica de la cola para la que se genera la alarma.
Trigger Condition	Especifica el umbral que activa la alarma. Si el valor del indicador actual excede este umbral, se genera la alarma.

Impacto en el sistema

- Una aplicación que se está ejecutando lleva más tiempo.
- Una aplicación no se ejecuta durante mucho tiempo después de haber sido enviada.

Causas posibles

- Los recursos del nodo de NodeManager son insuficientes.

- La capacidad de recursos máxima configurada de la cola es excesivamente pequeña.
- El porcentaje de recursos de AM máximo configurado es excesivamente pequeño.

Procedimiento

Ver detalles de alarma.

Paso 1 En el FusionInsight Manager, elija **O&M** > **Alarm > Alarms**.

Paso 2 Vea la información de ubicación de esta alarma y compruebe si **QueueName** es **root** y **QueueMetric** es **Memory** o **QueueName** es **root** y **QueueMetric** es **vCores**.

- En caso afirmativo, vaya a **Paso 3**.
- Si no, vaya a **Paso 4**.

Paso 3 La memoria o la CPU del clúster de Yarn es insuficiente. En este caso, inicie sesión en el nodo donde reside NodeManager y ejecute los comandos **free -g** y **cat /proc/cpuinfo** para consultar la memoria disponible y la CPU disponible del nodo, respectivamente. En FusionInsight Manager, aumente los valores de **yarn.NodeManager.resource.memory-mb** y **yarn.NodeManager.resource.cpu-vcores** para el NodeManager de Yarn en función de los resultados de la consulta. A continuación, reinicie la instancia de NodeManager. Verifique si la alarma se ha borrado.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 4**.

Paso 4 Vea la información de ubicación de esta alarma y comprobar si **QueueName** es ***<Tenant Queue>*** y **QueueMetric** es **Memory**, o **QueueName** es ***<Tenant Queue>*** y **QueueMetric** es **vCores** en **Location**, compruebe si **available Memory =** o **available vCores =** está incluido en **Additional Information**.

- En caso afirmativo, vaya a **Paso 5**.
- Si no, vaya a **Paso 7**.

Paso 5 La memoria o CPU de la cola de tenant es insuficiente. En este caso, elija **Tenant Resources** > **Dynamic Resource Plan > Resource Distribution Policy** y aumente el valor de **Maximum Capacity**. Luego, verifique si la alarma se rectificó.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 6**.

Paso 6 Elija **Cluster** > *Name of the desired cluster* > **Services** > **Yarn** > **Configurations** > **All Configurations**. Introduce la palabra clave "threshold" y haga clic en **ResourceManager**. Ajuste los valores de umbral de los siguientes parámetros:

Si **Additional Information** contiene **available Memory =**, cambie el valor de **yarn.queue.memory.alarm.threshold** a un valor menor que el de **available Memory =** de **Additional Information**.

Si **Additional Information** contiene **available vCores =**, cambie el valor de **yarn.queue.vcore.alarm.threshold** a un valor menor que el de **available vCores =** de **Additional Information**.

Espere cinco minutos y compruebe si la alarma está desactivada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 9**.

Paso 7 Si **available AmMemory =** or **available AmvCores =** is included in **Additional Information**, la memoria de ApplicationMaster o CPU de la cola de tenant es insuficiente. En este caso, elija **Tenant Resources** > **Dynamic Resource Plan** > **Queue Configuration** y aumente el valor de **Maximum Am Resource Percent**. A continuación, compruebe si esta alarma está desactivada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 8**.

Paso 8 Elija **Cluster** > *Name of the desired cluster* > **Services** > **Yarn** > **Configurations** > **All Configurations**. Introduce la palabra clave "threshold" y haga clic en **ResourceManager**. Ajuste los valores de umbral de los siguientes parámetros:

Si **Additional Information** contiene **available AmMemory =**, cambie el valor de **yarn.queue.memory.alarm.threshold** a un valor menor que el de **available AmMemory =** de **Additional Information**.

Si **Additional Information** contiene **available AmvCores =**, cambie el valor de **yarn.queue.vcore.alarm.threshold** a un valor menor que el de **available AmvCores =** de **Additional Information**.

Espere cinco minutos y compruebe si la alarma está desactivada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 9**.

Recopilar información de fallas.

Paso 9 Inicie sesión en el FusionInsight Manager del clúster activo y elija **O&M** > **Log** > **Download**.

Paso 10 Seleccione **Yarn** en el clúster requerido en el **Service**.

Paso 11 Haga clic en  en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 12 Póngase en contacto con el y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Referencia

Ninguna

9.148 ALM-18023 El número de tareas pendientes de Yarn supera el umbral

Descripción

El módulo de alarma comprueba el número de aplicaciones pendientes en la cola root de Yarn cada 60 segundos. La alarma se genera cuando el número excede de 60.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
18023	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
QueueName	Identifica la cola para la que se genera la alarma.
QueueMetric	Identifica el indicador de cola para el que se genera la alarma.

Impacto en el sistema

- Se necesita mucho tiempo para finalizar una solicitud.
- Una nueva aplicación no se puede ejecutar después del envío.

Causas posibles

- Los recursos del nodo de NodeManager son insuficientes.
- La capacidad máxima de recursos de la cola y el porcentaje máximo de recursos de AM son demasiado pequeños.
- El umbral de supervisión es demasiado pequeño.

Procedimiento

Comprobar los recursos de NodeManager.

Paso 1 En FusionInsight Manager, elija **Cluster** > *Name of the desired cluster* > **Services** > **Yarn** > **ResourceManager (Active)** para acceder a la interfaz de usuario web de ResourceManager.

Paso 2 Haga clic en **Scheduler** y compruebe si los recursos de cola raíz se utilizan en **Application Queues**.

- En caso afirmativo, vaya a **Paso 3**.
- Si no, vaya a **Paso 4**.

Paso 3 Amplíe la capacidad de la instancia NodeManager del servicio Yarn. Después de la ampliación de la capacidad, compruebe si la alarma está desactivada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 6**.

Comprobar la capacidad máxima de recursos de la cola y el porcentaje máximo de recursos de AM.

Paso 4 Compruebe si los recursos de la cola correspondientes a la tarea pendiente están agotados.

- En caso afirmativo, vaya a **Paso 5**.
- Si no, vaya a **Paso 6**.

Paso 5 En FusionInsight Manager, elija **Tenant Resources** > **Dynamic Resource Plan** y agregue recursos según sea necesario. Compruebe si las alarmas están desactivadas.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 6**.

Ajustar los umbrales de monitoreo.

Paso 6 En FusionInsight Manager, elija **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster* > **Yarn** > **Applications** > **Pending Applications**, y aumente los umbrales según sea necesario.

Paso 7 Compruebe si la alarma se borra 5 minutos más tarde.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 8**.

Recopilar información de fallas.

Paso 8 En FusionInsight Manager, seleccione **O&M**. En el panel de navegación de la izquierda, elija **Log** > **Download**.

Paso 9 Expanda la lista desplegable **Service** y seleccione **Yarn** para el clúster de destino.

Paso 10 Haga clic en  en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 11 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

Información relacionada

Ninguna

9.149 ALM-18024 El uso de memoria de Yarn pendiente supera el umbral

Descripción

El módulo de alarma comprueba la memoria pendiente de Yarn cada 60 segundos. La alarma se genera cuando la memoria pendiente excede el umbral. La memoria pendiente indica la memoria total que no está asignada a las aplicaciones de Yarn enviadas.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
18024	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
QueueName	Identifica la cola para la que se genera la alarma.
QueueMetric	Identifica el indicador de cola para el que se genera la alarma.

Impacto en el sistema

- Se necesita mucho tiempo para finalizar una solicitud.
- Una nueva aplicación no se puede ejecutar después del envío.

Causas posibles

- Los recursos del nodo de NodeManager son insuficientes.
- La capacidad máxima de recursos de la cola y el porcentaje máximo de recursos de AM son demasiado pequeños.
- El umbral de supervisión es demasiado pequeño.

Procedimiento

Comprobar los recursos de NodeManager.

Paso 1 En FusionInsight Manager, elija **Cluster** > *Name of the desired cluster* > **Services** > **Yarn** > **ResourceManager (Active)** para acceder a la interfaz de usuario web de ResourceManager.

Paso 2 Haga clic en **Scheduler** y compruebe si los recursos de cola raíz se utilizan en **Application Queues**.

- En caso afirmativo, vaya a **Paso 3**.
- Si no, vaya a **Paso 4**.

Paso 3 Amplíe la capacidad de la instancia de NodeManager del servicio Yarn. Después de la ampliación de la capacidad, compruebe si la alarma está desactivada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 6**.

Comprobar la capacidad máxima de recursos de la cola y el porcentaje máximo de recursos de AM.

Paso 4 Compruebe si los recursos de la cola correspondientes a la tarea pendiente están agotados.

- En caso afirmativo, vaya a **Paso 5**.
- Si no, vaya a **Paso 6**.

Paso 5 En FusionInsight Manager, elija **Tenant Resources** > **Dynamic Resource Plan** y agregue recursos según sea necesario. Compruebe si las alarmas están desactivadas.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 6**.

Ajustar los umbrales de monitoreo.

Paso 6 En FusionInsight Manager, elija **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster* > **Yarn** > **CPU and Memory** > **Pending Memory**, y aumentar el umbral según sea necesario.

Paso 7 Compruebe si la alarma se borra 5 minutos más tarde.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 8**.

Recopilar información de fallas.

Paso 8 En FusionInsight Manager, seleccione **O&M**. En el panel de navegación de la izquierda, elija **Log** > **Download**.

Paso 9 Expanda la lista desplegable **Service** y seleccione **Yarn** para el clúster de destino.

Paso 10 Haga clic en  en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 11 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

Información relacionada

Ninguna

9.150 ALM-18025 El número de tareas de Yarn terminadas supera el umbral

Descripción

El módulo de alarma comprueba el número de aplicaciones terminadas en la cola raíz de Yarn cada 60 segundos. La alarma se genera cuando el número excede de 50 por tres veces consecutivas.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
18025	Importante	Sí

Parámetros

Nombre	Significado
Cluster Name	Especifica el clúster para el que se genera la alarma.
Service Name	Especifica el servicio para el que se genera la alarma.
Role Name	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger Condition	Especifica el umbral que activa la alarma. Si el valor del indicador actual excede este umbral, se genera la alarma.

Impacto en el sistema

Un gran número de tareas de aplicación se terminan por la fuerza.

Causas posibles

- El usuario termina por la fuerza un gran número de tareas.
- El sistema termina las tareas debido a algún error.

Procedimiento

Comprobar detalles de la alarma.

Paso 1 En el portal del FusionInsight Manager, seleccione **O&M > Alarm > Alarms** para ir a la página de alarma.

Paso 2 Vea **Additional Information** en los detalles de la alarma para comprobar si el umbral de alarma es demasiado pequeño.

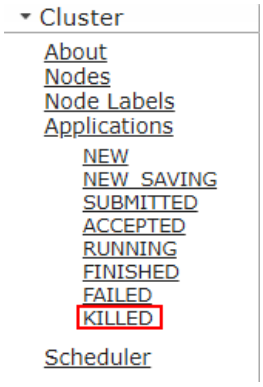
- En caso afirmativo, vaya a **Paso 3**.
- Si no, vaya a **Paso 4**.

Paso 3 Elija **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster* > **Yarn** > **Other** > **Terminated Applications of root queue** para modificar el umbral. Vaya a **Paso 6**.

Paso 4 Elija **Cluster** > *Name of the desired cluster* > **Services** > **Yarn** > **ResourceManager(Active)** para acceder a la interfaz de usuario web ResourceManager.

Paso 5 Haga clic en **KILLED** en **Applications** y haga clic en la tarea en la parte superior. Vea la descripción de **Diagnostics** y rectifique el error basándose en los detalles de terminación de la tarea (por ejemplo, la tarea es terminada por un usuario).

Figura 9-49 Haga clic en **KILLED**



Paso 6 Espere 3 minutos y compruebe si la alarma está desactivada.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 7**.

Recopilar información de fallas.

Paso 7 En el FusionInsight Manager, seleccione **O&M > Log > Download**.

Paso 8 Expanda la lista desplegable **Service** y seleccione **Yarn** para el clúster de destino.

Paso 9 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 10 Póngase en contacto con el y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.151 ALM-18026 El número de tareas de Yarn fallidas supera el umbral

Descripción

El módulo de alarma comprueba el número de aplicaciones fallidas en la cola de Yarn root cada 60 segundos. La alarma se genera cuando el número excede de 50 por tres veces consecutivas.

Atributo

ID de alarma	Gravedad de la alarma	Borrado automático
18026	Importante	Sí

Parámetros

Nombre	Significado
Cluster Name	Especifica el clúster para el que se genera la alarma.
Service Name	Especifica el servicio para el que se genera la alarma.
Role Name	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger Condition	Especifica el umbral que activa la alarma. Si el valor del indicador actual excede este umbral, se genera la alarma.

Impacto en el sistema

- No se puede ejecutar un gran número de tareas de aplicación.
- Las tareas fallidas deben enviarse de nuevo.

Causas posibles

La tarea no se puede ejecutar debido a algún error.

Procedimiento

Comprobar detalles de la alarma.

Paso 1 En el portal del administrador de FusionInsight, seleccione **O&M > Alarm > Alarms** para ir a la página de alarma.

Paso 2 Vea **Additional Information** en los detalles de la alarma para comprobar si el umbral de alarma es demasiado pequeño.

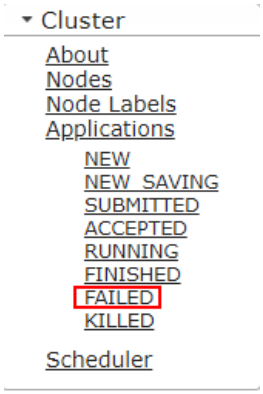
- En caso afirmativo, vaya a **Paso 3**.
- Si no, vaya a **Paso 4**.

Paso 3 Elija **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster* > **Yarn** > **Other** > **Failed Applications of root queue** para modificar el umbral. Vaya a **Paso 6**.

Paso 4 Elija **Cluster** > *Name of the desired cluster* > **Services** > **Yarn** > **ResourceManager(Active)** para acceder a la interfaz de usuario web ResourceManager.

Paso 5 Haga clic en **FAILED** en **Applications** y haga clic en la tarea en la parte superior. Vea la descripción de **Diagnostics** y rectifique el error basándose en las causas del error de la tarea.

Figura 9-50 Haga clic en **FAILED**



Paso 6 Espere 3 minutos y compruebe si la alarma está desactivada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 7**.

Recopilar información de fallas.

Paso 7 En el FusionInsight Manager, seleccione O&M > Log > Download.

Paso 8 Expanda la lista desplegable **Service** y seleccione **Yarn** para el clúster de destino.

Paso 9 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 10 Póngase en contacto con el y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.152 ALM-19000 Servicio HBase no disponible

Descripción

El módulo de alarma comprueba el estado del servicio HBase cada 120 segundos. Esta alarma se genera cuando el servicio HBase no está disponible.

Esta alarma se borra cuando se recupera el servicio HBase.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
19000	Crítica	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

No se pueden realizar operaciones como la lectura/escritura de datos y la creación de tablas.

Causas posibles

- ZooKeeper es anormal.
- HDFS es anormal.
- HBase es anormal.
- La conexión de red es anormal.
- El valor de configuración del servicio es incorrecto.

Procedimiento

Verificar el estado del servicio de ZooKeeper.

Paso 1 En la lista de servicios en el FusionInsight Manager, compruebe si **Running Status** de ZooKeeper es **Normal**.

- En caso afirmativo, vaya a **Paso 5**.
- Si no, vaya a **Paso 2**.

Paso 2 En la lista de alarmas, compruebe si existe **ALM-13000 Servicio ZooKeeper no disponible**.

- En caso afirmativo, vaya a **Paso 3**.
- Si no, vaya a **Paso 5**.

Paso 3 Rectificar la falla mediante la realización de las operaciones previstas para **ALM-13000 Servicio ZooKeeper no disponible**.

Paso 4 Espere varios minutos y compruebe si la alarma está desactivada.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 5**.

Comprobar el estado de servicio HDFS.

Paso 5 En la lista de alarmas, compruebe si existe **ALM-14000 Servicio HDFS no disponible**.

- En caso afirmativo, vaya a **Paso 6**.
- Si no, vaya a **Paso 8**.

Paso 6 Rectificar la falla mediante la realización de las operaciones previstas para **ALM-14000 Servicio HDFS no disponible**.

Paso 7 Espere varios minutos y compruebe si la alarma está desactivada.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 8**.

Paso 8 En FusionInsight Manager, elija **Cluster**, haga clic en el nombre del clúster deseado, elija **Services** > **HDFS** y compruebe si **Safe Mode** de HDFS es **ON**.

- En caso afirmativo, vaya a **Paso 9**.
- Si no, vaya a **Paso 12**.

Paso 9 Inicie sesión en el cliente HDFS como usuario **root**. Ejecute el comando **cd** para ir al directorio de instalación del cliente y ejecute el comando **source bigdata_env**.

Si el clúster utiliza el modo de seguridad, realice la autenticación de seguridad. Obtenga la contraseña del usuario **hdfs** del administrador del clúster MRS, ejecute el comando **kinit hdfs** e introduzca la contraseña como se le solicite.

Paso 10 Ejecute el siguiente comando para salir manualmente del modo seguro:

hdfs dfsadmin -safemode leave

Paso 11 Espere varios minutos y compruebe si la alarma está desactivada.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 12**.

Comprobar el estado de servicio de HBase.

Paso 12 En FusionInsight Manager, elija **Cluster**, haga clic en el nombre del clúster deseado y elija **Services** > **HBase**.

Paso 13 Compruebe si hay un HMaster activo y un HMaster en espera.

- En caso afirmativo, vaya a **Paso 15**.
- Si no, vaya a **Paso 14**.

Paso 14 Haga clic en **Instances** y seleccione la instancia de HMaster cuyo estado no sea **Active**. Haga clic en **More** y seleccione **Restart Instance** para reiniciar HMaster. A continuación, compruebe si hay un HMaster activo y un HMaster en espera.

- En caso afirmativo, vaya a **Paso 15**.
- Si no, vaya a **Paso 21**.

Paso 15 Elija **Cluster**, haga clic en el nombre del clúster deseado, elija **Services** > **HBase** y haga clic en **HMaster(Active)** para acceder a la interfaz de usuario web de HMaster.

NOTA

De forma predeterminada, el usuario **admin** no tiene los permisos para gestionar otros componentes. Si la página no se puede abrir o el contenido mostrado está incompleto al acceder a la interfaz de usuario nativa de un componente debido a la falta de permisos, puede crear manualmente un usuario con los permisos para gestionar ese componente.

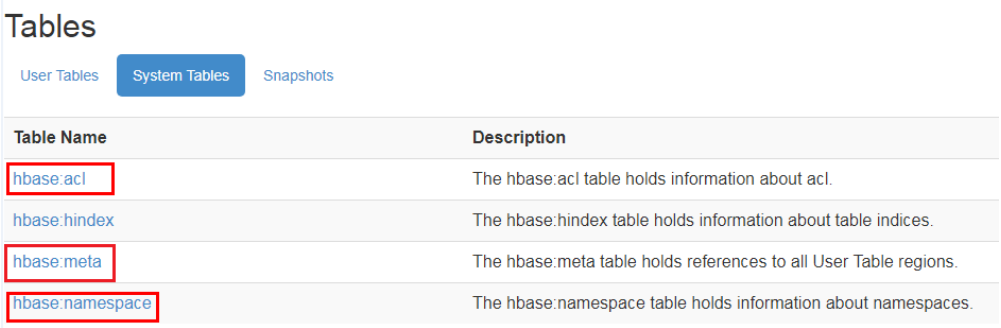
Paso 16 Comprueba si existe al menos un RegionServer en **Region Servers**.

- En caso afirmativo, vaya a **Paso 17**.
- Si no, vaya a **Paso 21**.

Paso 17 Elija **Tables** > **System Tables** y compruebe si **hbase:meta**, **hbase:namespace** y **hbase:acl** existen en la columna **Table Name** como se muestra en **Figura 9-51**.

- En caso afirmativo, vaya a **Paso 18**.
- Si no, vaya a **Paso 19**.

Figura 9-51 Tablas del sistema de HBase



Paso 18 Haga clic en **hbase:meta**, **hbase:namespace** y **hbase:acl** para comprobar si se pueden abrir todas las páginas. Si todos ellos se pueden abrir, las tablas son normales.

- En caso afirmativo, vaya a **Paso 19**.
- Si no, vaya a **Paso 25**.

NOTA

En un clúster normal, el control de permisos de ACL está deshabilitado para HBase de forma predeterminada. La tabla **hbase:acl** se genera solo después de que el control de permisos de ACL esté habilitado manualmente. En este caso, debe comprobar esta tabla.

Paso 19 Vea el estado de inicio de HMaster.

En la página **Tasks** mostrada en **Figura 9-52**, el valor **RUNNING** de la columna **State** indica que HMaster se está iniciando y proporciona cuánto tiempo HMaster permanece en ese estado. Como se muestra en **Figura 9-53**, si el estado es **COMPLETE**, se ha iniciado HMaster.

Compruebe si HMaster ha estado en el estado **RUNNING** durante mucho tiempo.

Figura 9-52 HMaster que se está iniciando

Figura 9-53 Inicio de HMaster completado

- En caso afirmativo, vaya a **Paso 20**.
- Si no, vaya a **Paso 21**.

Paso 20 En la interfaz de usuario web de HMaster, compruebe si algún **hbase:meta** está en el estado **Regions in Transition** durante mucho tiempo.

Figura 9-54 Regiones en transición

- En caso afirmativo, vaya a **Paso 21**.
- Si no, vaya a **Paso 22**.

Paso 21 Después de asegurarse de que los servicios no se ven afectados, inicie sesión en el FusionInsight Manager, elija **Cluster**, haga clic en el nombre del clúster deseado, elija **Services** > **HBase**, haga clic en **More** y seleccione **Restart Service**. En el cuadro de diálogo que se muestra, escriba la contraseña y haga clic en **OK**.

- En caso afirmativo, vaya a **Paso 22**.
- Si no, vaya a **Paso 25**.

Paso 22 Espere varios minutos y compruebe si la alarma está desactivada.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 25**.

Compruebe si las configuraciones de HBase están correctamente modificadas.

Paso 23 En FusionInsight Manager, seleccione **Audit**. En la página **Audit**, haga clic en **Advanced Search**, haga clic en ··· a la derecha de **Operation Type**, seleccione **Save configuration**, haga clic en **OK** y haga clic en **Search**.

Paso 24 En el resultado de la búsqueda, compruebe si las configuraciones históricas de los servicios relacionados con HBase en la columna **Service**, como ZooKeeper, HDFS y HBase, pueden afectar al estado del servicio HBase. **Tabla 9-5** enumera algunas configuraciones que pueden afectar al estado del servicio HBase.

Tabla 9-5 Configuraciones que afectan al estado del servicio HBase

Parámetro	Impacto posible
GC_OPTS	La configuración de la memoria puede ser incorrecta. Debe comprobar el estado de salud de los procesos de instancia.
hbase.rpc.protection	Si el servicio HBase no se reinicia sin conexión después de cambiar el valor de este parámetro, la autenticación de conexión falla y el servicio HBase se vuelve anormal.
hbase.regionserver.metahandler.count	Si hay demasiadas regiones en el clúster pero este parámetro se establece en un valor pequeño, RIT puede ocurrir y las regiones no se pueden poner en línea durante mucho tiempo.
hbase.regionserver.thread.compaction.large	Si este parámetro se establece en un valor grande, el uso de la CPU del nodo puede ser demasiado alto.
hbase.regionserver.thread.compaction.small	Si este parámetro se establece en un valor grande, el uso de la CPU del nodo puede ser demasiado alto.
hbase.coprocessor.master.classes	Si se utiliza un coprocesador personalizado en la configuración, un error lógico puede hacer que el servicio no esté disponible.
hbase.coprocessor.region.classes	Si se utiliza un coprocesador personalizado en la configuración, un error lógico puede hacer que el servicio no esté disponible.
hbase.coprocessor.regionserver.classes	Si se utiliza un coprocesador personalizado en la configuración, un error lógico puede hacer que el servicio no esté disponible.
zookeeper.session.timeout	Si este parámetro se establece en un valor pequeño, la conexión entre HBase y ZooKeeper se agota demasiado rápido. Como resultado, la instancia HMaster y el RegionServer pueden reiniciarse repetidamente.

Compruebe la conexión de red entre HMaster y los componentes dependientes.

Paso 25 En FusionInsight Manager, elija **Cluster**, haga clic en el nombre del clúster deseado y elija **Services** > **HBase**.

Paso 26 Haga clic en **Instances**. En la lista de instancias de HMaster, registre la dirección IP de gestión de la instancia de HMaster activa.

Paso 27 Inicie sesión en el nodo HMaster activo como usuario **omm** a través de la dirección IP obtenida en **Paso 26**.

Paso 28 Ejecute el comando **ping** para comprobar si la conexión de red entre el nodo HMaster activo y el host donde residen los componentes dependientes es normal. (Los componentes

dependientes incluyen ZooKeeper, HDFS, y Yarn. El método para obtener la dirección IP del host donde residen los componentes dependientes es el mismo que el de obtener la dirección IP del nodo HMaster activo.)

- En caso afirmativo, vaya a **Paso 31**.
- Si no, vaya a **Paso 29**.

Paso 29 Póngase en contacto con el administrador de red para restaurar la red.

Paso 30 En la lista de alarmas, compruebe si esta alarma está borrada.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 31**.

Recopilar información de fallas.

Paso 31 En FusionInsight Manager, seleccione **O&M**. En el panel de navegación de la izquierda, elija **Log** > **Download**.

Paso 32 Expanda la lista desplegable junto al campo **Service**. En el cuadro de diálogo **Services** que se muestra, seleccione los siguientes servicios para el clúster de destino:

- ZooKeeper
- HDFS
- HBase

Paso 33 Haga clic en  en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 34 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

Información relacionada

Ninguna

9.153 ALM-19006 Error de sincronización de replicación de HBase

Descripción

El módulo de alarma comprueba el estado de sincronización de datos HBase DR cada 30 segundos. Cuando los datos de recuperación ante desastres (DR) no se sincronizan con un clúster en espera, se activa la alarma.

Cuando la sincronización de datos de DR tiene éxito, la alarma se borra.

Atributo

ID de alarma	Gravedad de la alarma	Borrado automáticamente
19006	Crítica	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger Condition	Especifica el umbral que activa la alarma. Si el valor del indicador actual excede este umbral, se genera la alarma.

Impacto en el sistema

Los datos de HBase en un clúster no se sincronizan con el clúster en espera, lo que provoca incoherencia de datos entre los clústeres activo y en espera.

Causas posibles

- El servicio HBase en el clúster en espera es anormal.
- Se produce una excepción de red.

Procedimiento

Observar si el sistema borra automáticamente la alarma.

Paso 1 En el portal de FusionInsight Manager del clúster activo, haga clic en **O&M** > **Alarm** > **Alarms.**

Paso 2 En la lista de alarmas, haga clic en la alarma para obtener el tiempo de generación de alarma a partir del **Generated** de la alarma. Compruebe si la alarma ha existido durante cinco minutos.

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 3**.

Paso 3 Espere cinco minutos y compruebe si el sistema borra automáticamente la alarma.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 4**.

Verificar el estado del servicio HBase del clúster en espera.

Paso 4 Inicie sesión en el portal del FusionInsight Manager del clúster activo y haga clic en **O&M** > **Alarm** > **Alarms.**

Paso 5 En la lista de alarmas, haga clic en la alarma para obtener **HostName** de **Location**.

Paso 6 Acceda al nodo donde reside el cliente HBase del clúster activo como usuario **omm**.

Si el clúster utiliza un modo de seguridad, realice primero la autenticación de seguridad y, a continuación, acceda a la interfaz **hbase shell** como usuario **hbase**.

cd /opt/client

source ./bigdata_env

kinit *hbaseuser*

Paso 7 Ejecute el comando **status 'replication', 'source'** para comprobar el estado de sincronización de DR del nodo defectuoso.

El estado de sincronización de DR de un nodo es el siguiente.

```
10-10-10-153:
SOURCE: PeerID=abc, SizeOfLogQueue=0, ShippedBatches=2, ShippedOps=2,
ShippedBytes=320, LogReadInBytes=1636, LogEditsRead=5, LogEditsFiltered=3,
SizeOfLogToReplicate=0, TimeForLogToReplicate=0, ShippedHFiles=0,
SizeOfHFileRefsQueue=0, AgeOfLastShippedOp=0, TimeStampsOfLastShippedOp=Mon Jul
18 09:53:28 CST 2016, Replication Lag=0, FailedReplicationAttempts=0
SOURCE: PeerID=abc1, SizeOfLogQueue=0, ShippedBatches=1, ShippedOps=1,
ShippedBytes=160, LogReadInBytes=1636, LogEditsRead=5, LogEditsFiltered=3,
SizeOfLogToReplicate=0, TimeForLogToReplicate=0, ShippedHFiles=0,
SizeOfHFileRefsQueue=0, AgeOfLastShippedOp=16788, TimeStampsOfLastShippedOp=Sat
Jul 16 13:19:00 CST 2016, Replication Lag=16788, FailedReplicationAttempts=5
```

Paso 8 Obtenga **PeerID** correspondiente a un registro cuyo valor **FailedReplicationAttempts** es mayor que 0.

En la etapa anterior, los datos en el nodo 10-10-10-153 defectuoso no se sincronizan con un grupo de reserva cuyo **PeerID** es de **abc1**.

Paso 9 Ejecute el comando **list_peers** para encontrar el clúster y la instancia HBase correspondiente al valor **PeerID**.

```
PEER_ID CLUSTER_KEY STATE TABLE_CFS
abc1 10.10.10.110,10.10.10.119,10.10.10.133:2181:/hbase2 ENABLED
abc 10.10.10.110,10.10.10.119,10.10.10.133:2181:/hbase ENABLED
```

En la información anterior, **/hbase2** indica que los datos están sincronizados con la instancia HBase2 del clúster en espera.

Paso 10 En la lista de servicios del FusionInsight Manager del clúster en espera, compruebe si el estado de ejecución de la instancia de HBase obtenida mediante **Paso 9** es de **Normal**.

- En caso afirmativo, vaya a **Paso 14**.
- Si no, vaya a **Paso 11**.

Paso 11 En la lista de alarmas, compruebe si se genera la alarma **ALM-19000 Servicio HBase no disponible**.

- En caso afirmativo, vaya a **Paso 12**.

- Si no, vaya a **Paso 14**.

Paso 12 Siga los procedimientos de solución de problemas de **ALM-19000 Servicio HBase no disponible** para corregir el fallo.

Paso 13 Espere unos minutos y compruebe si la alarma está desactivada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 14**.

Verificar las conexiones de red entre RegionServers en clústeres activos y en espera.

Paso 14 Inicie sesión en el portal del FusionInsight Manager del clúster activo y haga clic en **O&M** > **Alarm** > **Alarms.**

Paso 15 En la lista de alarmas, haga clic en la alarma para obtener **HostName** de **Location**.

Paso 16 Utilice la dirección IP obtenida en **Paso 15** para iniciar sesión en un nodo RegionServer defectuoso como usuario **omm**.

Paso 17 Ejecute el comando **ping** para comprobar si las conexiones de red entre el nodo RegionServer defectuoso y el host donde reside el RegionServer del clúster en espera están en el estado normal.

- En caso afirmativo, vaya a **Paso 20**.
- Si no, vaya a **Paso 18**.

Paso 18 Póngase en contacto con el administrador de red para restaurar la red.

Paso 19 Después de que la red esté funcionando correctamente, compruebe si la alarma está borrada en la lista de alarmas.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 20**.

Recopilar información de fallas.

Paso 20 En la interfaz del FusionInsight Manager de los clústeres activos y en espera, seleccione **O&M** > **Log** > **Download**.

Paso 21 En el cuadro de lista desplegable **Service**, seleccione **HBase** en el clúster requerido.

Paso 22 Haga clic en  en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 23 Póngase en contacto con el y envíe los registros de fallas recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.154 ALM-19007 El tiempo de HBase GC supera el umbral

Descripción

El sistema comprueba el tiempo de recolección de basura (GC) de generación anterior del servicio HBase cada 60 segundos. Esta alarma se genera cuando el tiempo GC de generación antigua detectado excede el umbral (excede 5 segundos durante tres comprobaciones consecutivas por defecto). Para cambiar el umbral, en el portal del Administrador FusionInsight, elija **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster* > **HBase > GC > GC time for old generation**. Esta alarma se borra cuando el tiempo GC de generación antigua del servicio HBase es más corto o igual que el umbral.

Atributo

ID de alarma	Gravedad de la alarma	Borrado automáticamente
19007	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el nombre del servicio para el que se genera la alarma.
RoleName	Especifica el nombre del rol para el que se genera la alarma.
HostName	Especifica el objeto (ID de host) para el que se genera la alarma.

Impacto en el sistema

Si el tiempo de GC de generación antigua excede el umbral, la lectura y escritura de datos de HBase se ven afectadas.

Causas posibles

La memoria de las instancias de HBase se utiliza en exceso, la memoria heap se asigna de forma inapropiada o existe un gran número de operaciones de E/S en HBase. Como resultado, los GC ocurren con frecuencia.

Procedimiento

Comprobar el tiempo de GC.

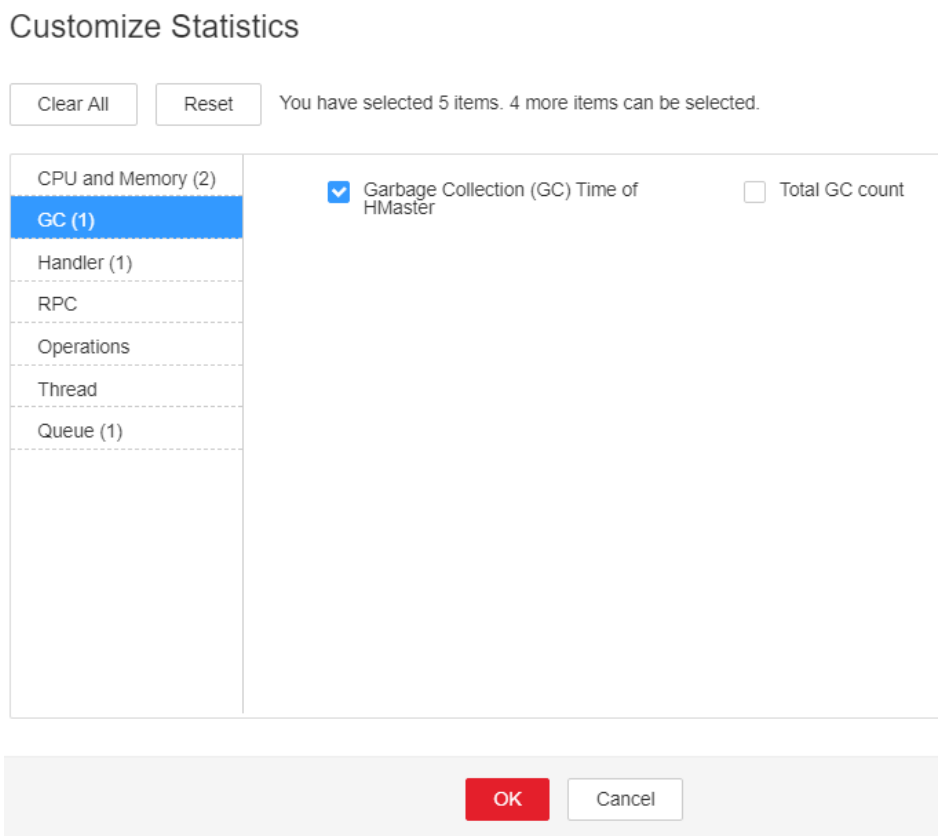
Paso 1 En el portal del FusionInsight Manager, haga clic en **O&M** > **Alarm** > **Alarms** y seleccione la alarma cuyo **ID** es **19007**. A continuación, compruebe el nombre del rol de **Location** y confirme la dirección IP de la instancia.

- Si el rol para el que se genera la alarma es HMaster, vaya a **Paso 2**.
- Si el rol para el que se genera la alarma es "RegionServer", vaya a **Paso 3**.

Paso 2 En el portal del FusionInsight Manager, elija **Cluster** > *Name of the desired cluster* > **Services** > **HBase** > **Instance** y haga clic en el HMaster para el que se genera la alarma para ir a la página **Dashboard**. Haga clic en el menú desplegable en el área **Chart** y elija **Customize** > **GC** > **Garbage Collection (GC) Time of HMaster** y haga clic en **OK** para comprobar si el valor de **GC time for old generation** es mayor que el umbral (excede 5 segundos por tres periodos de comprobación consecutivos de forma predeterminada).

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 6**.

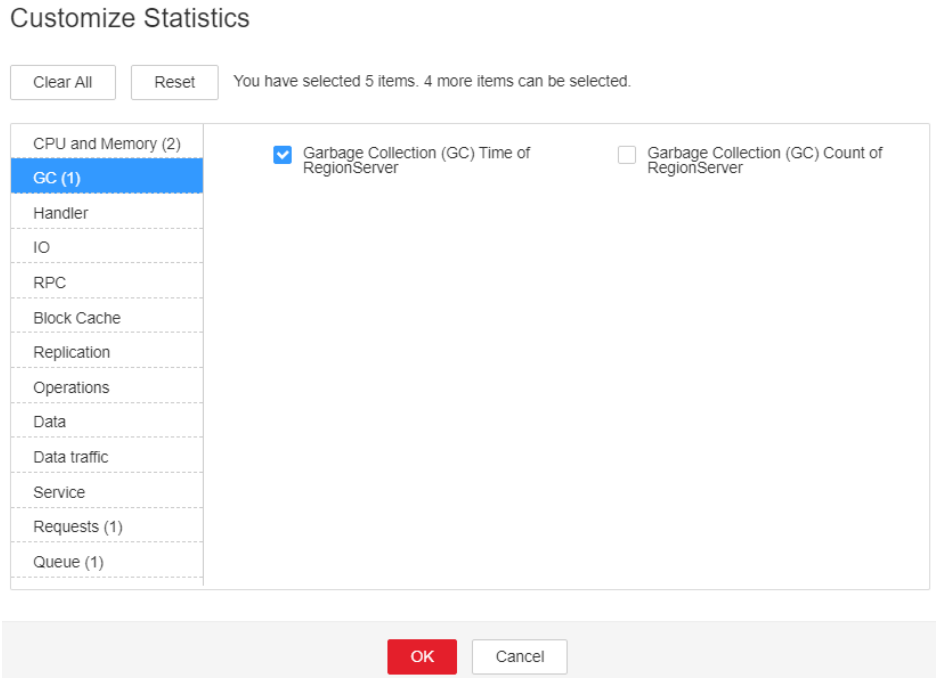
Figura 9-55 Tiempo de Recolección de basura (GC) de HMaster



Paso 3 En el portal del FusionInsight Manager, elija **Cluster** > *Name of the desired cluster* > **Services** > **HBase** > **Instance** y haga clic en el RegionServer para el que se genera la alarma para ir a la página **Dashboard**. Haga clic en el menú desplegable en el área **Chart** y elija **Customize** > **GC** > **Garbage Collection (GC) Time of RegionServer** y haga clic en **OK** para comprobar si el valor de **GC time for old generation** es mayor que el umbral (excede 5 segundos por tres periodos de comprobación consecutivos de forma predeterminada).

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 6**.

Figura 9-56 Tiempo de Recolección de basura (GC) de RegionServer



Comprobar la configuración de JVM actual.

Paso 4 En el portal de FusionInsight Manager, elija **Cluster** > *Name of the desired cluster* > **Services** > **HBase** > **Configurations** y haga clic en **All Configurations**. En Search, introduzca **GC_OPTS** para comprobar el parámetro de memoria **GC_OPTS** del rol HMaster(HBase->HMaster), RegionServer (HBase->RegionServer). Ajuste los valores de **-Xmx** y **-XX:CMSInitiatingOccupancyFraction** del parámetro GC_OPTS haciendo referencia a la Nota.

NOTA

1. Sugerencias sobre configuraciones de parámetros de GC para HMaster
   - Establezca **-Xms** y **-Xmx** en el mismo valor para evitar que JVM ajuste dinámicamente el tamaño de memoria heap y afecte al rendimiento.
   - Establezca **-XX:NewSize** en el valor de **-XX:MaxNewSize**, que es un octavo de **-Xmx**.
   - Para clústeres HBase a gran escala con un gran número de regiones, aumente los valores de los parámetros **GC_OPTS** para HMaster. Específicamente, establezca **-Xmx** en 4 GB si el número de regiones es inferior a 100,000. Si el número de regiones es superior a 100,000, establezca -Xmx para que sea superior o igual a 6 GB. Para cada región de 35,000 aumentada, aumente el valor de **-Xmx** en 2 GB. El valor máximo de **-Xmx** es 32 GB.
2. Sugerencias sobre configuraciones de parámetros de GC para RegionServer
   - Establezca **-Xms** y **-Xmx** en el mismo valor para evitar que JVM ajuste dinámicamente el tamaño de memoria heap y afecte al rendimiento.
   - Ajusta **-XX:NewSize** a un octavo de **-Xmx**.
   - Establezca la memoria de RegionServer para que sea mayor que la de HMaster. Si hay suficiente memoria disponible, aumente la memoria heap.
   - Establezca **-Xmx** según el tamaño de la memoria de la máquina. Específicamente, establezca **-Xmx** en 32 GB si la memoria del equipo es mayor que 200 GB, en 16 GB si la memoria del equipo es mayor que 128 GB y menor que 200 GB, y en 8 GB si la memoria del equipo es menor que 128 GB. Cuando **-Xmx** se establece en 32 GB, un nodo de RegionServer admite 2000 regiones y 200 regiones de hotspot.
   - **XX:CMSInitiatingOccupancyFraction** es menor e igual a **85** y se calcula de la siguiente manera: 100 x (hfile.block.cache.size + hbase.regionserver.global.memstore.size)

Paso 5 Verifique si la alarma se ha borrado.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 6**.

Recopilar información de fallas.

Paso 6 En la interfaz del FusionInsight Manager de los clústeres activos y en espera, seleccione **O&M** > **Log** > **Download**.

Paso 7 En el cuadro de lista desplegable **Service**, seleccione **HBase** en el clúster requerido.

Paso 8 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 9 Póngase en contacto con el y envíe los registros de fallas recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.155 ALM-19008 El uso de memoria heap del proceso HBase supera el umbral

Descripción

El sistema comprueba el estado del servicio HBase cada 30 segundos. La alarma se genera cuando el uso de memoria heap de un servicio HBase excede el umbral (90% de la memoria máxima).

Atributo

ID de alarma	Gravedad de la alarma	Borrado automáticamente
19008	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el nombre del servicio para el que se genera la alarma.
RoleName	Especifica el nombre del rol para el que se genera la alarma.
HostName	Especifica el objeto (ID de host) para el que se genera la alarma.

Impacto en el sistema

Si la memoria de heap de HBase disponible es insuficiente, se produce un desbordamiento de memoria y el servicio se interrumpe.

Causas posibles

La memoria heap del servicio HBase se utiliza en exceso o la memoria heap se asigna de forma inadecuada.

Procedimiento

Comprobar el uso de memoria heap.

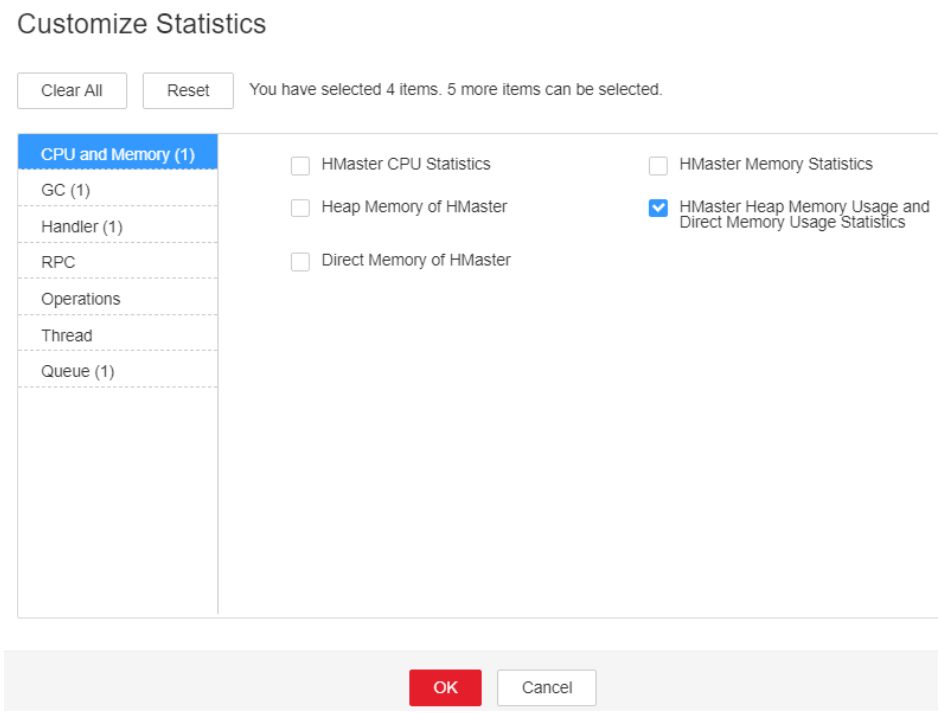
Paso 1 En el portal del FusionInsight Manager, haga clic en **O&M** > **Alarm** > **Alarms** y seleccione la alarma cuyo **ID** es **19008**. A continuación, compruebe el nombre del rol de **Location** y confirme la dirección IP de la instancia.

- Si el rol para el que se genera la alarma es HMaster, vaya a **Paso 2**.
- Si el rol para el que se genera la alarma es "RegionServer", vaya a **Paso 3**.

Paso 2 En el portal del FusionInsight Manager, elija **Cluster** > *Name of the desired cluster* > **Services** > **HBase** > **Instance** y haga clic en el HMaster para el que se genera la alarma para ir a la página **Dashboard**. Haga clic en el menú desplegable en el área **Chart** y elija **Customize** > **CPU and Memory** > **HMaster Heap Memory Usage and Direct Memory Usage Statistics** y haga clic en **OK** y compruebe si la memoria heap usada del servicio HBase alcanza el 90% de la memoria heap máxima especificada para HBase.

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 6**.

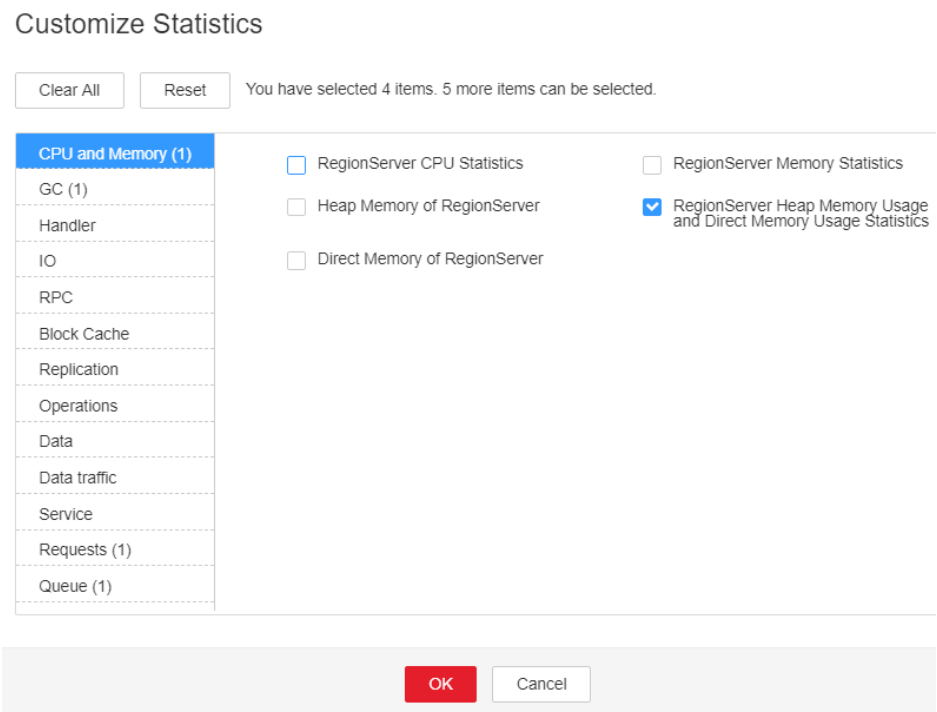
Figura 9-57 Estadísticas de uso de memoria heap de HMaster y uso de memoria directa



Paso 3 En el portal del FusionInsight Manager, elija **Cluster** > *Name of the desired cluster* > **Services** > **HBase** > **Instance** y haga clic en el RegionServer para el que se genera la alarma para ir a la página **Dashboard**. Haga clic en el menú desplegable en el área **Chart** y elija **Customize** > **CPU and Memory** > **RegionServer Heap Memory Usage and Direct Memory Usage Statistics** y haga clic en **OK** y compruebe si la memoria heap usada del servicio HBase alcanza el 90% de la memoria heap máxima especificada para HBase.

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 6**.

Figura 9-58 Estadísiticas de uso de memoria heap de RegionServer y uso de memoria directa



Paso 4 En el portal de FusionInsight Manager, elija **Cluster** > *Name of the desired cluster* > **Services** > **HBase** > **Configurations** y haga clic en **All Configurations**. Elija **HMaster/RegionServer** > **System**. Aumente el valor de **-Xmx** en **GC_OPTS** haciendo referencia a la Nota.

NOTA

1. Sugerencias sobre configuraciones de parámetros de GC para HMaster
   - Establezca **-Xms** y **-Xmx** en el mismo valor para evitar que JVM ajuste dinámicamente el tamaño de memoria heap y afecte al rendimiento.
   - Establezca **-XX:NewSize** en el valor de **-XX:MaxNewSize**, que es un octavo de **-Xmx**.
   - Para clústeres HBase a gran escala con un gran número de regiones, aumente los valores de los parámetros **GC_OPTS** para HMaster. Específicamente, establezca **-Xmx** en 4 GB si el número de regiones es inferior a 100,000. Si el número de regiones es superior a 100,000, establezca -Xmx para que sea superior o igual a 6 GB. Para cada región de 35,000 aumentada, aumente el valor de **-Xmx** en 2 GB. El valor máximo de **-Xmx** es 32 GB.
2. Sugerencias sobre configuraciones de parámetros de GC para RegionServer
   - Establezca **-Xms** y **-Xmx** en el mismo valor para evitar que JVM ajuste dinámicamente el tamaño de memoria heap y afecte al rendimiento.
   - Ajusta **-XX:NewSize** a un octavo de **-Xmx**.
   - Establezca la memoria de RegionServer para que sea mayor que la de HMaster. Si hay suficiente memoria disponible, aumente la memoria heap.
   - Establezca **-Xmx** según el tamaño de la memoria de la máquina. Específicamente, establezca **-Xmx** en 32 GB si la memoria del equipo es mayor que 200 GB, en 16 GB si la memoria del equipo es mayor que 128 GB y menor que 200 GB, y en 8 GB si la memoria del equipo es menor que 128 GB. Cuando **-Xmx** se establece en 32 GB, un nodo de RegionServer admite 2000 regiones y 200 regiones de hotspot.

Paso 5 Verifique si la alarma se ha borrado.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 6**.

Recopilar información de fallas.

Paso 6 En el portal del FusionInsight Manager, seleccione **O&M** > **Log** > **Download**.

Paso 7 Seleccione **HBase** en el clúster requerido en la lista desplegable **Service**.

Paso 8 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 9 Póngase en contacto con el y envíe los registros de fallas recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.156 ALM-19009 El uso de memoria directa del proceso HBase supera el umbral

Descripción

El sistema comprueba el estado del servicio HBase cada 30 segundos. La alarma se genera cuando el uso de memoria directa de un servicio HBase supera el umbral (90% de la memoria máxima).

La alarma se borra cuando el uso directo de memoria es menor que el umbral.

Atributo

ID de alarma	Gravedad de la alarma	Borrado automáticamente
19009	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el nombre del servicio para el que se genera la alarma.

Nombre	Significado
RoleName	Especifica el nombre del rol para el que se genera la alarma.
HostName	Especifica el objeto (ID de host) para el que se genera la alarma.

Impacto en el sistema

Si la memoria directa HBase disponible es insuficiente, se produce un desbordamiento de memoria y el servicio se interrumpe.

Causas posibles

La memoria directa del servicio HBase se utiliza en exceso o la memoria directa se asigna de forma inapropiada.

Procedimiento

Comprobar el uso de memoria directa.

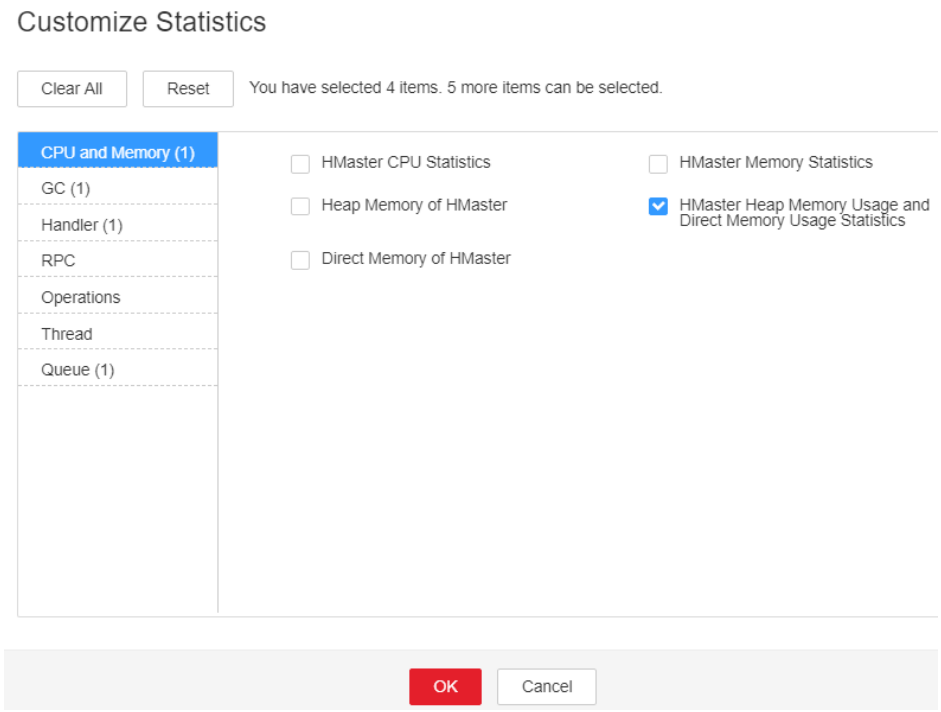
Paso 1 En el portal del FusionInsight Manager, haga clic en **O&M** > **Alarm** > **Alarms** y seleccione la alarma cuyo **ID** es **19009**. Compruebe el **RoleName** en **Location** y confirme la dirección IP de **HostName**.

- Si el rol para el que se genera la alarma es HMaster, vaya a **Paso 2**.
- Si el rol para el que se genera la alarma es "RegionServer", vaya a **Paso 3**.

Paso 2 En el portal del FusionInsight Manager, elija **Cluster** > *Name of the desired cluster* > **Services** > **HBase** > **Instance** y haga clic en el HMaster para el que se genera la alarma para ir a la página **Dashboard**. Haga clic en el menú desplegable en el área **Chart** y elija **Customize** > **CPU and Memory** > **HMaster Heap Memory Usage and Direct Memory Usage Statistics** y haga clic en **OK** para comprobar si la memoria directa utilizada del servicio HBase alcanza el 90% de la memoria directa máxima especificada para HBase.

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 8**.

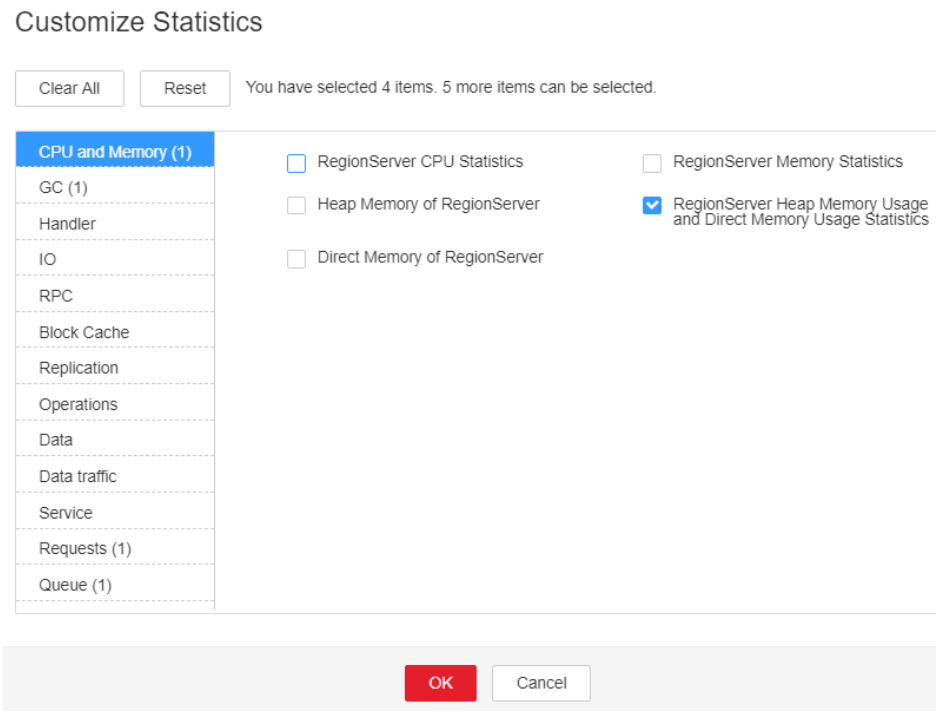
Figura 9-59 Estadísticas de uso de memoria heap de HMaster y uso de memoria directa



Paso 3 En el portal del FusionInsight Manager, elija **Cluster** > *Name of the desired cluster* > **Services** > **HBase** > **Instance** y haga clic en el RegionServer para el que se genera la alarma para ir a la página **Dashboard**. Haga clic en el menú desplegable en el área **Chart** y elija **Customize** > **CPU and Memory** > **RegionServer Heap Memory Usage and Direct Memory Usage Statistics** y haga clic en **OK** para comprobar si la memoria directa utilizada del servicio HBase alcanza el 90% de la memoria directa máxima especificada para HBase.

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 8**.

Figura 9-60 Estadísiticas de uso de memoria heap de RegionServer y uso de memoria directa



Paso 4 En el portal de FusionInsight Manager, elija **Cluster** > *Name of the desired cluster* > **Services** > **HBase** > **Configurations** y haga clic en **All Configurations**. Seleccione **HMaster/RegionServer** > **System** y compruebe si **XX:MaxDirectMemorySize** existe en **GC_OPTS**.

- En caso afirmativo, vaya a **Paso 5**.
- Si no, vaya a **Paso 6**.

Paso 5 En el portal del FusionInsight Manager, elija **Cluster** > *Nameof the desired cluster* > **Services** > **HBase** > **Configurations**, y haga clic en **All Configurations**. Elija **HMaster/RegionServer** > **System** y elimine **XX:MaxDirectMemorySize** de **GC_OPTS**.

Paso 6 Compruebe si se genera la alarma **ALM-19008 El uso de memoria heap del proceso HBase supera el umbral**.

En caso afirmativo, maneje la alarma haciendo referencia a **ALM-19008 El uso de memoria heap del proceso HBase supera el umbral**.

Si no, vaya a **Paso 8**.

Paso 7 Verifique si la alarma se ha borrado.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 8**.

Recopilar información de fallas.

Paso 8 En la interfaz del FusionInsight Manager de los clústeres activos y en espera, seleccione **O&M** > **Log** > **Download**.

Paso 9 En el **Service** del cuadro de lista desplegable del clúster requerido, seleccione **HBase**.

Paso 10 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 11 Póngase en contacto con el y envíe los registros de fallas recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.157 ALM-19011 El número de región de RegionServer supera el umbral

Descripción

El sistema comprueba el número de región en cada RegionServer en cada instancia de servicio HBase cada 30 segundos. El número de región se muestra en la página de supervisión del servicio HBase y en la página de supervisión del rol RegionServer. Esta alarma se genera cuando el número de Regions en un RegionServer excede el umbral (valor predeterminado: 2000) durante 20 veces consecutivas. El umbral se puede cambiar eligiendo **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster* > **HBase**. Esta alarma se borra cuando el número de regiones es menor o igual que el umbral.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
19011	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

El rendimiento de lectura/escritura de datos de HBase se ve afectado cuando el número de regiones en un RegionServer excede el umbral.

Causas posibles

- La distribución de región de RegionServer está desequilibrada.
- La escala del clúster HBase es demasiado pequeña.

Procedimiento

Vea información de localización de alarma.

Paso 1 En la página de inicio del FusionInsight Manager, seleccione **O&M** > **Alarm** > **Alarms**, seleccione esta alarma y vea la instancia de servicio y el nombre del host en **Location**.

Paso 2 En la página principal del FusionInsight Manager, seleccione **Cluster** > *Name of the desired cluster* > **Services**, haga clic en la instancia de servicio HBase para la que se genera la alarma y haga clic en **HMaster(Active)**. En el WebUI mostrado de la instancia de HBase, compruebe si la distribución de región en el RegionServer está equilibrada.

NOTA

De forma predeterminada, el usuario **admin** no tiene los permisos para gestionar otros componentes. Si la página no se puede abrir o el contenido mostrado está incompleto al acceder a la interfaz de usuario nativa de un componente debido a la falta de permisos, puede crear manualmente un usuario con los permisos para gestionar ese componente.

- En caso afirmativo, vaya a **Paso 9**.
- Si no, vaya a **Paso 3**.

Habilitar balanceo de carga.

Paso 3 Inicie sesión en el nodo donde se encuentra el cliente HBase como usuario **root**. Vaya al directorio de instalación del cliente y establezca las variables de entorno.

cd *client installation directory*

source bigdata_env

Si el clúster adopta el modo de seguridad, realice la autenticación de seguridad. Específicamente, ejecute el comando **kinit hbase** e introduzca la contraseña como se le solicite (obtenga la contraseña del administrador).

Paso 4 Ejecute los siguientes comandos para ir a la ventana de comandos del shell de HBase y verifique si la función de balanceo de carga está habilitada.

hbase shell

balancer_enabled

- En caso afirmativo, vaya a **Paso 6**.
- Si no, vaya a **Paso 5**.

Paso 5 En la ventana de comandos del shell de HBase, ejecute los siguientes comandos para habilitar la función de balanceo de carga y compruebe si la función está habilitada.

balance_switch true

balancer_enabled

Paso 6 En la ventana de comandos del shell HBase, ejecute el comando **balancer** para activar manualmente la función de balanceo de carga.

NOTA

Se recomienda habilitar y activar manualmente la función de balanceo de carga durante las horas no pico.

Paso 7 En la página de inicio del FusionInsight Manager, elija **Cluster** > *Name of the desired cluster* > **Services** > **HBase** y haga clic en **HMaster(Active)**. En la WebUI mostrada de la instancia de HBase, actualice la página y compruebe si la distribución de región está equilibrada.

- En caso afirmativo, vaya a **Paso 8**.
- Si no, vaya a **Paso 21**.

Paso 8 Verifique si la alarma se ha borrado.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 9**.

Eliminar tablas no deseadas de HBase.

NOTA

Tenga cuidado al eliminar datos para asegurarse de que los datos se eliminen correctamente.

Paso 9 En la página de inicio del FusionInsight Manager, elija **Cluster** > *Name of the desired cluster* > **Services** > **HBase** y haga clic en **HMaster(Active)**. En la WebUI mostrada de la instancia de HBase, vea las tablas almacenadas en la instancia de servicio de HBase y registre las tablas no deseadas que se puedan eliminar.

Paso 10 En la ventana de comandos del shell HBase, ejecute el comando **disable** y el comando **drop** para eliminar la tabla y reducir el número de Regions.

disable '*name of the table to be deleted***'**

drop '*name of the table to be deleted***'**

Paso 11 En la ventana de comandos del shell de HBase, ejecute el siguiente comando para comprobar si la función de balanceo de carga está habilitada.

balancer_enabled

- En caso afirmativo, vaya a **Paso 13**.
- Si no, vaya a **Paso 12**.

Paso 12 En la ventana de comandos del shell de HBase, ejecute los siguientes comandos para habilitar la función de balanceo de carga y confirmar que la función está habilitada.

balance_switch true

balancer_enabled

Paso 13 En la ventana de comandos del shell HBase, ejecute el comando **balancer** para activar manualmente la función de balanceo de carga.

Paso 14 En la página de inicio del FusionInsight Manager, elija **Cluster** > *Name of the desired cluster* > **Services** > **HBase** y haga clic en **HMaster(Active)**. En la WebUI mostrada de la instancia de HBase, actualice la página y compruebe si la distribución de región está equilibrada.

- En caso afirmativo, vaya a **Paso 15**.
- Si no, vaya a **Paso 21**.

Paso 15 Verifique si la alarma se ha borrado.

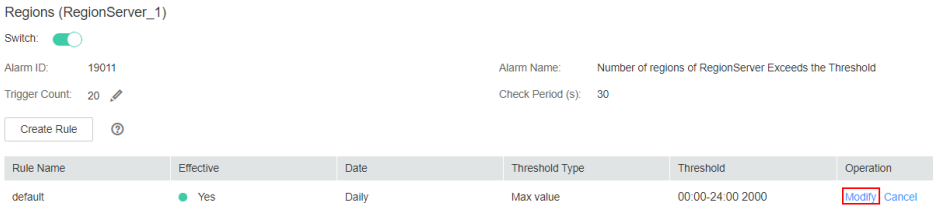
- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 16**.

Ajustar el umbral.

Paso 16 En la página de inicio del FusionInsight Manager, elija **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster* > **HBase** > **Regions(RegionServer)** y seleccione la regla aplicada y haga clic en **Modify** para comprobar si el umbral es correcto.

- Si es excesivamente pequeño, aumente el umbral según sea necesario y vaya a **Paso 17**.
- Si es apropiado, diríjase a **Paso 18**.

Figura 9-61 Regions(RegionServer_*1*)



Paso 17 Verifique si la alarma se ha borrado.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 18**.

Realizar expansión de capacidad de sistema.

Paso 18 Agregue nodos al clúster de HBase y agregue instancias de RegionServer a los nodos. A continuación, habilite y active manualmente la función de balanceo de carga.

Paso 19 En la página principal del FusionInsight Manager, seleccione **Cluster** > *Name of the desired cluster* > **Services**, haga clic en la instancia de servicio HBase para la que se genera la alarma y haga clic en **HMaster(Active)**. En la WebUI mostrada de la instancia de HBase, actualice la página y compruebe si la distribución de región está equilibrada.

- En caso afirmativo, vaya a **Paso 20**.
- Si no, vaya a **Paso 21**.

Paso 20 Verifique si la alarma se ha borrado.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 21**.

Recopilar información de fallas.

Paso 21 En la página principal del FusionInsight Manager de los clústeres activo y en espera, seleccione **O&M**> **Log** > **Download**.

Paso 22 Seleccione **HBase** en el clúster requerido en el **Service**.

Paso 23 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 24 Póngase en contacto con el y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.158 ALM-19012 Directorio de tabla de sistema de HBase o archivo perdido

Descripción

El sistema comprueba si existen directorios y archivos de HBase en el HDFS cada 120 segundos. Esta alarma se genera cuando el sistema detecta que los archivos o directorios no existen. Esta alarma se borra cuando se restauran los archivos o directorios.

Los directorios y archivos de HBase son los siguientes:

- Directorio del espacio de nombres **hbase** en HDFS
- Archivo **hbase.version**
- Directorio de la tabla **hbase:meta** en el archivo HDFS, .tableinfo y .regioninfo
- Directorio de la tabla **hbase:namespace** en el archivo HDFS, .tableinfo y .regioninfo
- Directorio de la tabla **hbase:hindex** en el archivo HDFS, .tableinfo y .regioninfo
- Directorio de la tabla **hbase:acl** en el archivo HDFS, .tableinfo y .regioninfo (Esta tabla no existe en el clúster de modo común de forma predeterminada.)

Atributo

ID de alarma	Gravedad de la alarma	Borrado automáticamente
19012	Crítica	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.

Nombre	Significado
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

El servicio HBase no puede reiniciarse o iniciarse.

Causas posibles

Faltan archivos o directorios en el HDFS.

Procedimiento

Localizar la causa de la alarma.

Paso 1 En el FusionInsight Manager, seleccione **O&M** > **Alarm** > **Alarms**. Haga clic en esta alarma y compruebe si **Alarm Cause** indica errores desconocidos.

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 2**

Paso 2 En la página de inicio del FusionInsight Manager, seleccione **O&M** > **Backup and Restoration** > **Backup Management**. Compruebe si hay registros de éxito de la tarea de copia de respaldo llamada **default** u otras tareas de copia de respaldo de metadatos de HBase que se han ejecutado correctamente.

- En caso afirmativo, vaya a **Paso 3**.
- Si no, vaya a **Paso 4**.

Paso 3 Utilice los metadatos de copia de respaldo más recientes para restaurar los metadatos del servicio HBase.

Recopilar información de fallas.

Paso 4 En la página FusionInsight Manager de los clústeres activo y en espera, seleccione **O&M** > **Log** > **Download**.

Paso 5 En el área **Service**, seleccione los servicios HBase defectuosos en el clúster requerido.

Paso 6 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 7 Póngase en contacto con el y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.159 ALM-19013 La duración de las regiones en estado de transacción supera el umbral

Descripción

El sistema comprueba el número de regiones en estado de transacción en HBase cada 300 segundos. Esta alarma se genera cuando el sistema detecta que la duración de las regiones en estado de transacción excede el umbral durante dos veces consecutivas. Esta alarma se borra cuando se restauran todas las regiones de tiempo de espera.

Atributo

ID de alarma	Gravedad de la alarma	Borrado automáticamente
19013	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

Algunos datos de la tabla se pierden o no están disponibles.

Causas posibles

- La compactación está permanentemente bloqueada.
- Los archivos HDFS son anormales.

Procedimiento

Localizar la causa de la alarma.

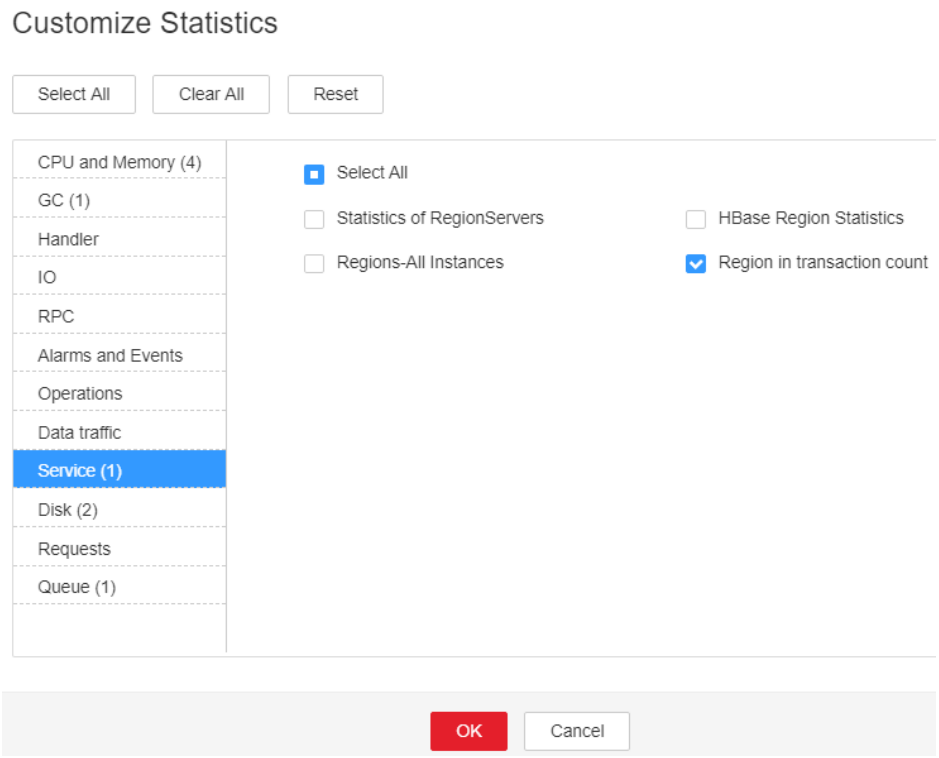
Paso 1 En FusionInsight Manager, elija **O&M** > **Alarm** > **Alarms**, seleccione esta alarma y vea **HostName** y **RoleName** en **Location**.

Paso 2 Elija **Cluster** > *Name of the desired cluster* > **Services > HBase**, haga clic en el menú desplegable en el área de gráfico y elija**Customize > Service** >

Region in transaction count para ver **Region in transaction count over threshold**. Compruebe si el elemento de supervisión detecta un valor en tres períodos de detección consecutivos. (El umbral predeterminado es 60 segundos.)

- En caso afirmativo, vaya a **Paso 3**.
- Si no, vaya a **Paso 7**.

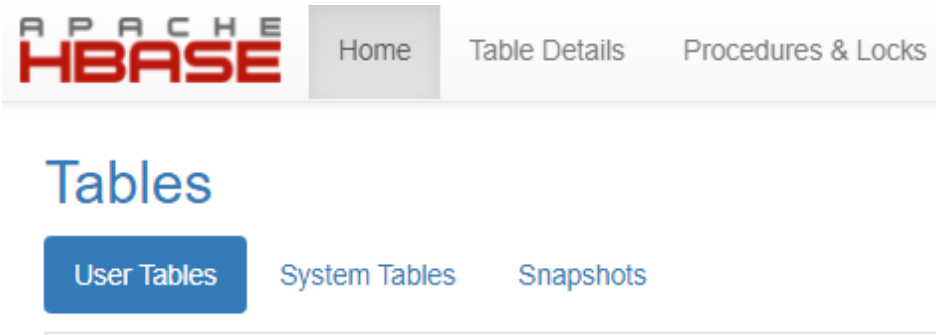
Figura 9-62 Region in transaction count



Paso 3 Seleccione **Cluster** > *Name of the desired cluster* > **Services** > **HBase** > **HMaster (Active)** > **Tables** para comprobar si las regiones de un solo estado de transacción de tabla se agotan.

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 7**.

Figura 9-63 Tablas



Paso 4 Ejecute el comando **hbase hbck** en el cliente y compruebe si se muestra el mensaje de error "No table descriptor file under hdfs://hacluster/hbase/data/default/table".

- En caso afirmativo, vaya a **Paso 5**.
- Si no, vaya a **Paso 7**.

Paso 5 Inicie sesión en el cliente como usuario **root**. Ejecute el siguiente comando:

cd *client installation directory*

source bigdata_env

Si el clúster está en modo de seguridad, ejecute el comando **kinit hbase**

Inicie sesión en HMaster WebUI, seleccione **Procedure & Locks** en el árbol de navegación y compruebe si algún ID de proceso está en el estado **Waiting** en **Procedures**. En caso afirmativo, ejecute el siguiente comando para liberar el bloqueo de procedimiento:

hbase hbck -j *client installation directory*/**HBase/hbase/tools/hbase-hbck2-*.jar bypass -o** *pid*

Compruebe si el estado está en el estado **Bypass**. Si el procedimiento en la interfaz de usuario está siempre en estado **RUNNABLE(Bypass)**, realice una conmutación activa/en espera. Ejecute el comando **assigns** para volver a conectar la región.

hbase hbck -j *client installation directory*/**HBase/hbase/tools/hbase-hbck2-*.jar assigns -o** *regionName*

Paso 6 Repita **Paso 4**. Ejecute el comando **hbase hbck** en el cliente y compruebe si se muestra el mensaje de error "No table descriptor file under hdfs://hacluster/hbase/data/default/table".

- En caso afirmativo, vaya a **Paso 7**.
- En caso negativo, no se requiere ninguna otra acción.

Recopilar información de fallas.

Paso 7 En la página FusionInsight Manager de los clústeres activo y en espera, seleccione **O&M** > **Log** > **Download**.

Paso 8 En el área **Service**, seleccione los servicios HBase defectuosos en el clúster requerido.

Paso 9 Haga clic en  en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 10 Póngase en contacto con el y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.160 ALM-19014 El uso de la cuota de capacidad en el ZooKeeper supera severamente el umbral

Descripción

El sistema comprueba el uso de ZNode del servicio HBase cada 120 segundos. Esta alarma se genera cuando el uso de capacidad ZNode del servicio HBase excede el umbral de alarma crítica (90% por defecto).

Esta alarma se borra cuando el uso de capacidad ZNode es menor que el umbral de alarma crítica.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
19014	Crítica	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Threshold	Especifica el umbral para el que se genera la alarma.

Impacto en el sistema

Esta alarma indica que el uso de capacidad del ZNode de HBase ha excedido severamente el umbral. Como resultado, la solicitud de escritura del servicio HBase falla.

Causas posibles

- La DR está configurada para HBase y la sincronización de datos falla o es lenta en la DR.
- Se está dividiendo un gran número de archivos WAL en el clúster HBase.

Procedimiento

Verificar la configuración de capacidad y el uso de ZNodes.

Paso 1 En FusionInsight Manager, seleccione **O&M** > **Alarm** > **Alarms**, seleccione la alarma cuyo ID es **19014** y vea el umbral en **Additional Information**.

Paso 2 Inicie sesión en el cliente HBase como usuario **root**. Ejecute el siguiente comando para ir al directorio de instalación del cliente:

cd *Client installation directory*

Ejecute el siguiente comando para establecer variables de entorno:

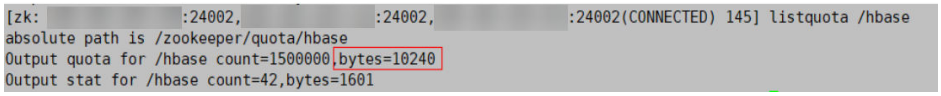
source bigdata_env

Si el clúster utiliza el modo de seguridad, ejecute el siguiente comando para realizar la autenticación de seguridad:

kinit hbase

Ingrese la contraseña como se le solicite (obtenga la contraseña del administrador del clúster de MRS).

Paso 3 Ejecute el comando **hbase zkcli** para iniciar sesión en el cliente ZooKeeper y ejecute el comando **listquota /hbase** para comprobar la cuota de capacidad de ZNode del servicio HBase. El directorio raíz ZNode en el comando se especifica mediante el parámetro **zookeeper.znode.parent** del servicio HBase. El área marcada en la siguiente figura muestra la configuración de capacidad del raíz ZNode del servicio HBase.



Paso 4 Ejecute el comando **getusage /hbase/splitWAL** para comprobar el uso de capacidad del ZNode. Compruebe si la relación de **Data size** a la cuota de capacidad de ZNode está cerca del umbral de alarma.

- En caso afirmativo, vaya a **Paso 5**.
- Si no, vaya a **Paso 6**.

Paso 5 En FusionInsight Manager, seleccione **O&M** > **Alarm** > **Alarms**. Compruebe si existe la alarma cuyo ID sea **12007**, **19000** o **19013** y el **ServiceName** de **Location** es el servicio HBase actual.

- En caso afirmativo, haga clic en **View Help** junto a la alarma y rectifique la falla consultando el documento de ayuda. A continuación, vaya a **Paso 8**.
- Si no, vaya a **Paso 9**.

Paso 6 Ejecute el comando **getusage /hbase/replication** para comprobar el uso de capacidad del ZNode. Compruebe si la relación de **Data size** a la cuota de capacidad de ZNode está cerca del umbral de alarma.

- En caso afirmativo, vaya a **Paso 7**.
- Si no, vaya a **Paso 9**.

Paso 7 En FusionInsight Manager, seleccione **O&M** > **Alarm** > **Alarms**. Compruebe si la alarma cuyo ID es **19006** y **ServiceName** en **Location** es el servicio HBase actual existe.

- En caso afirmativo, haga clic en **View Help** junto a la alarma y rectifique la falla consultando el documento de ayuda. A continuación, vaya a **Paso 8**.

- Si no, vaya a **Paso 9**.

Paso 8 Compruebe si la alarma se borra cinco minutos más tarde.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 9**.

Recopilar información de fallas.

Paso 9 En FusionInsight Manager, seleccione **O&M**. En el panel de navegación de la izquierda, elija **Log** > **Download**.

Paso 10 Expanda la lista desplegable junto al campo **Service**. En el cuadro de diálogo **Services** que se muestra, seleccione **HBase** para el clúster de destino.

Paso 11 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 12 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

Información relacionada

Ninguna

9.161 ALM-19015 El uso de cuotas de cantidad en el ZooKeeper supera el umbral

Descripción

El sistema comprueba el uso de ZNode del servicio HBase cada 120 segundos. Esta alarma se genera cuando el sistema detecta que el uso de la cantidad ZNode del servicio HBase supera el umbral de alarma (75% por defecto).

Esta alarma se borra cuando el uso de la cantidad de ZNode es menor que el umbral de alarma.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
19015	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Threshold	Especifica el umbral para el que se genera la alarma.

Impacto en el sistema

Esta alarma indica que el uso de la cantidad de ZNode en el servicio HBase ha excedido el umbral. Si esta alarma no se maneja de manera oportuna, la gravedad del problema puede escalarse a **Critical** lo que afecta a la escritura de datos.

Causas posibles

- La DR está configurada para HBase y la sincronización de datos falla o es lenta en la DR.
- Se está dividiendo un gran número de archivos WAL en el clúster HBase.

Procedimiento

Comprobar la cuota de cantidad y el uso de ZNodes.

Paso 1 En FusionInsight Manager, seleccione **O&M** > **Alarm** > **Alarms**, seleccione la alarma cuyo ID es **19015** y vea el umbral en **Additional Information**.

Paso 2 Inicie sesión en el cliente HBase como usuario **root**. Ejecute el siguiente comando para ir al directorio de instalación del cliente:

cd *Client installation directory*

Ejecute el siguiente comando para establecer variables de entorno:

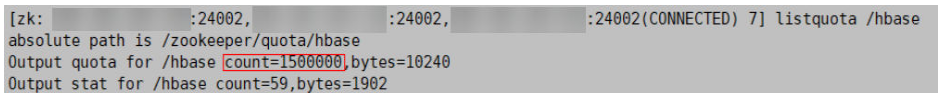
source bigdata_env

Si el clúster utiliza el modo de seguridad, ejecute el siguiente comando para realizar la autenticación de seguridad:

kinit hbase

Ingrese la contraseña como se le solicite (obtenga la contraseña del administrador del clúster de MRS).

Paso 3 Ejecute el comando **hbase zkcli** para iniciar sesión en el cliente ZooKeeper y ejecute el comando **listquota /hbase** para comprobar la cuota de cantidad ZNode del servicio HBase. El directorio raíz ZNode en el comando se especifica mediante el parámetro **zookeeper.znode.parent** del servicio HBase. El área marcada en la siguiente figura muestra la configuración de cuota de cantidad del ZNode raíz del servicio HBase.



Paso 4 Ejecute el comando **getusage /hbase/splitWAL** para comprobar el uso de la cantidad de ZNode y verifique si la relación de **Node count** en la salida del comando a la cuota de cantidad de ZNode está cerca del umbral de alarma.

- En caso afirmativo, vaya a **Paso 5**.
- Si no, vaya a **Paso 6**.

Paso 5 En FusionInsight Manager, seleccione **O&M** > **Alarm** > **Alarms**. Compruebe si existe la alarma cuyo ID sea **12007**, **19000** o **19013** y el **ServiceName** de **Location** es el servicio HBase actual.

- En caso afirmativo, haga clic en **View Help** junto a la alarma y rectifique la falla consultando el documento de ayuda. A continuación, vaya a **Paso 8**.
- Si no, vaya a **Paso 9**.

Paso 6 Ejecute el comando **getusage /hbase/replication** para comprobar el uso de la cantidad de ZNode y verifique si la relación de **Node count** en la salida del comando a la cuota de cantidad de ZNode está cerca del umbral de alarma.

- En caso afirmativo, vaya a **Paso 7**.
- Si no, vaya a **Paso 9**.

Paso 7 En FusionInsight Manager, seleccione **O&M** > **Alarm** > **Alarms**. Compruebe si la alarma cuyo ID es **19006** y **ServiceName** en **Location** es el servicio HBase actual existe.

- En caso afirmativo, haga clic en **View Help** junto a la alarma y rectifique la falla consultando el documento de ayuda. A continuación, vaya a **Paso 8**.
- Si no, vaya a **Paso 9**.

Paso 8 Verifique si la alarma se ha borrado.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 9**.

Recopilar información de fallas.

Paso 9 En FusionInsight Manager, seleccione **O&M**. En el panel de navegación de la izquierda, elija **Log** > **Download**.

Paso 10 Expanda la lista desplegable **Service** y seleccione **HBase** para el clúster de destino.

Paso 11 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 12 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

Información relacionada

Ninguna

9.162 ALM-19016 El uso de cuotas de cantidad en ZooKeeper supera severamente el umbral

Descripción

El sistema comprueba el uso de ZNode del servicio HBase cada 120 segundos. Esta alarma se genera cuando el uso de znode del servicio HBase excede el umbral de alarma crítica (90% de forma predeterminada).

Esta alarma se borra cuando la cantidad de uso del ZNode es menor que el umbral de alarma crítica.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
19016	Crítica	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Threshold	Especifica el umbral para el que se genera la alarma.

Impacto en el sistema

Esta alarma indica que la cantidad de uso del ZNode de HBase ha excedido severamente el umbral. Como resultado, la solicitud de escritura del servicio HBase falla.

Causas posibles

- La DR está configurada para HBase y la sincronización de datos falla o es lenta en la DR.
- Se está dividiendo un gran número de archivos WAL en el clúster HBase.

Procedimiento

Comprobar la cuota de cantidad y el uso de ZNodes.

Paso 1 En FusionInsight Manager, seleccione **O&M** > **Alarm** > **Alarms**, seleccione la alarma cuyo ID es **19016** y vea el umbral en **Additional Information**.

Paso 2 Inicie sesión en el cliente HBase como usuario **root**. Ejecute el siguiente comando para ir al directorio de instalación del cliente:

cd *Client installation directory*

Ejecute el siguiente comando para establecer variables de entorno:

source bigdata_env

Si el clúster utiliza el modo de seguridad, ejecute el siguiente comando para realizar la autenticación de seguridad:

kinit hbase

Ingrese la contraseña como se le solicite (obtenga la contraseña del administrador del clúster de MRS).

Paso 3 Ejecute el comando **hbase zkcli** para iniciar sesión en el cliente ZooKeeper y ejecute el comando **listquota /hbase** para comprobar la cuota de cantidad ZNode del servicio HBase. El directorio raíz ZNode en el comando se especifica mediante el parámetro **zookeeper.znode.parent** del servicio HBase. El área marcada en la siguiente figura muestra la configuración de cantidad del raíz ZNode del servicio HBase.

Paso 4 Ejecute el comando **getusage /hbase/splitWAL** para comprobar el uso de ZNode y verifique si la relación de **Node count** en la salida del comando a la cuota de cantidad de znode está cerca del umbral de alarma.

- En caso afirmativo, vaya a **Paso 5**.
- Si no, vaya a **Paso 6**.

Paso 5 En FusionInsight Manager, seleccione **O&M** > **Alarm** > **Alarms**. Compruebe si existe la alarma cuyo ID sea **12007**, **19000** o **19013** y el **ServiceName** de **Location** es el servicio HBase actual.

- En caso afirmativo, haga clic en **View Help** junto a la alarma y rectifique la falla consultando el documento de ayuda. A continuación, vaya a **Paso 8**.
- Si no, vaya a **Paso 9**.

Paso 6 Ejecute el comando **getusage /hbase/replication** para comprobar el uso de ZNode y verifique si la relación de **Node count** en la salida del comando a la cuota de cantidad ZNode está cerca del umbral de alarma.

- En caso afirmativo, vaya a **Paso 7**.
- Si no, vaya a **Paso 9**.

Paso 7 En FusionInsight Manager, seleccione **O&M** > **Alarm** > **Alarms**. Compruebe si la alarma cuyo ID es **19006** y **ServiceName** en **Location** es el servicio HBase actual existe.

- En caso afirmativo, haga clic en **View Help** junto a la alarma y rectifique la falla consultando el documento de ayuda. A continuación, vaya a **Paso 8**.
- Si no, vaya a **Paso 9**.

Paso 8 Verifique si la alarma se ha borrado.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 9**.

Recopilar información de fallas.

Paso 9 En FusionInsight Manager, seleccione **O&M**. En el panel de navegación de la izquierda, elija **Log** > **Download**.

Paso 10 Expanda la lista desplegable **Service** y seleccione **HBase** para el clúster de destino.

Paso 11 Haga clic en  en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 12 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

Información relacionada

Ninguna

9.163 ALM-19017 El uso de la cuota de capacidad en el ZooKeeper supera el umbral

Descripción

El sistema comprueba el uso de ZNode del servicio HBase cada 120 segundos. Esta alarma se genera cuando el sistema detecta que el uso de la capacidad de ZNodes del servicio HBase supera el umbral de alarma (75% por defecto).

Esta alarma se borra cuando el uso de capacidad de la capacidad ZNode es menor que el umbral.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
19017	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Threshold	Especifica el umbral para el que se genera la alarma.

Impacto en el sistema

Esta alarma indica que el uso de la capacidad de ZNodes en el servicio HBase ha excedido el umbral. Si esta alarma no se maneja de manera oportuna, la gravedad del problema puede escalarse a **Critical** lo que afecta a la escritura de datos.

Causas posibles

- La DR está configurada para HBase y la sincronización de datos falla o es lenta en la DR.
- Se está dividiendo un gran número de archivos WAL en el clúster HBase.

Procedimiento

Verificar la configuración de capacidad y el uso de ZNodes.

Paso 1 En FusionInsight Manager, seleccione **O&M** > **Alarm** > **Alarms**, seleccione la alarma cuyo ID es **19017** y vea el umbral en **Additional Information**.

Paso 2 Inicie sesión en el cliente HBase como usuario **root**. Ejecute el siguiente comando para ir al directorio de instalación del cliente:

cd *Client installation directory*

Ejecute el siguiente comando para establecer variables de entorno:

source bigdata_env

Si el clúster utiliza el modo de seguridad, ejecute el siguiente comando para realizar la autenticación de seguridad:

kinit hbase

Ingrese la contraseña como se le solicite (obtenga la contraseña del administrador del clúster de MRS).

Paso 3 Ejecute el comando **hbase zkcli** para iniciar sesión en el cliente ZooKeeper y ejecute el comando **listquota /hbase** para comprobar la cuota de cantidad ZNode del servicio HBase. El directorio raíz ZNode en el comando se especifica mediante el parámetro **zookeeper.znode.parent** del servicio HBase. El área marcada en la siguiente figura muestra la configuración de cantidad del raíz ZNode del servicio HBase.

Paso 4 Ejecute el comando **getusage /hbase/splitWAL** para comprobar el uso de capacidad del ZNode. Compruebe si la relación de **Data size** a la cuota de capacidad de ZNode está cerca del umbral de alarma.

- En caso afirmativo, vaya a **Paso 5**.
- Si no, vaya a **Paso 6**.

Paso 5 En FusionInsight Manager, compruebe si la alarma cuyo ID sea **12007**, **19000** o **19013** y **ServiceName** de **Location** es el servicio HBase actual.

- En caso afirmativo, haga clic en **View Help** junto a la alarma y rectifique la falla consultando el documento de ayuda. A continuación, vaya a **Paso 8**.
- Si no, vaya a **Paso 7**.

Paso 6 Ejecute el comando **getusage /hbase/replication** para comprobar el uso de capacidad del ZNode. Compruebe si la relación de **Data size** a la cuota de capacidad de ZNode está cerca del umbral de alarma.

- En caso afirmativo, vaya a **Paso 7**.
- Si no, vaya a **Paso 9**.

Paso 7 En FusionInsight Manager, seleccione **O&M** > **Alarm** > **Alarms**. Compruebe si la alarma cuyo ID es **19006** y **ServiceName** en **Location** es el servicio HBase actual existe.

- En caso afirmativo, haga clic en **View Help** junto a la alarma y rectifique la falla consultando el documento de ayuda. A continuación, vaya a **Paso 8**.
- Si no, vaya a **Paso 9**.

Paso 8 Verifique si la alarma se ha borrado.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 9**.

Recopilar información de fallas.

Paso 9 En FusionInsight Manager, seleccione **O&M**. En el panel de navegación de la izquierda, elija **Log** > **Download**.

Paso 10 Expanda la lista desplegable **Service** y seleccione **HBase** para el clúster de destino.

Paso 11 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 12 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

Información relacionada

Ninguna

9.164 ALM-19018 El tamaño de la cola de compactación de HBase supera el umbral

Descripción

El sistema comprueba el tamaño de la cola de compactación de HBase cada 300 segundos. Esta alarma se genera cuando el tamaño de la cola de compactación supera el umbral de alarma (**100** por defecto). Esta alarma se borra cuando el tamaño de la cola de compactación es menor que el umbral.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
19018	Leves	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

El rendimiento del clúster puede deteriorarse, lo que afecta a la lectura y escritura de datos.

Causas posibles

- El número de RegionServers de HBase es demasiado pequeño.
- Hay regiones excesivas en un solo RegionServer de HBase.
- El tamaño de heap de RegionServer de HBase es pequeño.
- Los recursos son insuficientes.
- Los parámetros relacionados no están configurados correctamente.

Procedimiento

Comprobar si los parámetros relacionados están configurados correctamente.

Paso 1 Inicie sesión en FusionInsight Manager y elija **O&M** > **Alarm** > **Alarms**. En la página que se muestra, compruebe si existe la alarma cuyo **Alarm ID** sea **19008** o **19011**.

- En caso afirmativo, haga clic en **View Help** junto a la alarma y rectifique la falla consultando el documento de ayuda. A continuación, vaya a **Paso 3**.
- Si no, vaya a **Paso 2**.

Paso 2 En FusionInsight Manager, elija **Cluster** > *Name of the desired cluster* > **Services** > **HBase**. En la página que se muestra, haga clic en la pestaña **Configuration** y luego en la subpestaña **All Configurations**, busque **hbase.hstore.compaction.min**, **hbase.hstore.compaction.max**, **hbase.regionserver.thread.compaction.small**, y **hbase.regionserver.thread.compaction.throttle**, y los establezca en valores más grandes.

Paso 3 Verifique si la alarma se ha borrado.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 4**.

Recopilar información de fallas.

Paso 4 En FusionInsight Manager, seleccione **O&M**. En el panel de navegación de la izquierda, elija **Log** > **Download**.

Paso 5 Expanda la lista desplegable **Service** y seleccione **HBase** para el clúster de destino.

Paso 6 Haga clic en  en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 7 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

Información relacionada

Ninguna

9.165 ALM-19019 El número de HBase HFiles que se van a sincronizar supera el umbral

Descripción

El sistema comprueba el número de HFiles a sincronizar por el RegionServer de cada instancia de servicio HBase cada 30 segundos. Este indicador se puede ver en la página de monitorización del rol de RegionServer. Esta alarma se genera cuando el número de HFiles a sincronizar en un RegionServer supera el umbral (superando 128 durante 20 veces consecutivas por defecto). Para cambiar el umbral, elija **O&M** > **Alarm** > **Threshold Configuration** > *Name of the desired cluster* > **HBase**. Esta alarma se borra cuando el número de HFiles a sincronizar es menor o igual que el umbral.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
19019	Grave	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger Condition	Especifica el umbral para activar la alarma.

Impacto en el sistema

Si el número de HFiles a sincronizar por un RegionServer excede el umbral, el número de ZNodes utilizados por HBase excede el umbral, afectando el estado del servicio HBase.

Causas posibles

- Estado anormal de la red.
- La distribución de Region de RegionServer está desequilibrada.
- La escala de servicio HBase del clúster en espera es demasiado pequeña.

Procedimiento

Vea información de ubicación de alarma.

Paso 1 Inicie sesión en FusionInsight Manager y elija **O&M**. En el panel de navegación de la izquierda, elija **Alarm** > **Alarms**. En la página que se muestra, busque la fila que contiene la alarma cuyo **Alarm ID** es de **19019** y vea la instancia de servicio y el nombre de host en **Location**.

Compruebe la conexión de red entre RegionServers en clústeres activos y en espera.

Paso 2 Ejecute el comando **ping** para comprobar si la conexión de red entre el nodo RegionServer defectuoso y el host donde reside el RegionServer del clúster en espera es normal.

- En caso afirmativo, vaya a **Paso 5**.
- Si no, vaya a **Paso 3**.

Paso 3 Póngase en contacto con el administrador de red para restaurar la red.

Paso 4 Después de que la red se recupere, compruebe si la alarma está borrada.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 5**.

Compruebe la distribución de Region de RegionServer en el clúster activo.

Paso 5 En FusionInsight Manager, elija **Cluster** > *Name of the desired cluster* > **Services** > **HBase**. Haga clic en **HMaster(Active)** para ir a la interfaz de usuario web de la instancia de HBase y comprobar si las regiones están distribuidas uniformemente en Region Server.

Paso 6 Inicie sesión en el nodo de RegionServer como usuario **omm**.

Paso 7 Ejecute los siguientes comandos para ir al directorio de instalación del cliente y establecer la variable de entorno:

cd *Client installation directory*

source bigdata_env

Si el clúster utiliza el modo de seguridad, realice la autenticación de seguridad. Ejecute el comando **kinit hbase** e introduzca la contraseña como se le solicite (obtenga la contraseña del administrador del clúster MRS).

Paso 8 Ejecute los siguientes comandos para comprobar si la función de balanceo de carga está habilitada.

hbase shell

balancer_enabled

- En caso afirmativo, vaya a **Paso 10**.
- Si no, vaya a **Paso 9**.

Paso 9 Ejecute los siguientes comandos en HBase Shell para habilitar la función de balanceo de carga y comprobar si la función está habilitada.

balance_switch true

balancer_enabled

Paso 10 Ejecute el comando **balancer** para activar manualmente la función de balanceo de carga.

NOTA

Se recomienda habilitar y activar manualmente la función de balanceo de carga durante las horas no pico.

Paso 11 Verifique si la alarma se ha borrado.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 12**.

Compruebe la escala de servicio HBase del clúster en espera.

Paso 12 Expanda el clúster HBase, agregue un nodo y agregue una instancia de RegionServer en el nodo. A continuación, realice **Paso 6** a **Paso 10** para habilitar la función de balanceo de carga y activarla manualmente.

Paso 13 En FusionInsight Manager, elija **Cluster** > *Name of the desired cluster* > **Services** > **HBase**. Haga clic en **HMaster(Active)** para ir a la interfaz de usuario web de la instancia de HBase, actualizar la página y comprobar si las regiones están distribuidas uniformemente.

- En caso afirmativo, vaya a **Paso 14**.
- Si no, vaya a **Paso 15**.

Paso 14 Verifique si la alarma se ha borrado.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 15**.

Recopilar información de fallas.

Paso 15 En FusionInsight Manager del clúster en espera, seleccione **O&M**. En el panel de navegación de la izquierda, elija **Log** > **Download**.

Paso 16 Expanda la lista desplegable **Service** y seleccione **HBase** para el clúster de destino.

Paso 17 Haga clic en  en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 18 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

Información relacionada

Ninguna

9.166 ALM-19020 El número de archivos HBase WAL a sincronizar supera el umbral

Descripción

El sistema comprueba el número de archivos WAL que debe sincronizar el RegionServer de cada instancia de servicio HBase cada 30 segundos. Este indicador se puede ver en la página de monitorización del rol de RegionServer. Esta alarma se genera cuando el número de archivos WAL a sincronizar en un RegionServer supera el umbral (superando 128 durante 20 veces consecutivas por defecto). Para cambiar el umbral, elija **O&M** > **Alarm** > **Threshold Configuration** > *Name of the desired cluster* > **HBase**. Esta alarma se borra cuando el número de archivos WAL a sincronizar es menor o igual que el umbral.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
19020	Grave	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger Condition	Especifica el umbral para activar la alarma.

Impacto en el sistema

Si el número de archivos WAL a sincronizar por un RegionServer excede el umbral, el número de ZNodes utilizados por HBase excede el umbral, lo que afecta al estado del servicio HBase.

Causas posibles

- Estado anormal de la red.
- La distribución de Region de RegionServer está desequilibrada.

- La escala de servicio HBase del clúster en espera es demasiado pequeña.

Procedimiento

Vea información de ubicación de alarma.

Paso 1 Inicie sesión en FusionInsight Manager y elija **O&M**. En el panel de navegación de la izquierda, elija **Alarm** > **Alarms**. En la página que se muestra, busque la fila que contiene la alarma cuyo **Alarm ID** es de **19020** y vea la instancia de servicio y el nombre de host de **Location**.

Compruebe la conexión de red entre RegionServers en clústeres activos y en espera.

Paso 2 Ejecute el comando **ping** para comprobar si la conexión de red entre el nodo RegionServer defectuoso y el host donde reside el RegionServer del clúster en espera es normal.

- En caso afirmativo, vaya a **Paso 5**.
- Si no, vaya a **Paso 3**.

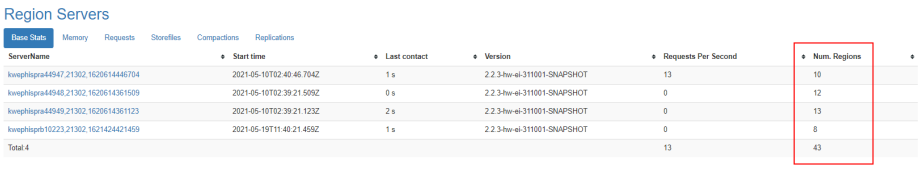
Paso 3 Póngase en contacto con el administrador de red para restaurar la red.

Paso 4 Después de que la red se recupere, compruebe si la alarma está borrada.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 5**.

Compruebe la distribución de Region de RegionServer en el clúster activo.

Paso 5 En FusionInsight Manager, elija **Cluster** > *Name of the desired cluster* > **Services** > **HBase**. Haga clic en **HMaster(Active)** para ir a la interfaz de usuario web de la instancia de HBase y comprobar si las regiones están distribuidas uniformemente en Region Server.



Paso 6 Inicie sesión en el nodo de RegionServer como usuario **omm**.

Paso 7 Ejecute los siguientes comandos para ir al directorio de instalación del cliente y establecer la variable de entorno:

cd *Client installation directory*

source bigdata_env

Si el clúster utiliza el modo de seguridad, realice la autenticación de seguridad. Ejecute el comando **kinit hbase** e introduzca la contraseña como se le solicite (obtenga la contraseña del administrador del clúster MRS).

Paso 8 Ejecute los siguientes comandos para comprobar si la función de balanceo de carga está habilitada.

hbase shell

balancer_enabled

- En caso afirmativo, vaya a **Paso 10**.

- Si no, vaya a **Paso 9**.

Paso 9 Ejecute los siguientes comandos en HBase Shell para habilitar la función de balanceo de carga y comprobar si la función está habilitada.

balance_switch true

balancer_enabled

Paso 10 Ejecute el comando **balancer** para activar manualmente la función de balanceo de carga.

NOTA

Se recomienda habilitar y activar manualmente la función de balanceo de carga durante las horas no pico.

Paso 11 Verifique si la alarma se ha borrado.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 12**.

Compruebe la escala de servicio HBase del clúster en espera.

Paso 12 Expanda el clúster HBase, agregue un nodo y agregue una instancia de RegionServer en el nodo. A continuación, realice **Paso 6** a **Paso 10** para habilitar la función de balanceo de carga y activarla manualmente.

Paso 13 En FusionInsight Manager, elija **Cluster** > *Name of the desired cluster* > **Services** > **HBase**. Haga clic en **HMaster(Active)** para ir a la interfaz de usuario web de la instancia de HBase, actualizar la página y comprobar si las regiones están distribuidas uniformemente.

- En caso afirmativo, vaya a **Paso 14**.
- Si no, vaya a **Paso 15**.

Paso 14 Verifique si la alarma se ha borrado.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 15**.

Recopilar información de fallas.

Paso 15 En FusionInsight Manager del clúster en espera, seleccione **O&M**. En el panel de navegación de la izquierda, elija **Log** > **Download**.

Paso 16 Expanda la lista desplegable **Service** y seleccione **HBase** para el clúster de destino.

Paso 17 Haga clic en  en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 18 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

Información relacionada

Ninguna

9.167 ALM-19021 El uso de RegionServer handler supera el umbral

Descripción

El sistema comprueba el uso del handler de RegionServer de cada instancia de servicio HBase cada 30 segundos. Esta alarma se genera cuando el uso del handler de un RegionServer excede el umbral (90% durante cinco veces consecutivas por defecto). Esta alarma se borra si el uso del handler es inferior o igual al umbral.

NOTA

Esta sección se aplica a MRS 3.2.0 o posterior.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
19021	Grave	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger Condition	Especifica el umbral para activar la alarma.

Impacto en el sistema

RegionServers y HBase no pueden proporcionar servicios correctamente.

Causas posibles

- El valor de un handler es demasiado pequeño.

- Se produce hotspotting.

Procedimiento

Ver información de ubicación de alarma.

Paso 1 Inicie sesión en FusionInsight Manager y elija **O&M**. En el panel de navegación de la izquierda, elija **Alarm** > **Alarms**, busque la fila que contiene la alarma cuyo **Alarm ID** es **19021**, y vea la instancia de servicio y el nombre de host en **Location**.

Comprobar la configuración de handler.

Paso 2 Elija **Cluster** > **Services** > **HBase** y haga clic en la pestaña **Configurations**. En la esquina superior derecha de la página, busque **hbase.regionserver.handler.count** y compruebe si su valor es demasiado pequeño. El valor predeterminado es **200**.

- En caso afirmativo, vaya a **Paso 3**.
- Si no, vaya a **Paso 5**.

Paso 3 Cambie el valor de este parámetro a un valor mayor y guarde la configuración. Elija **Cluster** > **Services** > **HBase**, haga clic en la pestaña **Instance**, seleccione las instancias de RegionServer afectadas y elija **More** > **Instance Rolling Restart**. En el cuadro de diálogo que se muestra, escriba el nombre de usuario y la contraseña. En el cuadro de diálogo **Instance Rolling Restart**, haga clic en **OK** y espere hasta que se complete el reinicio continuo.

Paso 4 Después de que la configuración surta efecto, compruebe si la alarma está borrada.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 5**.

Compruebe si se produce hotspotting en el clúster.

Paso 5 En FusionInsight Manager, elija **Cluster** > **Services** > **HBase** y haga clic en **HMaster(Active)** después de **HMaster WebUI** para ir a la interfaz de usuario web de la instancia de HBase. En el área **Region Servers** de la página **Home**, haga clic en **Requests** y compruebe si las solicitudes de las columnas **Filtered Read Request Count** y **Write Request Count** están distribuidas uniformemente.

- En caso afirmativo, vaya a **Paso 13**.
- Si no, vaya a **Paso 6**.

Paso 6 Compruebe si las regiones están distribuidas uniformemente.

En FusionInsight Manager, elija **Cluster** > **Services** > **HBase** y haga clic en **HMaster(Active)** después de **HMaster WebUI** para ir a la interfaz de usuario web de la instancia de HBase. En el área **Region Servers** de la página **Home**, haga clic en **Base Stats** y compruebe si las regiones de la columna **Num.Regions** están distribuidas uniformemente.

- En caso afirmativo, vaya a **Paso 13**.
- Si no, vaya a **Paso 7**.

Paso 7 Inicie sesión en el nodo RegionServer defectuoso como usuario **omm**.

Paso 8 Ejecute los siguientes comandos para ir al directorio de instalación del cliente y establecer la variable de entorno:

cd *Client installation directory*

source bigdata_env

Si el clúster utiliza el modo de seguridad, ejecute el siguiente comando para realizar la autenticación de seguridad:

kinit hbase

Ingrese la contraseña como se le solicite (obtenga la contraseña del administrador del clúster de MRS).

Paso 9 Ejecute los siguientes comandos para comprobar si la función de balanceo de carga está habilitada. Si la salida del comando es **true**, se activa la función de balanceo de carga.

hbase shell

balancer_enabled

```
hbase:004:0> balancer_enabled
true
Took 0.0165 seconds
=> true
```

- En caso afirmativo, vaya a **Paso 13**.
- Si no, vaya a **Paso 10**.

Paso 10 Ejecute los siguientes comandos en HBase Shell para habilitar la función de balanceo de carga y comprobar si la función está habilitada.

balance_switch true

balancer_enabled

NOTA

Se recomienda habilitar y activar manualmente la función de balanceo de carga durante las horas no pico.

Paso 11 Ejecute el siguiente comando para activar manualmente la función de balanceo de carga:

balancer

Paso 12 Una vez finalizado el balanceo de carga, inicie sesión en FusionInsight Manager y elija **O&M**. En el panel de navegación de la izquierda, elija **Alarm** > **Alarms** y compruebe si la alarma está desactivada.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 13**.

Recopilar información de fallas.

Paso 13 En FusionInsight Manager, seleccione **O&M**. En el panel de navegación de la izquierda, elija **Log** > **Download**.

Paso 14 Expanda la lista desplegable **Service** y seleccione **HBase** para el clúster de destino.

Paso 15 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas respectivamente. A continuación, haga clic en **Download**.

Paso 16 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

Información relacionada

Ninguna

9.168 ALM-20002 Servicio de Hue no disponible

Descripción

Esta alarma se genera cuando el servicio Hue no está disponible. El sistema comprueba el estado del servicio Hue cada 60 segundos.

Esta alarma se borra cuando el servicio Hue es normal.

Atributo

ID de alarma	Gravedad de la alarma	Borrado automáticamente
20002	Crítica	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

El sistema no puede proporcionar servicios de carga, consulta y extracción de datos.

Causas posibles

- El servicio de KrbServer interno del que depende el servicio de Hue es anormal.
- El servicio DBService interno del que depende el servicio Hue es anormal.
- La conexión de red al DBService es anormal.

Procedimiento

Comprobar si el KrbServer es anormal.

Paso 1 En la página de inicio del FusionInsight Manager, seleccione **Cluster** > *Name of the desired cluster* > **Services**. En la lista de servicios, compruebe si el estado de ejecución del **KrbServer** es **Normal**.

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 2**.

Paso 2 Reinicie el servicio KrbServer.

Paso 3 Espere varios minutos y compruebe si **Hue Service Unavailable** está borrado.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 4**.

Comprobar si DBService es anormal.

Paso 4 En la página de inicio del FusionInsight Manager, seleccione **Cluster** > *Name of the desired cluster* > **Services**.

Paso 5 En la lista de servicios, compruebe si el estado de ejecución del **DBService** es **Normal**.

- En caso afirmativo, vaya a **Paso 8**.
- Si no, vaya a **Paso 6**.

Paso 6 Reinicie el DBService.

NOTA

Para reiniciar el servicio, introduzca la contraseña de administrador del FusionInsight Manager.

Paso 7 Espere varios minutos y compruebe si **Hue Service Unavailable** está borrado.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 8**.

Comprobar si la conexión de red al DBService es normal.

Paso 8 Elija **Cluster** > *Name of the desired cluster* > **Services** > **Hue** > **Instance**, registre la dirección IP del Hue activo.

Paso 9 Inicie sesión en el Hue activo.

Paso 10 Ejecute el comando **ping** para comprobar si la comunicación entre el host que ejecuta el Hue activo y los hosts que ejecutan el DBService es normal. (Obtener las direcciones IP de los hosts que ejecutan el DBService de la misma manera que para obtener la dirección IP del Hue activo.)

- En caso afirmativo, vaya a **Paso 13**.
- Si no, vaya a **Paso 11**.

Paso 11 Póngase en contacto con el administrador para restaurar la red.

Paso 12 Espere varios minutos y compruebe si **Hue Service Unavailable** está borrado.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 13**.

Recopilar información de fallas.

Paso 13 En FusionInsight Manager, elija **O&M** > **Log** > **Download**.

Paso 14 Seleccione los siguientes nodos en el clúster requerido en la lista desplegable **Service** :

- Hue
- Controller

Paso 15 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 16 En el FusionInsight Manager, elija **Cluster** > *Name of the desired cluster* > **Services** > **Hue**.

Paso 17 Elija **More** > **Restart Service** y haga clic en **OK**.

Paso 18 Verifique si la alarma se ha borrado.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 19**.

Paso 19 Póngase en contacto con el y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.169 ALM-23001 Servicio de Loader no disponible

Descripción

El sistema comprueba la disponibilidad del servicio del Loader cada 60 segundos. Esta alarma se genera cuando el sistema detecta que el servicio Loader no está disponible. Esta alarma se borra cuando el servicio del Loader está disponible.

Atributo

ID de alarma	Gravedad de la alarma	Borrado automáticamente
23001	Crítica	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

Cuando el servicio Loader no está disponible, las funciones de carga, importación y conversión de datos no están disponibles.

Causas posibles

- El servicio interno del que depende el servicio del Loader es anormal.
  - El servicio ZooKeeper es anormal.
  - El servicio HDFS es anormal.
  - El servicio DBService es anormal.
  - El servicio Yarn es anormal.
  - El servicio Mapreduce es anormal.
- Falla del entorno: La red es anormal, por lo que el servicio Loader no puede comunicarse con los servicios internos dependientes y no puede proporcionar servicios.
- Falla del software: El servicio Loader no puede ejecutarse correctamente.

Procedimiento

Verificar el estado del servicio de ZooKeeper.

Paso 1 En la página de inicio del FusionInsight Manager, seleccione **Cluster** > *Name of the desired cluster* > **Services** > **ZooKeeper** para comprobar si el estado de ejecución del ZooKeeper es **Normal**.

- En caso afirmativo, vaya a **Paso 3**.

- Si no, vaya a **Paso 2**.

Paso 2 Elija **More** > **Restart Service** para reiniciar el servicio ZooKeeper. En la lista de alarmas, compruebe si **LoaderService no disponible** está borrada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 3**.

Paso 3 En el FusionInsight Manager, compruebe si la lista de alarmas contiene **Process Fault**.

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 7**.

Paso 4 En el área **Location** de **Process Fault**, compruebe si **ServiceName** es **ZooKeeper**.

- En caso afirmativo, vaya a **Paso 5**.
- Si no, vaya a **Paso 7**.

Paso 5 Rectifique la falla siguiendo los pasos indicados en **ALM-12007 Falla de proceso**.

Paso 6 En la lista de alarmas, compruebe si **Servicio Loader no disponible** está borrada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 7**.

Comprobar el estado de servicio HDFS.

Paso 7 En el FusionInsight Manager, compruebe si la lista de alarmas contiene **HDFS Service Unavailable**.

- En caso afirmativo, vaya a **Paso 8**.
- Si no, vaya a **Paso 10**.

Paso 8 Rectifique la falla siguiendo los pasos indicados en **ALM-14000 Servicio HDFS no disponible**.

Paso 9 En la lista de alarmas, compruebe si **Servicio Loader no disponible** está borrada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 10**.

Comprobar el estado de DBService.

Paso 10 En la página principal del FusionInsight Manager, seleccione **Cluster** > *Name of the desired cluster* > **Services** > **DBService** para comprobar si el estado de ejecución de DBService es de **Normal**.

- En caso afirmativo, vaya a **Paso 12**.
- Si no, vaya a **Paso 11**.

Paso 11 Elija **More** > **Restart Service** para reiniciar el servicio DBService. En la lista de alarmas, compruebe si **LoaderService no disponible** está borrada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 12**.

Comprobar el estado de Mapreduce.

Paso 12 En la página principal del FusionInsight Manager, seleccione **Cluster** > *Name of the desired cluster* > **Services** > **Mapreduce** para comprobar si el estado de ejecución de Mapreduce es de **Normal**.

- En caso afirmativo, vaya a **Paso 16**.
- Si no, vaya a **Paso 13**.

Paso 13 Elija **More** > **Restart Service** para reiniciar el servicio Mapreduce. En la lista de alarmas, compruebe si **LoaderService no disponible** está borrada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 16**.

Comprobar el estado de Yarn.

Paso 14 En la página de inicio del FusionInsight Manager, seleccione **Cluster** > *Name of the desired cluster* > **Services** > **Yarn** para comprobar si el estado de ejecución del Yarn es de **Normal**.

- En caso afirmativo, vaya a **Paso 16**.
- Si no, vaya a **Paso 15**.

Paso 15 Elija **More** > **Restart Service** para reiniciar el servicio de Yarn. En la lista de alarmas, compruebe si **LoaderService no disponible** está borrada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 16**.

Paso 16 En el FusionInsight Manager, compruebe si la lista de alarmas contiene **Servicio Yarn no disponible**.

- En caso afirmativo, vaya a **Paso 17**.
- Si no, vaya a **Paso 19**.

Paso 17 Rectifique la falla siguiendo los pasos indicados en **ALM-18000 Servicio Yarn no disponible**.

Paso 18 En la lista de alarmas, compruebe si **Servicio Loader no disponible** está borrada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 19**.

Comprobar la conexión de red entre Loader y los componentes dependientes.

Paso 19 En el FusionInsight Manager, elija **Cluster** > *Name of the desired cluster* > **Services** > **Loader**.

Paso 20 Haga clic en **Instance** y aparecerá la lista de instancias LoaderServer.

Paso 21 Registra el **Management IP Address** en la fila de **LoaderServer(Active)**.

Paso 22 Inicie sesión en el host donde se ejecuta el LoaderServer activo como usuario **omm** usando la dirección IP obtenida en **Paso 21**.

Paso 23 Ejecute el comando **ping** para comprobar si la comunicación entre el host que ejecuta el LoaderServer activo y los hosts que ejecutan los componentes dependientes. (Los componentes dependientes incluyen ZooKeeper, DBService, HDFS, Mapreduce y Yarn. Obtenga las direcciones IP de los hosts que ejecutan estos servicios de la misma manera que para obtener la dirección IP del LoaderServer activo.)

- En caso afirmativo, vaya a **Paso 26**.
- Si no, vaya a **Paso 24**.

Paso 24 Póngase en contacto con el administrador para restaurar la red.

Paso 25 En la lista de alarmas, compruebe si **Servicio Loader no disponible** está borrada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 26**.

Recopilar información de fallas.

Paso 26 En el FusionInsight Manager, elija **O&M** > **Log** > **Download**.

Paso 27 Seleccione los siguientes nodos en el clúster requerido en la lista desplegable **Service**:

- ZooKeeper
- HDFS
- DBService
- Yarn
- Mapreduce
- Loader

Paso 28 Haga clic en  en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 29 En el FusionInsight Manager, elija **Cluster** > *Name of the desired cluster* > **Services** > **Loader**.

Paso 30 Elija **More** > **Restart Service** y haga clic en **OK**.

Paso 31 Verifique si la alarma se ha borrado.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 32**.

Paso 32 Póngase en contacto con el y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.170 ALM-23003 Error de ejecución de tareas del Loader

Descripción

Esta alarma se genera inmediatamente cuando el sistema detecta que el trabajo del Loader falla. Esta alarma se borra cuando el trabajo fallido es manejado manualmente por un usuario. Esta alarma debe borrarse manualmente.

Atributo

ID de alarma	Gravedad de la alarma	Borrado automáticamente
23003	Leves	No

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
JobID	Especifica el ID del trabajo de Loader fallido.
JobName	Especifica el trabajo de cargador fallido.
UserName	Especifica el nombre del usuario que envía el trabajo Loader.
Details	Información complementaria para la que se genera la alarma.

Impacto en el sistema

Se produce una excepción durante la ejecución del trabajo de cargador enviado y la ejecución falla. No se puede obtener ningún resultado de ejecución. Ejecute el trabajo de nuevo después de rectificar la falla.

Causas posibles

- Los parámetros de tarea están configurados incorrectamente.
- Las excepciones se producen cuando Yarn está ejecutando un trabajo.

Procedimiento

Comprobar si los parámetros de la tarea están configurados incorrectamente.

Paso 1 En el FusionInsight Manager, seleccione **O&M** > **Alarm** > **Alarms** y haga clic en la lista desplegable de alarmas de la lista de alarmas, obtenga la **Alarm Cause**.

Paso 2 Si la causa de la alarma es "Failure to send job", vea los detalles del error de **Información adicional** y vaya al Loader WebUI para ver el historial de ejecución del trabajo.

NOTA

De forma predeterminada, el usuario **admin** no tiene los permisos para gestionar otros componentes. Si la página no se puede abrir o el contenido mostrado está incompleto al acceder a la interfaz de usuario nativa de un componente debido a la falta de permisos, puede crear manualmente un usuario con los permisos para gestionar ese componente.

Paso 3 Vuelva a enviar la tarea.

Paso 4 Compruebe si la tarea se ejecutó correctamente.

- En caso afirmativo, vaya a **Paso 9**.
- Si no, vaya a **Paso 5**.

Comprobar si se producen excepciones cuando Yarn está ejecutando un trabajo.

Paso 5 En FusionInsight Manager, haga clic en la lista desplegable de alarmas de la lista de alarmas y obtenga el **Alarm Cause**.

Paso 6 Compruebe si la actividad de Yarn se ejecuta correctamente en el **Alarm Cause**. Si la causa de la alarma es "Yarn execution failed", la actividad de Yarn es anormal.

- En caso afirmativo, vaya a **Paso 7**.
- Si no, vaya a **Paso 10**.

Paso 7 Vuelva a enviar la tarea.

Paso 8 Compruebe si la tarea se ejecutó correctamente.

- En caso afirmativo, vaya a **Paso 9**.
- Si no, vaya a **Paso 10**.

Paso 9 En la lista de alarmas, haga clic en **Clear** de **Operation** para borrar manualmente la alarma. No se requiere ninguna otra acción.

Recopilar información de fallas.

Paso 10 En FusionInsight Manager, elija **O&M** > **Log** > **Download**.

Paso 11 Seleccione los siguientes nodos en el clúster requerido en la lista desplegable **Service**:

- DBService
- HDFS
- Loader
- Mapreduce
- Yarn
- ZooKeeper

Paso 12 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 13 Póngase en contacto con el y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema no borra automáticamente esta alarma, y es necesario borrar manualmente la alarma.

Información relacionada

Ninguna

9.171 ALM-23004 El uso de memoria heap del Loader supera el umbral

Descripción

El sistema comprueba el uso de memoria heap del servicio Loader cada 60 segundos. La alarma se genera cuando el uso de memoria heap de una instancia de Loader excede el umbral (95% de la memoria máxima) durante 10 veces consecutivas. La alarma se borra cuando el uso de memoria heap es menor que el umbral.

Atributo

ID de alarma	Gravedad de la alarma	Borrado automáticamente
23004	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger Condition	Especifica el umbral que activa la alarma. Si el valor del indicador actual excede este umbral, se genera la alarma.

Impacto en el sistema

El desbordamiento de la memoria heap puede provocar una avería del servicio.

Causas posibles

La memoria heap de la instancia de Loader se utiliza en exceso o la memoria heap se asigna de forma inadecuada.

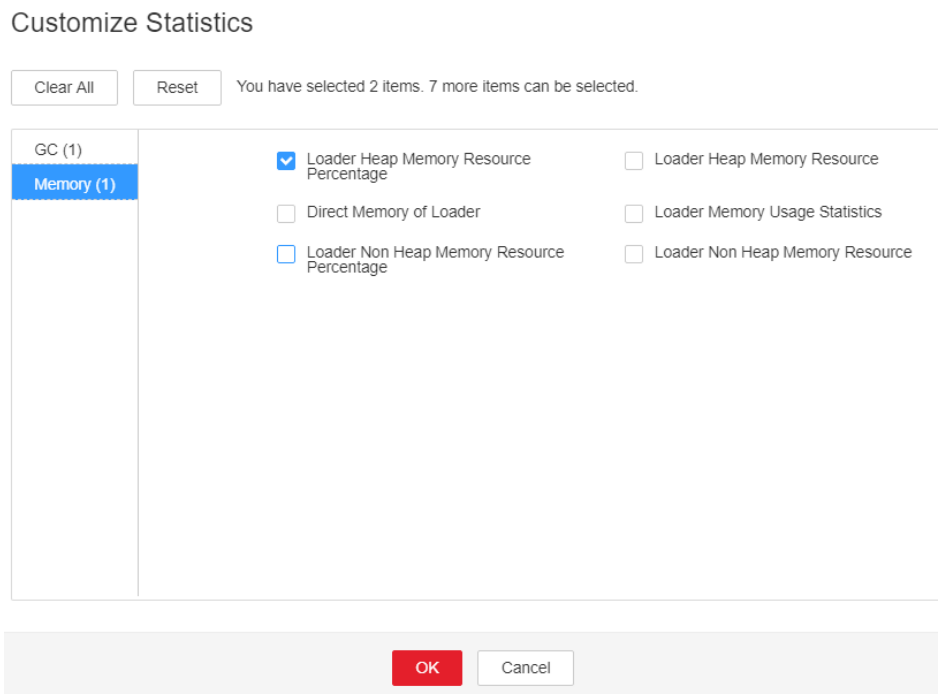
Procedimiento

Comprobar el uso de memoria heap.

Paso 1 En el portal de FusionInsight Manager, elija **O&M** > **Alarm** > **Alarms** > **Loader Heap Memory Usage Exceeds the Threshold** > **Location.** Compruebe el nombre de host de la instancia involucrada en esta alarma.

Paso 2 En el portal de FusionInsight Manager, seleccione **Cluster** > *Name of the desired cluster* > **Services** > **Loader** > **Instance**. Haga clic en la instancia para la que se genera la alarma para ir a la página de la instancia. Haga clic en el menú desplegable en el área del gráfico y elija **Customize** > **Memory** > **Loader Heap Memory Resource Percentage**. Haga clic en **OK**.

Figura 9-64 Porcentaje de recursos de memoria heap de Loader



Paso 3 Compruebe si la memoria heap usada de Loader alcanza el umbral (el valor predeterminado es el 95% de la memoria heap máxima) especificado para Loader.

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 6**.

Paso 4 En el portal del FusionInsight Manager, seleccione **Cluster** > *Name of the desired cluster* > **Services** > **Loader** > **Configurations**. Haga clic en **All Configurations**. Aumente el valor de **-Xmx** en **GC_OPTS** según sea necesario y haga clic en **Save**. Haga clic en **OK**.

NOTA

- Si se genera esta alarma, la memoria heap configurada para la instancia de Loader actual es insuficiente para la transmisión de datos. Se recomienda abrir la página de supervisión de instancias, mostrar el gráfico de supervisión de estado de recursos de memoria heap del Loader y observar la tendencia de cambio de la memoria heap utilizada por Loader en el gráfico de supervisión. A continuación, cambie el valor de **-Xmx** al doble del uso actual de memoria heap o a otro valor para cumplir con los requisitos del sitio.
- Al configurar la memoria de pila, puede establecer **-Xms** y **-Xmx** en valores similares para evitar el deterioro del rendimiento causado por el ajuste del tamaño de heap después de cada GC.
- Asegúrese de que la suma de **-Xmx** y **XX:MaxPermSize** no es mayor que la memoria física del servidor del nodo.

Paso 5 Reinicie los servicios o instancias afectados y compruebe si la alarma está desactivada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 6**.

Recopilar información de fallas.

Paso 6 En el portal del FusionInsight Manager, seleccione **O&M** > **Log** > **Download**.

Paso 7 Seleccione **Loader** en el clúster requerido en la lista desplegable **Service**.

Paso 8 Haga clic en  en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 9 Póngase en contacto con el y envíe los registros de fallas recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.172 ALM-23005 El uso de memoria de no heap de Loader supera el umbral

Descripción

El sistema comprueba el uso de memoria no acumulable del servicio Loader cada 30 segundos. La alarma se genera cuando el uso de memoria no heap de una instancia de Loader excede el umbral (80% de la memoria máxima) durante 5 veces consecutivas. La alarma se borra cuando el uso de memoria de no heap es menor que el umbral.

Atributo

ID de alarma	Gravedad de la alarma	Borrado automáticamente
23005	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger Condition	Especifica el umbral que activa la alarma. Si el valor del indicador actual excede este umbral, se genera la alarma.

Impacto en el sistema

El desbordamiento de la memoria no heap puede provocar una interrupción del servicio.

Causas posibles

La memoria no heap de la instancia de Loader se utiliza en exceso o la memoria no heap se asigna de forma inadecuada.

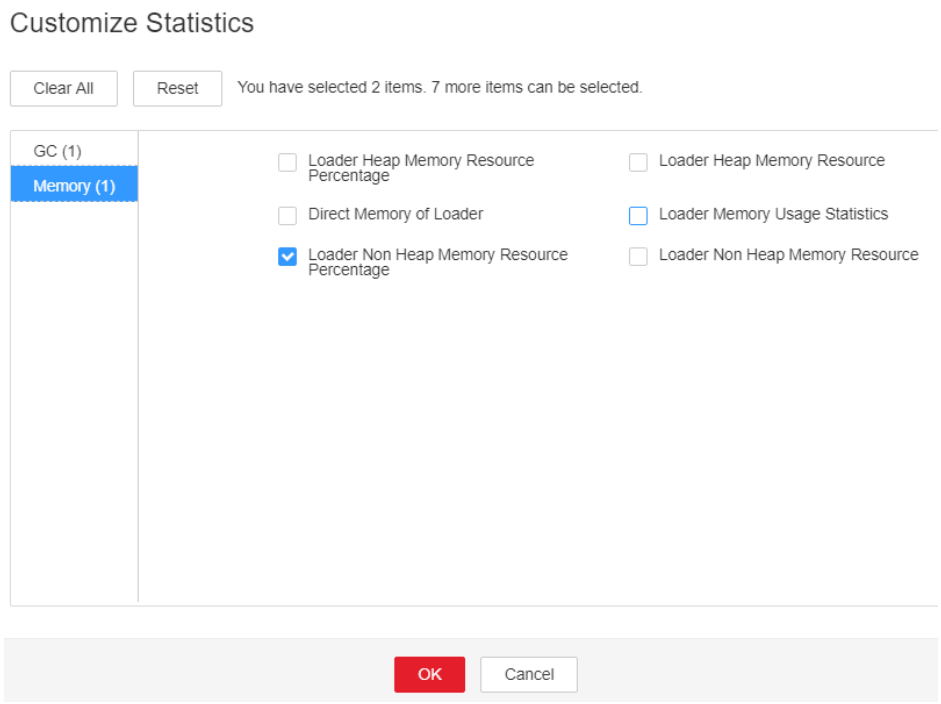
Procedimiento

Verifique el uso de memoria no heap.

Paso 1 En el portal del Administrador FusionInsight, elija **O&M** > **Alarm** > **Alarms** > **Loader Non-Heap Memory Usage Exceeds the Threshold** > **Location.** Compruebe el nombre de host de la instancia involucrada en esta alarma.

Paso 2 En el portal de FusionInsight Manager, seleccione **Cluster** > *Name of the desired cluster* > **Services** > **Loader** > **Instance**. Haga clic en la instancia para la que se genera la alarma para ir a la página de la instancia. Haga clic en el menú desplegable en el área del gráfico y elija **Customize** > **Memory** > **Loader Non Heap Memory Resource Percentage**. Haga clic en **OK**.

Figura 9-65 Porcentaje de recursos de memoria no heap del Loader



Paso 3 Comprobar si la memoria usada no heap de Loader alcanza el umbral (el valor predeterminado es el 80% de la memoria máxima que no es de almacenamiento dinámico) especificado para Loader.

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 6**.

Paso 4 En el portal del FusionInsight Manager, seleccione **Cluster** > *Name of the desired cluster* > **Services** > **Loader** > **Configurations**. Haga clic en **All Configurations** Buscar **LOADER_GC_OPTS** en el cuadro de búsqueda. Si el parámetro **-XX: MaxPermSize** no está configurado, establezca el valor inicial en **-XX: MaxPermSize=256M** por primera vez. (Si la alarma persiste después del primer ajuste, realice el segundo ajuste haciendo referencia a la siguiente nota.) Y haga clic en **Save**. Haga clic en **OK**.

NOTA

Si se genera esta alarma, la memoria no heap configurada para la instancia actual del Loader es insuficiente para el escenario de servicio. Se recomienda abrir la página de supervisión de instancias, abrir el gráfico de supervisión de estado de recursos de memoria no heap del Loader y observar la tendencia de cambio de la memoria no heap utilizada por Loader en el gráfico de supervisión. A continuación, cambie el valor de **-XX:MaxPermSize** a dos veces el uso actual de memoria no heap o a otro valor para cumplir con los requisitos del sitio.

Paso 5 Reinicie los servicios o instancias afectados y compruebe si la alarma está desactivada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 6**.

Recopilar información de fallas.

Paso 6 En el portal del FusionInsight Manager, seleccione **O&M** > **Log** > **Download**.

Paso 7 Seleccione **Loader** en el clúster requerido en la lista desplegable **Service**.

Paso 8 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 9 Póngase en contacto con el y envíe los registros de fallas recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.173 ALM-23006 El uso de memoria directa del Loader supera el umbral

Descripción

El sistema comprueba el uso de memoria directa del servicio Loader cada 30 segundos. La alarma se genera cuando el uso de memoria directa de una instancia de Loader excede el umbral (80% de la memoria máxima) durante 5 veces consecutivas. La alarma se borra cuando el uso de memoria directa del cargador es menor o igual al umbral.

Atributo

ID de alarma	Gravedad de la alarma	Borrado automáticamente
23006	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Nombre	Significado
Trigger Condition	Especifica el umbral que activa la alarma. Si el valor del indicador actual excede este umbral, se genera la alarma.

Impacto en el sistema

El desbordamiento de la memoria directa puede provocar una avería del servicio.

Causas posibles

La memoria directa de la instancia de Loader se utiliza en exceso o la memoria directa se asigna de forma inadecuada.

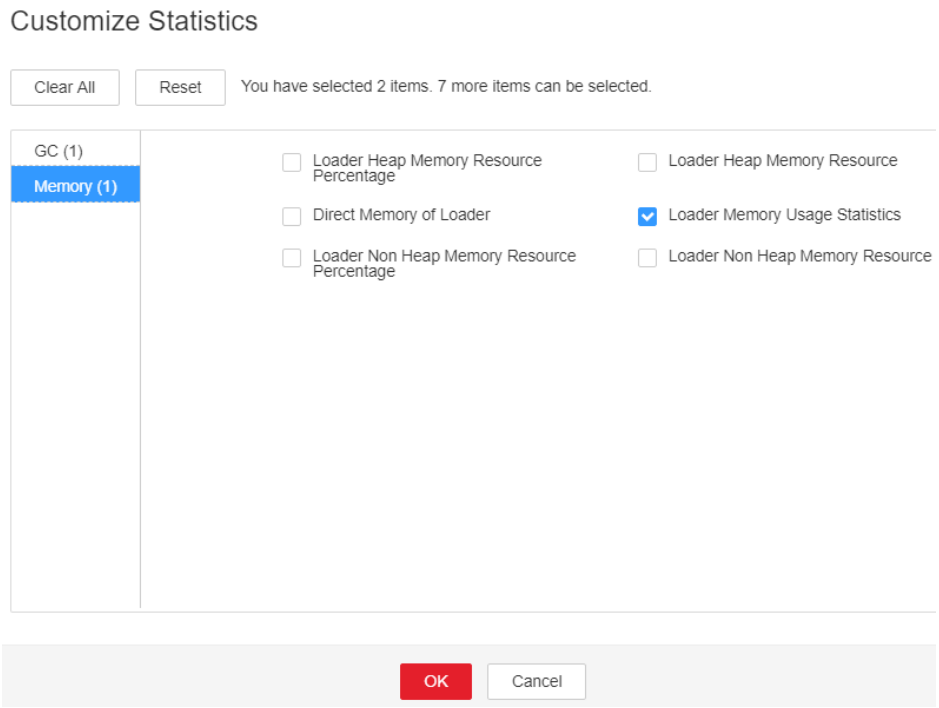
Procedimiento

Comprobar el uso de memoria directa.

Paso 1 En el portal del FusionInsight Manager, elija **O&M** > **Alarm** > **Alarms** > **Loader Direct Memory Usage Exceeds the Threshold** > **Location**. Compruebe el nombre de host de la instancia involucrada en esta alarma.

Paso 2 En el portal de FusionInsight Manager, seleccione **Cluster** > *Name of the desired cluster* > **Services** > **Loader** > **Instance**. Haga clic en la instancia para la que se genera la alarma para ir a la página de la instancia. Haga clic en el menú desplegable en el área del gráfico y elija **Customize** > **Memory** > **Loader Memory Usage Statistics**. Haga clic en **OK**.

Figura 9-66 Estadísticas de uso de memoria del Loader



Paso 3 Comprobar si la memoria directa utilizada de Loader alcanza el umbral (el valor predeterminado es 80% de la memoria directa máxima) especificado para Loader.

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 6**.

Paso 4 En el portal del FusionInsight Manager, seleccione **Cluster** > *Name of the desired cluster* > **Services** > **Loader** > **Configurations**. Haga clic en **All Configurations**. Busque **LOADER_GC_OPTS** en el cuadro de búsqueda. Aumente el valor de **-XX:MaxDirectMemorySize** según sea necesario y haga clic en **Save**. Haga clic en **OK**.

NOTA

Si se genera esta alarma, la memoria directa configurada para la instancia actual del Loader es insuficiente para el escenario de servicio. Se recomienda abrir la página de supervisión de instancias, mostrar el gráfico de supervisión de estado de recursos de memoria directa del cargador y observar la tendencia de cambio de la memoria directa utilizada por el Loader en el gráfico de supervisión. A continuación, cambie el valor de **-XX:MaxDirectMemorySize** al doble del uso actual de memoria directa o a otro valor para cumplir con los requisitos del sitio.

Paso 5 Reinicie los servicios o instancias afectados y compruebe si la alarma está desactivada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 6**.

Recopilar información de fallas.

Paso 6 En el portal del FusionInsight Manager, seleccione **O&M** > **Log** > **Download**.

Paso 7 Seleccione **Loader** en el clúster requerido en la lista desplegable **Service**.

Paso 8 Haga clic en  en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 9 Póngase en contacto con el y envíe los registros de fallas recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.174 ALM-23007 El tiempo de recolección de basura (GC) del proceso del Loader supera el umbral

Descripción

El sistema comprueba el tiempo de GC del proceso del cargador cada 60 segundos. La alarma se genera cuando el tiempo de GC del proceso del Loader excede el umbral (valor predeterminado **12 seconds**) durante 5 veces consecutivas. La alarma se borra cuando el tiempo de GC es menor que el umbral.

Atributo

ID de alarma	Gravedad de la alarma	Borrado automáticamente
23007	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger Condition	Especifica el umbral que activa la alarma. Si el valor del indicador actual excede este umbral, se genera la alarma.

Impacto en el sistema

La respuesta del servicio del Loader es lenta.

Causas posibles

La memoria heap de la instancia de Loader se utiliza en exceso o la memoria heap se asigna de forma inadecuada.

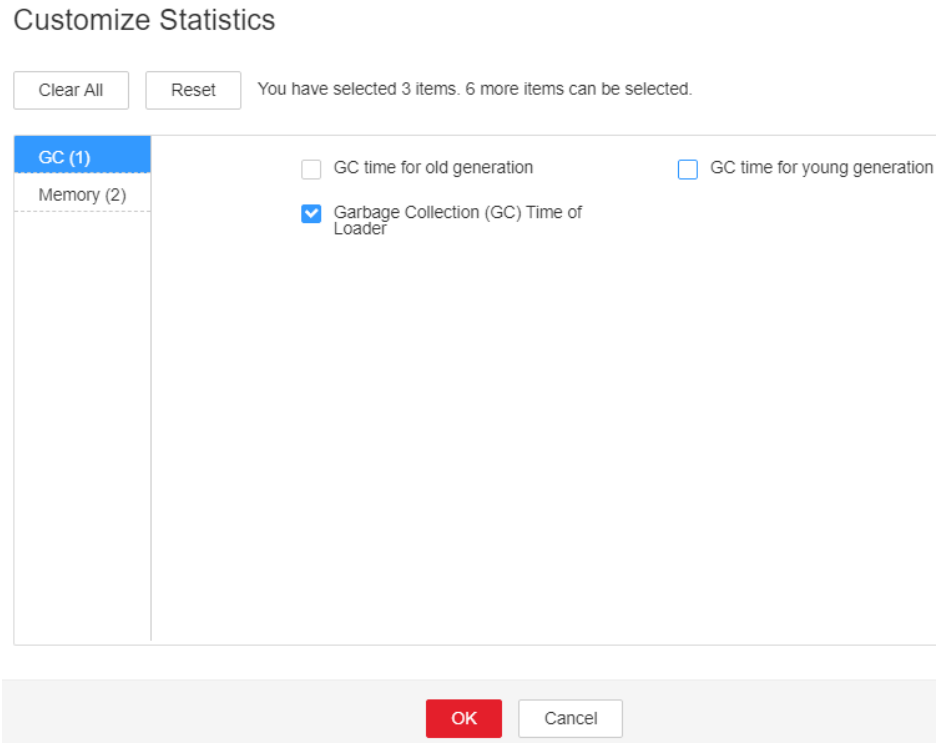
Procedimiento

Comprobar el tiempo de GC.

Paso 1 En el portal del FusionInsight Manager, elija **O&M** > **Alarm** > **Alarms** > **Garbage Collection (GC) Time of the Loader Process Exceeds the Threshold** > **Location**. Compruebe el nombre de host de la instancia involucrada en esta alarma.

Paso 2 En el portal de FusionInsight Manager, seleccione **Cluster** > *Name of the desired cluster* > **Services** > **Loader** > **Instance**. Haga clic en la instancia para la que se genera la alarma para ir a la página de la instancia. Haga clic en el menú desplegable en el área del chart y elija **Customize** > **GC** > **Garbage Collection (GC) Time of Loader**. Haga clic en **OK**.

Figura 9-67 Tiempo de Recolección de basura (GC) de Loader



Paso 3 Compruebe si el tiempo de GC del proceso del Loader excede cada segundo el umbral (valor predeterminado **12 seconds**).

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 6**.

Paso 4 En el portal del FusionInsight Manager, seleccione **Cluster** > *Name of the desired cluster* > **Services** > **Loader** > **Configurations**. Haga clic en **All Configurations**. Busque **LOADER_GC_OPTS** en el cuadro de búsqueda. Aumente el valor de **-Xmx** según sea necesario y haga clic en **Save**. Haga clic en **OK**.

NOTA

Si se genera esta alarma, la memoria heap configurada para la instancia actual del Loader no puede cumplir con la memoria heap requerida para la transmisión de datos. Le aconsejamos que solucione el problema haciendo referencia a **Paso 4** en la sección **ALM-23004 El uso de memoria heap del Loader supera el umbral**.

Paso 5 Reinicie los servicios o instancias afectados y compruebe si la alarma está desactivada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 6**.

Recopilar información de fallas.

Paso 6 En el portal del FusionInsight Manager, seleccione **O&M** > **Log** > **Download**.

Paso 7 Seleccione **Loader** en el clúster requerido en la lista desplegable **Service**.

Paso 8 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 9 Póngase en contacto con el y envíe los registros de fallas recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.175 ALM-24000 Servicio de Flume no disponible

Descripción

El módulo de alarma comprueba el estado de servicio de Flume cada 180 segundos. Esta alarma se genera si el servicio Flume es anormal.

Esta alarma se borra automáticamente una vez que se recupera el servicio Flume.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
24000	Crítica	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

Flume no puede funcionar y la transmisión de datos se interrumpe.

Causas posibles

Todas las instancias de Flume son defectuosas.

Procedimiento

Paso 1 Inicie sesión en un nodo Flume como usuario **omm** y ejecute el comando **ps -ef|grep "flume.role=server"** para comprobar si el proceso Flume existe en el nodo.

- En caso afirmativo, vaya a **Paso 3**.
- Si no, reinicie el nodo de Flume o el servicio de Flume defectuosos y vaya a **Paso 2**.

Paso 2 En la lista de alarmas, compruebe si la alarma "Servicio de Flume no disponible" está desactivada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 3**.

Recopilar información de fallas.

Paso 3 En FusionInsight Manager, seleccione **O&M**. En el panel de navegación de la izquierda, elija **Log** > **Download**.

Paso 4 Expanda la lista desplegable **Service** y seleccione **Flume** para el clúster de destino.

Paso 5 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 1 hora antes y después del tiempo de generación de alarma, respectivamente. A continuación, haga clic en **Download**.

Paso 6 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

Información relacionada

Ninguna

9.176 ALM-24001 Excepción de Flume Agent

Descripción

No se puede iniciar la instancia del Flume Agent para la que se genera la alarma. Esta alarma se genera cuando el proceso del Flume Agent está defectuoso (El sistema comprueba cada 5 segundos) o el Flume Agent no se inicia (El sistema informa de alarmas inmediatamente).

Esta alarma se borra cuando el proceso del Flume Agent se recupera, el agente de Flume se inicia con éxito y se completa el manejo de la alarma.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
24001	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
AgentId	Especifica el ID del agente para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

La instancia del Flume Agent para la que se genera la alarma no puede proporcionar servicios correctamente, y las tareas de transmisión de datos de la instancia se interrumpen temporalmente. Los datos en tiempo real se pierden durante la transmisión de datos en tiempo real.

Causas posibles

- El directorio JAVA_HOME no existe o el permiso Java es incorrecto.
- El permiso del directorio del Flume Agent es incorrecto.
- Flume Agent no se inicia.

Procedimiento

Comprobar si existe el directorio JAVA_HOME o si el permiso JAVA es correcto.

Paso 1 Inicie sesión en el host para el que se genera la alarma como usuario **root**.

Paso 2 Ejecute el siguiente comando para obtener el directorio de instalación del cliente Flume para el que se genera la alarma: (El valor de **AgentId** se puede obtener del **Location** de la alarma.)

ps -ef|grep *AgentId* **| grep -v grep | awk -F 'conf-file ' '{print $2}' | awk -F 'fusioninsight' '{print $1}'**

Paso 3 Ejecute el comando **su -** *Flume installation user* para cambiar al usuario de instalación de Flume y ejecute el comando **cd** *Flume client installation directory*/**fusioninsight-flume-1.9.0/conf/** para ir al directorio de configuración de Flume.

Paso 4 Ejecute el comando **cat ENV_VARS | grep JAVA_HOME**.

Paso 5 Compruebe si el directorio **JAVA_HOME** existe. Si la salida del comando de **Paso 4** no está vacía y **ll $JAVA_HOME/** no está vacía, el directorio **JAVA_HOME** existe.

- En caso afirmativo, vaya a **Paso 7**.

- Si no, vaya a **Paso 6**.

Paso 6 Especifique un directorio de **JAVA_HOME** correcto, por ejemplo, **export JAVA_HOME=${BIGDATA_HOME}/common/runtime0/jdk***Version number*.

Paso 7 Ejecute el comando **$JAVA_HOME/bin/java -version** para comprobar si el usuario en ejecución del Flume agent tiene el permiso de ejecución de Java. Si la versión de Java se muestra en la salida del comando, el permiso Java cumple con el requisito. De lo contrario, el permiso Java no cumple con el requisito.

- En caso afirmativo, vaya a **Paso 9**.
- Si no, vaya a **Paso 8**.

NOTA

JAVA_HOME es la variable de entorno exportada durante la instalación del cliente de Flume. También puede ir a *Flume client installation directory*/**fusioninsight-flume-1.9.0/conf** y ejecutar el comando **cat ENV_VARS | grep JAVA_HOME** para ver el valor de la variable.

Paso 8 Ejecute el comando **chmod 750 $JAVA_HOME/bin/java** para conceder el permiso de ejecución de Java al usuario en ejecución del Flume agent.

Comprobar el permiso de directorio del Flume agent.

Paso 9 Inicie sesión en el host para el que se genera la alarma como **root**.

Paso 10 Ejecute el siguiente comando para cambiar al directorio de instalación del Flume agent:

cd *Flume client installation directory*/**fusioninsight-flume-1.9.0/conf/**

Paso 11 Ejecute el comando **ls -al * -R** para comprobar si algún propietario de archivo es el usuario que ejecuta el Flume agent.

- En caso afirmativo, vaya a **Paso 12**.
- Si no, ejecute el comando **chown** para cambiar el propietario del archivo al usuario que ejecuta el Flume agent.

Comprobar la configuración de Flume agent.

Paso 12 Ejecute los comandos **cat properties.properties | grep spooldir** y **cat properties.properties | grep TAILDIR** para comprobar si el tipo de origen de Flume es spoolDir o tailDir. Si se muestra algún resultado de comando, el tipo de origen de Flume es spoolDir o tailDir.

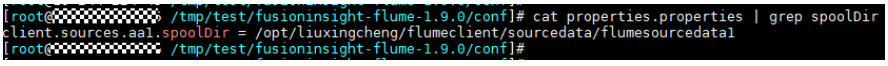
- En caso afirmativo, vaya a **Paso 13**.
- Si no, vaya a **Paso 17**.

Paso 13 Compruebe si existe el directorio de supervisión de datos.

- En caso afirmativo, vaya a **Paso 15**.
- Si no, vaya a **Paso 14**.

NOTA

Ejecute el comando **cat properties.properties | grep spoolDir** para ver el directorio de spoolDir.



Ejecute el comando **cat properties.properties | grep parentDir** para ver el directorio de monitoreo de tailDir.

Paso 14 Especifique un directorio de supervisión de datos correcto.

Paso 15 Compruebe si el usuario del agente de Flume tiene los permisos de lectura, escritura y ejecución en el directorio de supervisión especificado en **Paso 13**.

- En caso afirmativo, vaya a **Paso 17**.
- Si no, vaya a **Paso 16**.

NOTA

Vaya al directorio de supervisión como usuario en ejecución de Flume. Si se pueden crear archivos, el usuario en ejecución de Flume tiene los permisos de lectura, escritura y ejecución en el directorio de monitoreo.

Paso 16 Ejecute el comando **chmod 777** *Flume monitoring directory* para conceder al usuario en ejecución del Flume agent los permisos de lectura, escritura y ejecución en el directorio de supervisión especificado en el **Paso 13**.

Paso 17 Compruebe si los componentes conectados al sink de Flume están en modo seguro.

- En caso afirmativo, vaya a **Paso 18**.
- Si no, vaya a **Paso 23**.

NOTA

Si los sumideros del archivo de configuración **properties.properties** son el sink de HDFS, y el sink de HBase, y el archivo de configuración contiene un archivo keytab, los componentes conectados al sink de Flume están en modo seguro.

Si el sink en el archivo de configuración **properties.properties** es el sink kafka y ***.security.protocol** está establecido en **SASL_PLAINTEXT** o **SASL_SSL** el Kafka conectado al sink Flume está en modo seguro.

Paso 18 Ejecute el comando **ll** *ketab path* para comprobar si existe la ruta de autenticación keytab especificada por el parámetro ***.kerberosKeytab** en el archivo de configuración.

- En caso afirmativo, vaya a **Paso 20**.
- Si no, vaya a **Paso 19**.

NOTA

Para ver la ruta de acceso ketab, ejecute el comando **cat properties.properties | grep keytab**.

Paso 19 Cambie el valor de **kerberosKeytab** de **Paso 18** a la ruta de keytab personalizada y vaya a **Paso 21**.

Paso 20 Realice **Paso 18** para comprobar si el usuario en ejecución del Flume agent tiene permiso para acceder al archivo de autenticación de keytab. Si se devuelve la ruta del keytab, el usuario tiene el permiso. De lo contrario, el usuario no tiene el permiso.

- En caso afirmativo, vaya a **Paso 22**.
- Si no, vaya a **Paso 21**.

Paso 21 Ejecute el comando **chmod 755** *ketab file* para conceder el permiso de lectura en el archivo keytab especificado en **Paso 19** y reinicie el proceso Flume.

Paso 22 Verifique si la alarma se ha borrado.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 23**.

Recopilar información de fallas.

Paso 23 En FusionInsight Manager, seleccione **O&M**. En el panel de navegación de la izquierda, elija **Log** > **Download**.

Paso 24 Expanda la lista desplegable **Service** y seleccione **Flume** para el clúster de destino.

Paso 25 Haga clic en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 1 hora antes y después del tiempo de generación de alarma, respectivamente. A continuación, haga clic en **Download**.

Paso 26 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

Información relacionada

Ninguna

9.177 ALM-24003 Conexión de Flume client interrumpida

Descripción

El módulo de alarma supervisa el estado de la conexión del puerto en el Flume server. Esta alarma se genera si Flume server no recibe un mensaje de conexión del Flume client en tres minutos consecutivos.

Esta alarma se borra después de que el Flume server recibe un mensaje de conexión del Flume client.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
24003	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
Client IP Address	Especifica la dirección IP del cliente de Flume.
Client Name	Especifica el nombre del agente del cliente de Flume.

Nombre	Significado
Sink Name	Especifica el nombre del sink de Flume Agent.

Impacto en el sistema

La comunicación entre el Flume client y server falla. El Flume client no puede enviar datos al Flume server.

Causas posibles

- La conexión de red entre el Flume client y el server es defectuosa.
- El proceso del Flume client es anormal.
- El Flume client está configurado incorrectamente.

Procedimiento

Comprobar la conexión de red entre Flume client y Flume server.

Paso 1 Inicie sesión en el host cuya dirección IP es especificada por **Flume ClientIP** en la información de alarma como usuario **root**.

Paso 2 Ejecute el comando **ping** *Flume server IP address* para comprobar si la conexión de red entre Flume client y el server es normal.

- En caso afirmativo, vaya a **Paso 3**.
- Si no, vaya a **Paso 11**.

Comprobar si el proceso de Flume client es normal.

Paso 3 Inicie sesión en el host cuya dirección IP es especificada por **Flume ClientIP** en la información de alarma como usuario **root**.

Paso 4 Ejecute el comando **ps -ef|grep flume |grep client** para comprobar si existe el proceso Flume client.

- En caso afirmativo, vaya a **Paso 5**.
- Si no, vaya a **Paso 11**.

Comprobar la configuración de Flume client.

Paso 5 Inicie sesión en el host cuya dirección IP es especificada por **Flume ClientIP** en la información de alarma como usuario **root**.

Paso 6 Ejecute el comando **cd** *Flume client installation directory*/**fusioninsight-flume-1.9.0/conf/** para ir al directorio de configuración de Flume.

Paso 7 Ejecute el comando **cat properties.properties** para consultar el archivo de configuración actual del Flume client.

Paso 8 Compruebe si el archivo **properties.properties** está configurado correctamente de acuerdo con la descripción de configuración del agente de Flume.

- En caso afirmativo, vaya a **Paso 9**.

- Si no, vaya a **Paso 11**.

Paso 9 Modifique el archivo de configuración **properties.properties**.

Comprobar si la alarma se ha borrado.

Paso 10 Verifique si la alarma se ha borrado.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 11**.

Recopilar información de fallas.

Paso 11 En FusionInsight Manager, seleccione **O&M**. En el panel de navegación de la izquierda, elija **Log** > **Download**.

Paso 12 Expanda la lista desplegable **Service** y seleccione **Flume** para el clúster de destino.

Paso 13 Haga clic en  en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 1 hora antes y después del tiempo de generación de alarma, respectivamente. A continuación, haga clic en **Download**.

Paso 14 Recopile los registros en el directorio **/var/log/Bigdata/flume-client** del cliente Flume mediante una herramienta de transmisión.

Paso 15 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

Información relacionada

Ninguna

9.178 ALM-24004 Se produce una excepción cuando Flume lee datos

Descripción

El módulo de alarma monitoriza el estado de Flume Source. Esta alarma se genera inmediatamente cuando la duración en la que Source no puede leer los datos excede el umbral.

El umbral predeterminado es **0**, lo que indica que el umbral está deshabilitado. Puede cambiar el umbral modificando el archivo **properties.properties** en el directorio **conf**. Específicamente, modifique el parámetro **NoDatatime** de source requerido.

La alarma se borra cuando Source lee los datos y se completa el manejo de la alarma.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
24004	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
AgentId	Especifica el ID del agente para el que se genera la alarma.
ComponentType	Especifica el tipo de componente para el que se genera la alarma.
ComponentName	Especifica el nombre del componente para el que se genera la alarma.

Impacto en el sistema

Si se encuentran datos en el origen de datos y Flume Source continuamente no puede leer datos, la recopilación de datos se detiene.

Causas posibles

- Flume Source está defectuoso, por lo que los datos no se pueden enviar.
- La red está defectuosa, por lo que los datos no se pueden enviar.

Procedimiento

Comprobar si Flume Source está defectuoso.

Paso 1 Abra el archivo de configuración **properties.properties** en el PC local, busque **keyword type = spooldir** en el archivo y compruebe si el tipo de Flume source es spoolDir.

- En caso afirmativo, vaya a **Paso 2**.
- Si no, vaya a **Paso 3**.

Paso 2 Vea el directorio spoolDir para comprobar si todos los archivos ya se han transferido.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 5**.

> **NOTA**
>
> El directorio de monitorización de spooDir se especifica mediante el parámetro **.spoolDir** en el archivo de configuración **properties.properties**. Si se han transferido todos los archivos del directorio de supervisión, la extensión del nombre de archivo de todos los archivos del directorio de supervisión es **.COMPLETED**.

Paso 3 Abra el archivo de configuración **properties.properties** en el PC local, busque **org.apache.flume.source.kafka.KafkaSource** en el archivo y compruebe si el tipo de Flume source es Kafka.

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 7**.

Paso 4 Compruebe si se han agotado los datos del tema configurados por Kafka Source.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 5**.

Paso 5 En FusionInsight Manager, elija **Cluster** > *Name of the desired cluster* > **Services** > **Flume** > **Instance**.

Paso 6 Vaya a la página de instancia de Flume del nodo defectuoso para comprobar si el indicador **Source Speed Metrics** en la alarma es 0.

- En caso afirmativo, vaya a **Paso 11**.
- Si no, vaya a **Paso 7**.

Verificar la conexión de red entre el nodo defectuoso y el nodo que corresponde a la dirección IP de Flume Source.

Paso 7 Abra el archivo de configuración **properties.properties** en el PC local, busque **type = avro** en el archivo y compruebe si el tipo de Flume source es Avro.

- En caso afirmativo, vaya a **Paso 8**.
- Si no, vaya a **Paso 11**.

Paso 8 Inicie sesión en el nodo defectuoso como usuario **root**, y ejecute el comando **ping** *IP address of the Flume source* para comprobar si el host del mismo nivel se puede hacer ping correctamente.

- En caso afirmativo, vaya a **Paso 11**.
- Si no, vaya a **Paso 9**.

Paso 9 Póngase en contacto con el administrador de red para restaurar la red.

Paso 10 En la lista de alarmas, compruebe si la alarma se borra después de un período.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 11**.

Recopilar información de fallas.

Paso 11 En FusionInsight Manager, seleccione **O&M**. En el panel de navegación de la izquierda, elija **Log** > **Download**.

Paso 12 Expanda la lista desplegable **Service** y seleccione **Flume** para el clúster de destino.

Paso 13 Haga clic en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 1 hora antes y después del tiempo de generación de alarma, respectivamente. A continuación, haga clic en **Download**.

Paso 14 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

Información relacionada

Ninguna

9.179 ALM-24005 Se produce una excepción cuando Flume transmite datos

Descripción

El módulo de alarma monitoriza el estado de capacidad de Flume Channel. La alarma se genera inmediatamente cuando la duración en la que el Channel está completamente ocupado excede el umbral o el número de veces que la Source no envía datos al Channel excede el umbral.

El umbral predeterminado es **10**. Puede cambiar el umbral modificando el parámetro **channelfullcount** del channel relacionado en el archivo de configuración **properties.properties** del directorio **conf**.

La alarma se borra cuando se libera el espacio del Flume Channel y se completa el manejo de la alarma.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
24005	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
AgentId	Especifica el ID del agente para el que se genera la alarma.

Nombre	Significado
ComponentType	Especifica el tipo del componente para el que se genera la alarma.
ComponentName	Especifica el componente para el que se genera la alarma.

Impacto en el sistema

Si el uso del disco de Flume Channel aumenta continuamente, el tiempo necesario para importar datos a un destino específico se prolonga. Cuando el uso del disco de Flume Channel alcanza el 100%, el proceso del agente de Flume se detiene.

Causas posibles

- Flume Sink está defectuoso, por lo que los datos no se pueden enviar.
- La red está defectuosa, por lo que los datos no se pueden enviar.

Procedimiento

Compruobar si Flume Sink está defectuoso.

Paso 1 Abra el archivo de configuración **properties.properties** en el PC local, busque **type = hdfs** en el archivo y compruebe si el tipo de Flume sink es HDFS.

- En caso afirmativo, vaya a **Paso 2**.
- Si no, vaya a **Paso 3**.

Paso 2 En FusionInsight Manager, compruebe si se genera una alarma **HDFS Service Unavailable** en la lista de alarmas y si el servicio HDFS está detenido en la lista de servicios.

- Si se informa de la alarma, bórrela de acuerdo con las sugerencias de manejo de ALM-14000 El servicio HDFS no disponible; si el servicio HDFS está detenido, inícielo. A continuación, vaya a **Paso 7**.
- Si no, vaya a **Paso 7**.

Paso 3 Abra el archivo de configuración **properties.properties** en el PC local, busque **type = hbase** en el archivo y compruebe si el tipo de Flume sink es HBase.

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 5**.

Paso 4 En FusionInsight Manager, compruebe si se genera una alarma **HBase Service Unavailable** en la lista de alarmas y si el servicio HBase está detenido en la lista de servicios.

- Si se informa de la alarma, bórrela de acuerdo con las sugerencias de manejo de ALM-19000 El servicio HBase no disponible; si se detiene el servicio HBase, inícielo. A continuación, vaya a **Paso 7**.
- Si no, vaya a **Paso 7**.

Paso 5 Abra el archivo de configuración **properties.properties** en el PC local, busque **org.apache.flume.sink.kafka.KafkaSink** en el archivo y compruebe si el tipo de Flume sink es Kafka.

- En caso afirmativo, vaya a **Paso 6**.
- Si no, vaya a **Paso 9**.

Paso 6 En FusionInsight Manager, compruebe si se genera una alarma **Kafka Service Unavailable** en la lista de alarmas y si el servicio Kafka está detenido en la lista de servicios.

- Si se informa de la alarma, bórrela de acuerdo con las sugerencias de manejo de ALM-38000 El servicio Kafka no disponible; si el servicio Kafka está detenido, inícielo. A continuación, vaya a **Paso 7**.
- Si no, vaya a **Paso 7**.

Paso 7 En FusionInsight Manager, elija **Cluster** > *Name of the desired cluster* > **Services** > **Flume** > **Instance**.

Paso 8 Vaya a la página de instancia de Flume del nodo defectuoso para comprobar si el indicador **Sink Speed Metrics** es 0.

- En caso afirmativo, vaya a **Paso 13**.
- Si no, vaya a **Paso 9**.

Verificar la conexión de red entre el nodo defectuoso y el nodo que corresponde a la dirección IP del Flume Sink.

Paso 9 Abra el archivo de configuración **properties.properties** en el PC local, busque **type = avro** en el archivo y compruebe si el tipo de Flume sink es Avro.

- En caso afirmativo, vaya a **Paso 10**.
- Si no, vaya a **Paso 13**.

Paso 10 Inicie sesión en el nodo defectuoso como usuario **root** y ejecute el comando **ping** *IP address of the Flume sink* para comprobar si se puede hacer ping con éxito al host del mismo nivel.

- En caso afirmativo, vaya a **Paso 13**.
- Si no, vaya a **Paso 11**.

Paso 11 Póngase en contacto con el administrador de red para restaurar la red.

Paso 12 En la lista de alarmas, compruebe si la alarma se borra después de un período.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 13**.

Recopilar información de fallas.

Paso 13 En FusionInsight Manager, seleccione **O&M**. En el panel de navegación de la izquierda, elija **Log** > **Download**.

Paso 14 Expanda la lista desplegable **Service** y seleccione **Flume** para el clúster de destino.

Paso 15 Haga clic en  en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 1 hora antes y después del tiempo de generación de alarma, respectivamente. A continuación, haga clic en **Download**.

Paso 16 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

Información relacionada

Ninguna

9.180 ALM-24006 El uso de memoria heap de Flume Server supera el umbral

Descripción

El sistema comprueba el uso de memoria heap del servicio Flume cada 60 segundos. Esta alarma se genera cuando el uso de memoria heap de la instancia Flume supera el umbral (95% de la memoria máxima) durante 10 veces consecutivas. Esta alarma se borra cuando el uso de memoria heap es menor que el umbral.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
24006	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger Condition	Especifica el umbral para activar la alarma.

Impacto en el sistema

El desbordamiento de la memoria heap puede causar una falla en el servicio.

Causas posibles

La memoria heap de la instancia de Flume se utiliza en exceso o la memoria heap se asigna de forma inadecuada.

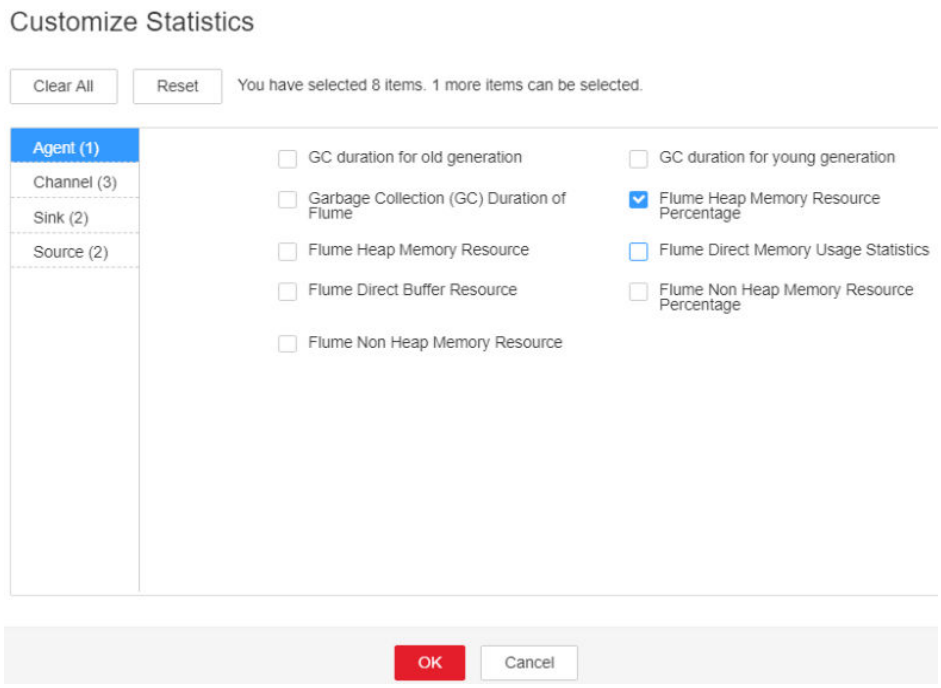
Procedimiento

Comprobar el uso de la memoria heap.

Paso 1 Inicie sesión en el administrador de FusionInsight y elija **O&M**. En el panel de navegación de la izquierda, elija **Alarm** > **Alarms**. En la página que se muestra, busque la fila que contiene **Flume Heap Memory Usage Exceeds the Threshold** y vea la información del **Location**. Compruebe el nombre del host para el que se genera la alarma.

Paso 2 En FusionInsight Manager, seleccione **Cluster** > *Name of the target cluster* > **Services** > **Flume**. En la página que se muestra, haga clic en la pestaña **Instance**. En la pestaña mostrada, seleccione el rol correspondiente al nombre de host para el que se genera la alarma y seleccione **Customize** en la lista desplegable en la esquina superior derecha del área del gráfico. Elija **Agent** y seleccione **Flume Heap Memory Resource Percentage**. A continuación, haga clic en **OK**.

Figura 9-68 Porcentaje de recursos de memoria heap de Flume



Paso 3 Compruebe si la memoria heap utilizada por Flume alcanza el umbral (95% de la memoria heap máxima de forma predeterminada).

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 6**.

Paso 4 En el Administrador de FusionInsight, seleccione **Cluster** > *Name of the desired cluster* > **Service** > **Flume** > **Configuration**. En la página que se muestra, haga clic en **All Configurations** y elija **Flume** > **System**. Establezca **-Xmx** en el parámetro **GC_OPTS** a un valor mayor según los requisitos del sitio y guarde la configuración.

NOTA

Si se genera esta alarma, la memoria heap configurada para el Flume server es insuficiente para la transmisión de datos. Se recomienda cambiar la memoria heap a: Capacidad del canal x Tamaño máximo de un solo registro de datos x Número de canales. Tenga en cuenta que el valor de **xmx** no puede exceder la memoria restante del nodo.

Paso 5 Reinicie los servicios o instancias afectados y compruebe si la alarma está desactivada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 6**.

Recopilar información de fallas.

Paso 6 En FusionInsight Manager, seleccione **O&M**. En el panel de navegación de la izquierda, elija **Log** > **Download**.

Paso 7 Expanda la lista desplegable **Service** y seleccione **Flume** para el clúster de destino.

Paso 8 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 9 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

Información relacionada

Ninguna

9.181 ALM-24007 El uso de memoria directa del servidor Flume supera el umbral

Descripción

El sistema comprueba el uso directo de memoria del servicio Flume cada 60 segundos. Esta alarma se genera cuando el uso directo de memoria de la instancia Flume supera el umbral (80% de la memoria máxima) durante cinco veces consecutivas. Esta alarma se borra cuando el uso de memoria directa de Flume es menor o igual que el umbral.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
24007	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger Condition	Especifica el umbral para activar la alarma.

Impacto en el sistema

El desbordamiento de la memoria directa puede provocar una falla en el servicio.

Causas posibles

La memoria directa del proceso Flume se utiliza en exceso o la memoria directa se asigna de forma inadecuada.

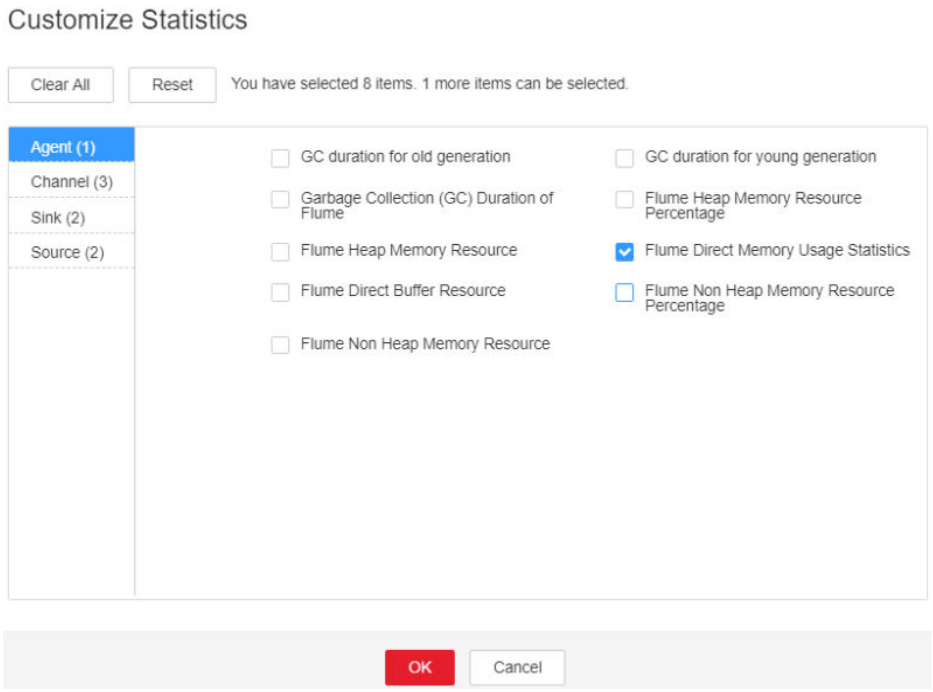
Procedimiento

Comprobar el uso de la memoria directa.

Paso 1 Inicie sesión en FusionInsight Manager y elija **O&M**. En el panel de navegación de la izquierda, elija **Alarm** > **Alarms**. En la página que se muestra, busque la fila que contiene **Flume Direct Memory Usage Exceeds the Threshold** y vea la información del **Location**. Compruebe el nombre del host para el que se genera la alarma.

Paso 2 En FusionInsight Manager, seleccione **Cluster** > *Name of the target cluster* > **Services** > **Flume**. En la página que se muestra, haga clic en la pestaña **Instance**. En la pestaña mostrada, seleccione el rol correspondiente al nombre de host para el que se genera la alarma y seleccione **Customize** en la lista desplegable en la esquina superior derecha del área del gráfico. Elija **Agent** y seleccione **Flume Direct Memory Resource Percentage**. A continuación, haga clic en **OK**.

Figura 9-69 Estadísticas de uso de memoria directa de Flume



Paso 3 Compruebe si la memoria directa utilizada por Flume alcanza el umbral (80% de la memoria directa máxima por defecto).

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 6**.

Paso 4 En FusionInsight Manager, seleccione **Cluster** > *Name of the desired cluster* > **Service** > **Flume** > **Configuration**. En la página que se muestra, haga clic en **All Configurations** y elija **Flume** > **System**. Establezca **-XX:MaxDirectMemorySize** en el parámetro **GC_OPTS** a un valor mayor según los requisitos del sitio y guarde la configuración.

NOTA

Si se genera esta alarma, el tamaño de memoria directa configurado para la instancia del servidor Flume no puede cumplir con los requisitos de servicio. Se recomienda cambiar el valor de **-XX:MaxDirectMemorySize** al doble del tamaño actual de memoria directa o cambiar el valor según los requisitos del sitio.

Paso 5 Reinicie los servicios o instancias afectados y compruebe si la alarma está desactivada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 6**.

Recopilar información de fallas.

Paso 6 En FusionInsight Manager, seleccione **O&M**. En el panel de navegación de la izquierda, elija **Log** > **Download**.

Paso 7 Expanda la lista desplegable **Service** y seleccione **Flume** para el clúster de destino.

Paso 8 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 9 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

Información relacionada

Ninguna

9.182 ALM-24008 El uso de memoria no heap del Flume Server supera el umbral

Descripción

El sistema comprueba el uso de memoria no heap del servicio Flume cada 60 segundos. Esta alarma se genera cuando el uso de memoria no heap de la instancia Flume supera el umbral (80% de la memoria máxima) durante cinco veces consecutiva. Esta alarma se borra cuando el uso de memoria no heap es menor que el umbral.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
24008	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger Condition	Especifica el umbral para activar la alarma.

Impacto en el sistema

El desbordamiento de la memoria no heap puede provocar una falla en el servicio.

Causas posibles

La memoria no heap de la instancia de Flume se sobreutiliza o la memoria no heap se asigna de forma inadecuada.

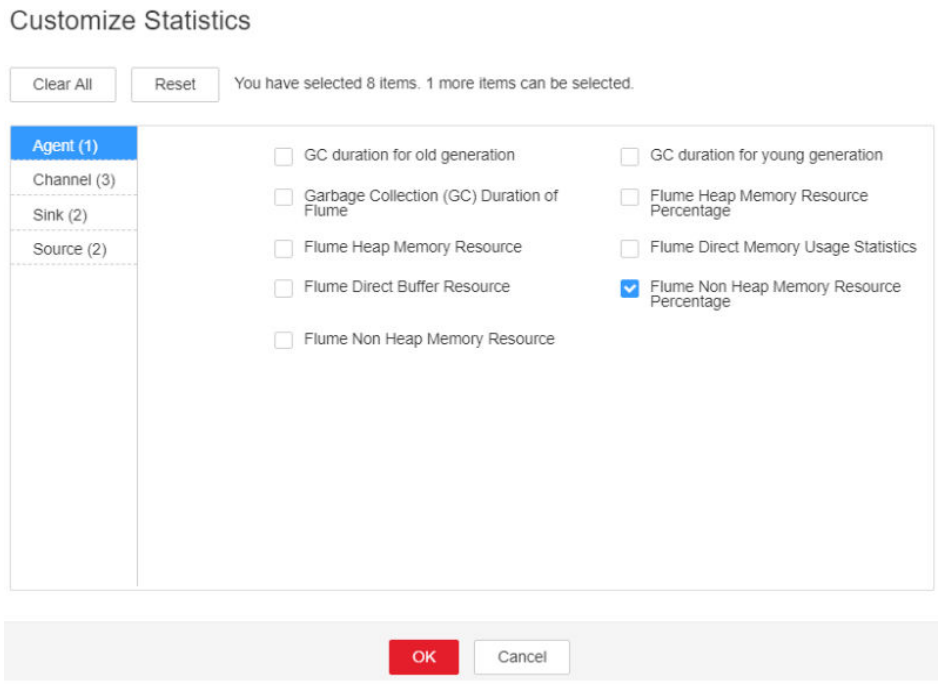
Procedimiento

Verificar el uso de memoria no heap.

Paso 1 Inicie sesión en el FusionInsight Manager y elija **O&M**. En el panel de navegación de la izquierda, elija **Alarm** > **Alarms**. En la página que se muestra, busque la fila que contiene **Flume Non Heap Memory Usage Exceeds the Threshold** y vea la información del **Location**. Compruebe el nombre del host para el que se genera la alarma.

Paso 2 En FusionInsight Manager, seleccione **Cluster** > *Name of the target cluster* > **Services** > **Flume**. En la página que se muestra, haga clic en la pestaña **Instance**. En la pestaña mostrada, seleccione el rol correspondiente al nombre de host para el que se genera la alarma y seleccione **Customize** en la lista desplegable en la esquina superior derecha del área del gráfico. Elija **Agent** y seleccione **Flume Non Heap Memory Resource Percentage**. A continuación, haga clic en **OK**.

Figura 9-70 Porcentaje de recursos de memoria no heap de Flume



Paso 3 Compruebe si la memoria no heap utilizada por Flume alcanza el umbral (80% de la memoria no heap máxima de forma predeterminada).

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 6**.

Paso 4 En FusionInsight Manager, seleccione **Cluster** > *Name of the desired cluster* > **Service** > **Flume** > **Configuration**. En la página que se muestra, haga clic en **All Configurations** y elija **Flume** > **System**. Establezca **-XX: MaxPermSize** en el parámetro **GC_OPTS** a un valor mayor según los requisitos del sitio y guarde la configuración.

NOTA

Si se genera esta alarma, el tamaño de memoria no heap configurado para la instancia del Flume server no puede cumplir con los requisitos de servicio. Se recomienda cambiar el valor de **-XX:MaxPermSize** al doble del tamaño actual de memoria no heap o cambiar el valor en función de los requisitos del sitio.

Paso 5 Reinicie los servicios o instancias afectados y compruebe si la alarma está desactivada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 6**.

Recopilar información de fallas.

Paso 6 En FusionInsight Manager, seleccione **O&M**. En el panel de navegación de la izquierda, elija **Log** > **Download**.

Paso 7 Expanda la lista desplegable **Service** y seleccione **Flume** para el clúster de destino.

Paso 8 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 9 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

Información relacionada

Ninguna

9.183 ALM-24009 El tiempo de recolección de basura (GC) del Flume Server supera el umbral

Descripción

El sistema comprueba la duración de GC del proceso de Flume cada 60 segundos. Esta alarma se genera cuando la duración de GC del proceso de Flume supera el umbral (12 segundos por defecto) durante cinco veces consecutivas. Esta alarma se borra cuando la duración de GC es menor que el umbral.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
24009	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger Condition	Especifica el umbral para activar la alarma.

Impacto en el sistema

La eficiencia de transmisión de datos de Flume disminuye.

Causas posibles

La memoria heap del proceso Flume se usa en exceso o se asigna de forma inadecuada, lo que provoca la ocurrencia frecuente del proceso de GC.

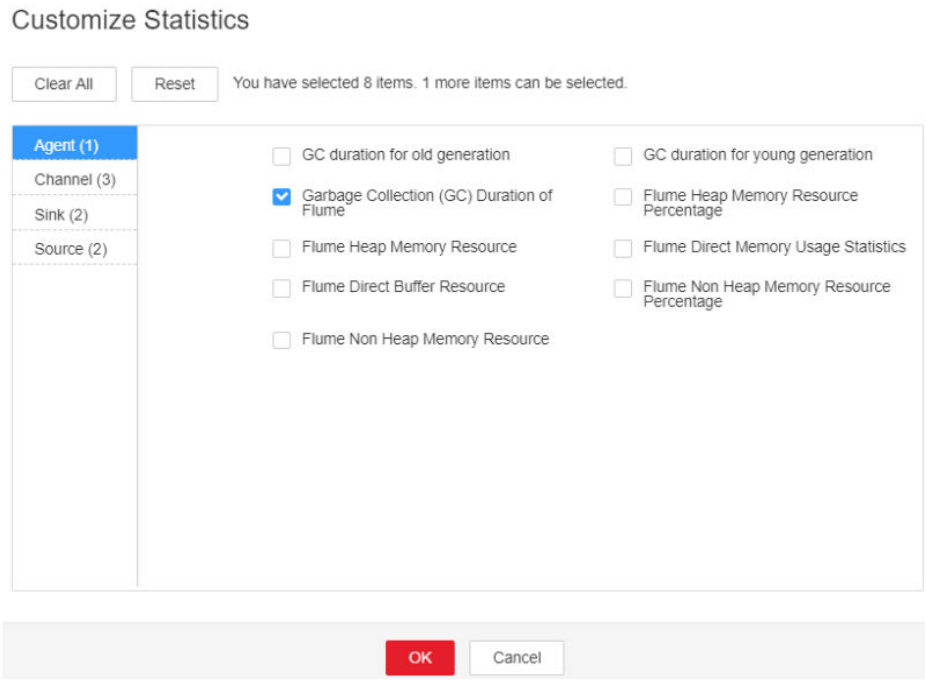
Procedimiento

Comprobar la duración del GC.

Paso 1 Inicie sesión en el FusionInsight Manager y elija **O&M**. En el panel de navegación de la izquierda, elija **Alarm** > **Alarms**. En la página que se muestra, busque la fila que contiene **GC Duration Exceeds the Threshold** y vea la información del **Location**. Compruebe el nombre del host para el que se genera la alarma.

Paso 2 En FusionInsight Manager, seleccione **Cluster** > *Name of the target cluster* > **Services** > **Flume**. En la página que se muestra, haga clic en la pestaña **Instance**. En la pestaña mostrada, seleccione el rol correspondiente al nombre de host para el que se genera la alarma y seleccione **Customize** en la lista desplegable en la esquina superior derecha del área del gráfico. Elija **Agent** y seleccione **Garbage Collection (GC) Duration of Flume**. A continuación, haga clic en **OK**.

Figura 9-71 Duración de Recolección de Basura (GC) de Flume



Paso 3 Compruebe si la duración de GC del proceso de Flume recopilado cada minuto supera el umbral (12 segundos por defecto).

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 6**.

Paso 4 En FusionInsight Manager, seleccione **Cluster** > *Name of the desired cluster* > **Service** > **Flume** > **Configuration**. En la página que se muestra, haga clic en **All Configurations** y elija **Flume** > **System**. Establezca **-Xmx** en el parámetro **GC_OPTS** a un valor mayor según los requisitos del sitio y guarde la configuración.

NOTA

Si se genera esta alarma, la memoria heap configurada para el Flume server es insuficiente para la transmisión de datos. Se recomienda cambiar la memoria heap a: Capacidad del canal x Tamaño máximo de un solo registro de datos x Número de canales. Tenga en cuenta que el valor de **xmx** no puede exceder la memoria restante del nodo.

Paso 5 Reinicie los servicios o instancias afectados y compruebe si la alarma está desactivada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 6**.

Recopilar información de fallas.

Paso 6 En FusionInsight Manager, seleccione **O&M**. En el panel de navegación de la izquierda, elija **Log** > **Download**.

Paso 7 Expanda la lista desplegable **Service** y seleccione **Flume** para el clúster de destino.

Paso 8 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 9 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

Información relacionada

Ninguna

9.184 ALM-25000 Servicio LdapServer no disponible

Descripción

El sistema comprueba el estado del servicio LdapServer cada 30 segundos. Esta alarma se genera cuando el sistema detecta que tanto los servicios de LdapServer activo como en espera son anormales.

Esta alarma se borra cuando el sistema detecta que uno o dos servicios de LdapServer son normales.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
25000	Crítica	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

Cuando se genera esta alarma, no se puede realizar ninguna operación para los usuarios KrbServer y LdapServer en el clúster. Por ejemplo, los usuarios, grupos de usuarios o roles no se pueden agregar, eliminar o modificar, y las contraseñas de usuario no se pueden cambiar en

el portal de FusionInsight Manager. La autenticación de los usuarios existentes en el clúster no se ve afectada.

Causas posibles

- El nodo donde se encuentra el servicio LdapServer es defectuoso.
- El proceso LdapServer es anormal.

Procedimiento

Compruebe si los nodos donde se encuentran las dos instancias SlapdServer del servicio LdapServer están defectuosos.

Paso 1 En FusionInsight Manager, elija **Cluster >** *Name of the desired cluster* **> Services** > **LdapServer** > **Instance** para ir a la página de instancia de LdapServer para obtener el nombre de host del nodo donde se ubican las dos instancias de SlapdServer.

Paso 2 Elija **O&M > Alarm > Alarms**. En la página **Alarm** del sistema de FusionInsight Manager, compruebe si existe alguna alarma de **Falla de nodo**.

- En caso afirmativo, vaya a **Paso 3**.
- Si no, vaya a **Paso 6**.

Paso 3 Compruebe si el nombre de host en la alarma es consistente con el nombre de host de **Paso 1**.

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 6**.

Paso 4 Manejar la alarma según "ALM-12006 Falla de nodo".

Paso 5 Compruebe si **Servicio LdapServer no disponible** está borrado en la lista de alarmas.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 10**.

Compruebe si el proceso de LdapServer es normal.

Paso 6 Elija **O&M > Alarm > Alarms**. En la página **Alarm** del sistema de FusionInsight Manager, compruebe si existe alguna alarma de **Falla de proceso**.

- En caso afirmativo, vaya a **Paso 7**.
- Si no, vaya a **Paso 10**.

Paso 7 Compruebe si el servicio y el nombre de host en la alarma son coherentes con el servicio LdapServer y el nombre de host.

- En caso afirmativo, vaya a **Paso 8**.
- Si no, vaya a **Paso 10**.

Paso 8 Maneje la alarma según "ALM-12007 Falla de proceso".

Paso 9 Compruebe si **Servicio LdapServer no disponible** está borrado en la lista de alarmas.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 10**.

Recopilar información de fallas.

Paso 10 En el FusionInsight Manager, elija **O&M** > **Log > Download**.

Paso 11 Seleccione **LdapServer** en el clúster requerido en el **Service**.

Paso 12 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 13 Póngase en contacto con el y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.185 ALM-25004 Sincronización anormal de datos de LdapServer

Descripción

El sistema comprueba los datos del LdapServer cada 30 segundos. Esta alarma se genera cuando los datos en el LdapServers activo y en espera de Manager son inconsistentes durante 12 veces consecutivas. Esta alarma se borra cuando los datos en el LdapServers activo y en espera son consistentes.

El sistema comprueba los datos del LdapServer cada 30 segundos. Esta alarma se genera cuando los datos LdapServer en el clúster son incompatibles con los de Manager durante 12 veces consecutivas. Esta alarma se borra cuando los datos son consistentes.

Atributo

ID de alarma	Gravedad de la alarma	Borrado automático
25004	Crítica	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.

Nombre	Significado
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

La incoherencia de los datos de LdapServer se produce porque los datos de LdapServer en Manager están dañados o los datos de LdapServer en el clúster están dañados. El proceso LdapServer con datos dañados no puede proporcionar servicios externamente, y las funciones de autenticación de Manager y del clúster se ven afectadas.

Causas posibles

- La red del nodo donde se localiza el proceso LdapServer es defectuosa.
- El proceso LdapServer es anormal.
- El reinicio del sistema operativo daña los datos de LdapServer.

Procedimiento

Compruebe si la red donde residen los nodos LdapServer está defectuosa.

Paso 1 En el portal de FusionInsight Manager, seleccione **O&M > Alarm > Alarms**. Registre la dirección IP de HostName en la información de localización de alarma como IP1 (si existen múltiples alarmas, registre las direcciones IP como IP1, IP2 e IP3 respectivamente).

Paso 2 Contacte e inicie sesión en los nodos correspondientes a IP 1. Ejecute el comando ping para comprobar si la dirección IP del plano de gestión del nodo OMS activo se puede hacer ping.

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 3**.

Paso 3 Póngase en contacto con el administrador de la red para recuperar la red y comprobar si **Sincronización anormal de datos de LdapServer** está borrado.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 4**.

Comprobar si los procesos de LdapServer son normales.

Paso 4 En la página **Alarm** del FusionInsight Manager, compruebe si el **OLdap Resource Abnormal** existe.

- En caso afirmativo, vaya a **Paso 5**.
- Si no, vaya a **Paso 7**.

Paso 5 Borre la alarma siguiendo los pasos proporcionados en "ALM-12004 OLdap Resource Abnormal".

Paso 6 Compruebe si **Abnormal LdapServer Data Synchronization** está borrado en la lista de alarmas.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 7**.

Paso 7 En la página **Alarm** de FusionInsight Manager, compruebe si **Process Faul** se genera para el servicio LdapServer.

- En caso afirmativo, vaya a **Paso 8**.
- Si no, vaya a **Paso 10**.

Paso 8 Maneje la alarma según "ALM-12007 Process Fault".

Paso 9 Compruebe si **Abnormal LdapServer Data Synchronization** está borrado.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 10**.

Comprobar si los procesos de LdapServer son normales.

Paso 10 En FusionInsight Manager, seleccione **O&M** > **Alarm** > **Alarms**. Registre la dirección IP de HostName en la información de localización de alarma como "IP1" (si existen múltiples alarmas, registre las direcciones IP como "IP1", "IP2" e "IP3" respectivamente). Seleccione **Cluster** > *Name of the desired cluster* > **Services** > **LdapServer** > **Configurations**. Registre el número de puerto de LdapServer como "PORT". (Si la dirección IP en la información de localización de alarma es la dirección IP del nodo de gestión en espera, elija **System** > **OMS** > **oldap** > **Modify Configuration** y registre el número de puerto de escucha de LdapServer.)

Paso 11 Inicie sesión en los nodos correspondientes a IP1 como **omm**.

Paso 12 Ejecute el siguiente comando para comprobar si se muestran errores en la información consultada.

ldapsearch -H ldaps://*IP1*:*PORT* **-LLL -x -D cn=root,dc=hadoop,dc=com -W -b ou=Peoples,dc=hadoop,dc=com**

Después de ejecutar el comando, introduzca la contraseña de administrador **LDAP**. Póngase en contacto con el administrador del sistema para obtener la contraseña.

- En caso afirmativo, vaya a **Paso 13**.
- Si no, vaya a **Paso 15**.

Paso 13 Recupere los nodos LdapServer y OMS utilizando los datos respaldados antes de generar la alarma.

NOTA

Utilice los datos de OMS y los datos de LdapServer respaldados en el mismo momento para recuperar los datos. De lo contrario, el servicio y la operación pueden fallar. Para recuperar datos cuando los servicios se ejecutan correctamente, se le aconseja hacer una copia de respaldo manual de los últimos datos de gestión y luego recuperar los datos. De lo contrario, se perderán los datos del Manager generados entre el punto de copia de respaldo y el punto de recuperación.

Paso 14 Compruebe si el **Abnormal LdapServer Data Synchronization** de alarma está borrado.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 15**.

Recopilar información de fallas.

Paso 15 En el portal del FusionInsight Manager, elija **O&M** > **Log > Download**.

Paso 16 Seleccione **LdapServer** en el clúster requerido y **OmsLdapServer** en el **Service**.

Paso 17 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 1 hora antes y después del tiempo de generación de alarma, respectivamente. A continuación, haga clic en **Download**.

Paso 18 Póngase en contacto con el y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.186 ALM-25005 Excepción de servicio nscd

Descripción

El sistema comprueba el estado del servicio nscd cada 60 segundos. Esta alarma se genera cuando el proceso nscd no se consulta durante cuatro veces consecutivas (tres minutos) o los usuarios de LdapServer no se pueden obtener.

Esta alarma se borra cuando se restablece el proceso y se pueden obtener los usuarios de LdapServer.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
25005	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
HostName	Host para el que se genera la alarma.

Impacto en el sistema

El nodo alarmado puede no ser capaz de sincronizar datos de LdapServer. El comando **id** puede no obtener los datos LDAP, lo que afecta a los servicios de capa superior.

Causas posibles

- El servicio nscd no se inicia.
- La red está defectuosa y no puede acceder al servidor LDAP.
- NameService es anormal.
- No se puede consultar a los usuarios porque el sistema operativo ejecuta los comandos con demasiada lentitud.

Procedimiento

Comprobar si se ha iniciado el servicio nscd.

Paso 1 Inicie sesión en FusionInsight Manager y elija **O&M** > **Alarm** > **Alarms**. Registre la dirección IP de **HostName** en **Location** de la alarma como **IP1** (si existen varias alarmas, registre las direcciones IP como **IP1**, **IP2** y **IP3** respectivamente).

Paso 2 Póngase en contacto con el para acceder al nodo usando IP1 como usuario **root**. Ejecute el comando **ps -ef | grep nscd** en el nodo y compruebe si el proceso **/usr/sbin/nscd** está iniciado.

- En caso afirmativo, vaya a **Paso 5**.
- Si no, vaya a **Paso 3**.

Paso 3 Ejecute el comando **service nscd restart** como usuario **root** para reiniciar el servicio nscd. A continuación, ejecute el comando **ps -ef | grep nscd** para comprobar si se ha iniciado el servicio nscd.

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 15**.

Paso 4 Espere 5 minutos y vuelva a ejecutar el comando ps -ef | grep nscd como usuario root. Compruebe si el servicio existe.

- En caso afirmativo, vaya a **Paso 11**.
- Si no, vaya a **Paso 15**.

Comprobar si la red está defectuosa y si se puede acceder al servidor LDAP.

Paso 5 Inicie sesión en el nodo con alarma como usuario **root** y ejecute el comando **ping** para comprobar si la conectividad de red entre este nodo y el nodo LdapServer es normal.

- En caso afirmativo, vaya a **Paso 6**.
- Si no, póngase en contacto con los administradores de red para solucionar el problema.

Comprobar si el NameService es normal.

Paso 6 Inicie sesión en el nodo con alarma como usuario **root**. Ejecute el comando **cat /etc/nsswitch.conf** para comprobar si el **passwd**, **group**, **services**, **netgroup** y el **aliases** de NameService están configurados correctamente.

Las configuraciones de parámetros correctas son las siguientes:

passwd: **compat ldap**; **group**: **compat ldap**; **services**: **files ldap**; **netgroup**: **files ldap**; **aliases**: **files ldap**

- En caso afirmativo, vaya a **Paso 7**.
- Si no, vaya a **Paso 9**.

Paso 7 Inicie sesión en el nodo con alarma como usuario **root**. Ejecute el comando **cat /etc/nscd.conf** para comprobar si **enable-cache passwd**, **positive-time-to-live passwd**, **enable-cache group** y **positive-time-to-live group** en el archivo de configuración están configurados correctamente.

Las configuraciones de parámetros correctas son las siguientes:

enable-cache passwd: **yes**; **positive-time-to-live passwd**: **600**; **enable-cache group**: **yes**; **positive-time-to-live group**: **3600**

- En caso afirmativo, vaya a **Paso 8**.
- Si no, vaya a **Paso 10**.

Paso 8 Ejecute los comandos **/usr/sbin/nscd -i group** y **/usr/sbin/nscd -i passwd** como usuario **root**. Espere 2 minutos y ejecute los comandos **id admin** y **id backup/manager** para comprobar si se pueden consultar los resultados.

- En caso afirmativo, vaya a **Paso 11**.
- Si no, vaya a **Paso 15**.

Paso 9 Ejecute el comando **vi /etc/nsswitch.conf** como usuario **root**. Corrija las configuraciones de **Paso 6** y guarde el archivo. Ejecute el comando **service nscd restart** para reiniciar el servicio nscd. Espere 2 minutos y ejecute los comandos **id admin** y **id backup/manager** para comprobar si se pueden consultar los resultados.

- En caso afirmativo, vaya a **Paso 11**.
- Si no, vaya a **Paso 15**.

Paso 10 Ejecute el comando **vi /etc/nscd.conf** como usuario **root**. Corrija las configuraciones de **Paso 7** y guarde el archivo. Ejecute el comando **service nscd restart** para reiniciar el servicio nscd. Espere 2 minutos y ejecute los comandos **id admin** y **id backup/manager** para comprobar si se pueden consultar los resultados.

- En caso afirmativo, vaya a **Paso 11**.
- Si no, vaya a **Paso 15**.

Paso 11 Inicie sesión en el portal del FusionInsight Manager. Espere 5 minutos y compruebe si la alarma **nscd Service Exception** está desactivada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 12**.

Verificar si se congela el marco cuando se ejecuta un comando en el sistema operativo..

Paso 12 Inicie sesión en el nodo defectuoso como usuario **root**, ejecute el comando **id admin** y compruebe si la ejecución del comando tarda mucho tiempo. Si la ejecución del comando tarda más de 3 segundos, se considera que la ejecución del comando es lenta.

- En caso afirmativo, vaya a **Paso 13**.
- Si no, vaya a **Paso 15**.

Paso 13 Ejecute el comando **cat /var/log/messages** para comprobar si el nscd se reinicia con frecuencia o si existe la información de error "Can't contact LDAP server".

Ejemplo de excepción nscd:

```
Feb 11 11:44:42 10-120-205-33 nscd: nss_ldap: failed to bind to LDAP server
ldaps://10.120.205.55:21780: Can't contact LDAP server
Feb 11 11:44:43 10-120-205-33 ntpq: nss_ldap: failed to bind to LDAP server
ldaps://10.120.205.55:21780: Can't contact LDAP server
```



```
Feb 11 11:44:44 10-120-205-33 ntpq: nss_ldap: failed to bind to LDAP server
ldaps://10.120.205.92:21780: Can't contact LDAP server
```

- En caso afirmativo, vaya a **Paso 14**.
- Si no, vaya a **Paso 15**.

Paso 14 Ejecute el comando **vi$BIGDATA_HOME/tmp/random_ldap_ip_order** para modificar el número al final. Si el número original es un número impar, cámbielo a un número par. Si el número es un número par, cámbielo a un número impar.

Ejecute el comando **vi /etc/ldap.conf** para entrar en el modo de edición, presione **Insert** para comenzar a editar y, a continuación, cambie las dos primeras direcciones IP del elemento de configuración de URI.

Una vez completada la modificación, pulse **Esc** para salir del modo de edición y entrar en **:wq!** para guardar la configuración y salir.

Ejecute el comando **service nscd restart** para reiniciar el servicio nscd. Espere 5 minutos y vuelva a ejecutar el comando **id admin**. Compruebe si la ejecución del comando es lenta.

- En caso afirmativo, vaya a **Paso 15**.
- Si no, inicie sesión en otros nodos defectuosos y repita **Paso 12** en **Paso 14** para comprobar si el primer nodo LdapServer en el URI antes de modificar **/etc/ldap.conf** es defectuoso. Por ejemplo, compruebe si la dirección IP del servicio es inalcanzable, si el retraso de la red es demasiado largo o si se despliega otro software anormal.

Recopilar información de fallas.

Paso 15 En FusionInsight Manager, seleccione **O&M**. En el panel de navegación de la izquierda, elija **Log** > **Download**.

Paso 16 Expanda la lista desplegable junto al campo **Service**. En el cuadro de diálogo **Services** que se muestra, seleccione **LdapClient** para el clúster de destino.

Paso 17 Haga clic en  en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 1 hora antes y después del tiempo de generación de alarma, respectivamente. A continuación, haga clic en **Download**.

Paso 18 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

Información relacionada

Ninguna

9.187 ALM-25006 Excepción de servicio Sssd

Descripción

El sistema comprueba el estado del servicio sssd cada 60 segundos. Esta alarma se genera cuando el proceso sssd no se consulta durante cuatro veces consecutivas (tres minutos) o no se pueden obtener usuarios de LdapServer.

Esta alarma se borra cuando se restablece el proceso y se pueden obtener los usuarios de LdapServer.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
25006	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el nombre del servicio para el que se genera la alarma.
HostName	Especifica el objeto (ID de host) para el que se genera la alarma.

Impacto en el sistema

El nodo alarmado puede no ser capaz de sincronizar datos de LdapServer. El comando id puede fallar al obtener los datos LDAP, lo que afecta los servicios de la capa superior.

Causas posibles

- El servicio sssd no se inicia o se inicia incorrectamente.
- La red está defectuosa y no puede acceder al servidor LDAP.
- NameService es anormal.
- No se puede consultar a los usuarios porque el sistema operativo ejecuta los comandos con demasiada lentitud.

Procedimiento

Comprobar si el servicio sssd se ha iniciado correctamente.

Paso 1 En el portal de FusionInsight Manager, seleccione **O&M > Alarm > Alarms**. Encontrar la dirección IP de **HostName** en **Location** de la alarma y registrarla como IP1 (si existen múltiples alarmas, registre las direcciones IP como IP1, IP2 e IP3 respectivamente).

Paso 2 Póngase en contacto con el para acceder al nodo usando IP1 como usuario root. Ejecute el comando **ps -ef | grep sssd** y compruebe si el proceso **/usr/sbin/sssd** está iniciado.

- Si se inicia el proceso, vaya a **Paso 3**.
- Si el proceso no se ha iniciado, vaya a **Paso 4**.

Paso 3 Compruebe si el proceso sssd consultado en **Paso 2** tiene tres subprocesos.

- En caso afirmativo, vaya a **Paso 5**.
- Si no, vaya a **Paso 4**.

Paso 4 Ejecute el comando **service sssd restart** como usuario **root** para reiniciar el servicio sssd. A continuación, ejecute el comando **ps -ef | grep sssd** para comprobar si el proceso sssd es normal.

En el estado normal, el proceso **/usr/sbin/sssd** tiene tres subprocesos: **/usr/libexec/sssd/sssd_be**, **/usr/libexec/sssd/sssd_nss** y **/usr/libexec/sssd/sssd_pam**.

- Si existe, vaya a **Paso 9**.
- Si no existe, vaya a **Paso 13**.

Comprobar si se puede acceder al servidor LDAP.

Paso 5 Inicie sesión en el nodo con alarma como usuario **root**. Ejecute el comando **ping** para comprobar la conectividad de red entre este nodo y el nodo LdapServer.

- Si la red es normal, vaya a **Paso 6**.
- Si la red está defectuosa, póngase en contacto con los administradores de la red para solucionar el problema.

Comprobar si NameService es normal.

Paso 6 Inicie sesión en el nodo con alarma como usuario **root**. Ejecute el comando **cat /etc/nsswitch.conf** y compruebe las configuraciones **passwd** y **group** de NameService.

Las configuraciones de parámetros correctas son **passwd: compat ldap** y **group: compat ldap**.

- Si las configuraciones son correctas, vaya a **Paso 7**.
- Si las configuraciones son incorrectas, vaya a **Paso 8**.

Paso 7 Ejecute los comandos **/usr/sbin/sss_cache -G** y **/usr/sbin/sss_cache -U** como usuario **root**. Espere 2 minutos y ejecute los comandos **id admin** y **id backup/manager** para comprobar si se pueden consultar los resultados.

- Si se consultan los resultados, vaya a **Paso 9**.
- Si no se consulta ningún resultado, vaya a **Paso 13**.

Paso 8 Ejecute el comando **vi /etc/nsswitch.conf** como usuario **root**. Corrija las configuraciones en **Paso 6** y guarde el archivo. Ejecute el comando **service sssd restart** para reiniciar el servicio sssd. Espere 2 minutos y ejecute los comandos **id admin** y **id backup/manager** para comprobar si se pueden consultar los resultados.

- Si se consultan los resultados, vaya a **Paso 9**.

- Si no se consulta ningún resultado, vaya a **Paso 13**.

Paso 9 Inicie sesión en el portal del FusionInsight Manager. Espere 5 minutos y compruebe si la alarma **sssd Service Exception** está desactivada.

- Si la alarma se ha borrado, no se requiere ninguna acción adicional.
- Si la alarma persiste, vaya a **Paso 10**.

Verifique si se congela el marco cuando se ejecuta un comando en el sistema operativo.

Paso 10 Inicie sesión en el nodo defectuoso como usuario **root**, ejecute el comando **id admin** y compruebe si la ejecución del comando tarda mucho tiempo. Si la ejecución del comando tarda más de 3 segundos, se considera que la ejecución del comando es lenta.

- En caso afirmativo, vaya a **Paso 11**.
- Si no, vaya a **Paso 13**.

Paso 11 Ejecute el comando **cat /var/log/messages** para comprobar si el sssd se reinicia con frecuencia o si existe la información de error **Can't contact LDAP server**.

Ejemplo de reinicio de sssd:

```
Feb  7 11:38:16 10-132-190-105 sssd[pam]: Shutting down
Feb  7 11:38:16 10-132-190-105 sssd[nss]: Shutting down
Feb  7 11:38:16 10-132-190-105 sssd[nss]: Shutting down
Feb  7 11:38:16 10-132-190-105 sssd[be[default]]: Shutting down
Feb  7 11:38:16 10-132-190-105 sssd: Starting up
Feb  7 11:38:16 10-132-190-105 sssd[be[default]]: Starting up
Feb  7 11:38:16 10-132-190-105 sssd[nss]: Starting up
Feb  7 11:38:16 10-132-190-105 sssd[pam]: Starting up
```

- En caso afirmativo, vaya a **Paso 12**.
- Si no, vaya a **Paso 13**.

Paso 12 Ejecute el comando **vi $BIGDATA_HOME/tmp/random_ldap_ip_order** para modificar el número al final. Si el número original es un número impar, cámbielo a un número par. Si el número es un número par, cámbielo a un número impar.

Ejecute el comando **vi /etc/sssd/sssd.conf** para invertir las dos primeras direcciones IP del elemento de configuración del **ldap_uri**, guarde la configuración y salga.

Ejecute el comando **ps -ef | grep sssd** para consultar el ID del proceso sssd, elimínelo y ejecute el comando **/usr/sbin/sssd -D -f** para reiniciar el servicio sssd. Espere 5 minutos y vuelva a ejecutar el comando **id admin**.

Compruebe si la ejecución del comando es lenta.

- En caso afirmativo, vaya a **Paso 13**.
- Si no, inicie sesión en otros nodos defectuosos y ejecute **Paso 10** en **Paso 12**. Recopile registros y compruebe si el primer nodo ldapserver en ldap_uri antes de modificar **/etc/sssd/sssd.conf** es defectuoso. Por ejemplo, compruebe si la dirección IP del servicio es inalcanzable, la latencia de la red es demasiado larga o si se implementa otro software anormal.

Recopilar información de fallas.

Paso 13 En el portal del FusionInsight Manager, elija **O&M** > **Log > Download**.

Paso 14 Seleccione **LdapClient** en el clúster requerido en el **Service**.

Paso 15 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 1 hora antes y después del tiempo de generación de alarma, respectivamente. A continuación, haga clic en **Download**.

Paso 16 Póngase en contacto con el y envíe los registros de fallas recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.188 ALM-25500 Servicio KrbServer no disponible

Descripción

El sistema comprueba el estado del servicio KrbServer cada 30 segundos. Esta alarma se genera cuando el sistema detecta que el servicio KrbServer es anormal.

Esta alarma se borra cuando el sistema detecta que el servicio KrbServer es normal.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
25500	Crítica	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

Cuando se genera esta alarma, no se puede realizar ninguna operación para el componente KrbServer en el clúster. La autenticación de KrbServer en otros componentes se verá afectada. El estado de ejecución de los componentes que dependen de KrbServer en el clúster es Bad.

Causas posibles

- El nodo donde se encuentra el servicio KrbServer es defectuoso.
- El servicio OLdap es anormal.

Procedimiento

Compruebe si el nodo donde se ubica el servicio KrbServer está defectuoso.

Paso 1 En la página principal de FusionInsight Manager, elija **Cluster** > *Name of the desired cluster* > **Services** > **KrbServer** > **Instance** para ir a la página de instancia de KrbServer para obtener el nombre de host del nodo donde el servicio KrbServer localiza.

Paso 2 En la página **Alarm** del sistema de FusionInsight Manager, compruebe si existe alguna alarma de **Falla de nodo**.

- En caso afirmativo, vaya a **Paso 3**.
- Si no, vaya a **Paso 6**.

Paso 3 Compruebe si el nombre de host en la alarma es consistente con el nombre de host de **Paso 1**.

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 6**.

Paso 4 Manejar la alarma según "ALM-12006 Falla de nodo".

Paso 5 Compruebe si **Servicio KrbServer no disponible** está borrado en la lista de alarmas.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 6**.

Comprobar si el servicio OLdap es normal.

Paso 6 En la página **Alarm** del sistema de FusionInsight Manager, compruebe si existe alguna alarma de **Recurso de OLdap anormal**.

- En caso afirmativo, vaya a **Paso 7**.
- Si no, vaya a **Paso 9**.

Paso 7 Maneje la alarma según "ALM-12004 Recurso de OLdap Resource Anormal".

Paso 8 Compruebe si **Servicio KrbServer no disponible** está borrado en la lista de alarmas.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 9**.

Recopilar información de fallas.

Paso 9 En el FusionInsight Manager, elija **O&M** > **Log > Download**.

Paso 10 Seleccione **KrbServer** en el clúster requerido en el **Service**.

Paso 11 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 12 Póngase en contacto con el y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.189 ALM-26051 Servicio de Storm no disponible

Descripción

El sistema comprueba el estado del servicio de Storm cada 30 segundos. Esta alarma se genera cuando todos los nodos Nimbus del clúster son anormales y el servicio Storm no está disponible.

Esta alarma se borra cuando el servicio Storm se recupera.

Atributo

ID de alarma	Gravedad de la alarma	Borrado automáticamente
26051	Crítica	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

El clúster no puede proporcionar el servicio Storm y los usuarios no pueden realizar nuevas tareas de Storm.

Causas posibles

- El clúster de Kerberos es defectuoso.
- El clúster ZooKeeper es defectuoso o está suspendido.
- Los nodos Nimbus activos y en espera en el clúster Storm son anormales

Procedimiento

Comprobar el estado del clúster de Kerberos. (Omita este paso si se usa el modo normal).

Paso 1 En el portal del administrador de FusionInsight, elija **Cluster** > *Name of the desired cluster* > **Services**.

Paso 2 Compruebe si el estado de ejecución del servicio Kerberos es de **Normal**.

- En caso afirmativo, vaya a **Paso 5**.
- Si no, vaya a **Paso 3**.

Paso 3 Consulte la información de mantenimiento relacionada de **ALM-25500 Servicio KrbServer no disponible**.

Paso 4 Verifique si la alarma se ha borrado.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 5**.

Verificar el estado del clúster de ZooKeeper.

Paso 5 Compruebe si el estado de ejecución del servicio ZooKeeper es de tipo **Normal**.

- En caso afirmativo, vaya a **Paso 8**.
- Si no, vaya a **Paso 6**.

Paso 6 Si se detiene el servicio ZooKeeper, inícielo, de lo contrario vea la información de mantenimiento relacionada de **ALM-13000 Servicio ZooKeeper no disponible**.

Paso 7 Verifique si la alarma se ha borrado.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 8**.

Comprobar el estado de los nodos Nimbus activos y en espera.

Paso 8 Seleccione **Cluster** > *Name of the desired cluster* > **Services** > **Storm** > **Nimbus** para ir a la página Instancias de Nimbus.

Paso 9 Comprueba si solo un nodo Nimbus está en estado **Active** en **Roles**.

- En caso afirmativo, vaya a **Paso 13**.
- Si no, vaya a **Paso 10**.

Paso 10 Seleccione dos instancias de rol Nimbus, elija **More** > **Restart Instance** y compruebe si las instancias se reinician correctamente.

- En caso afirmativo, vaya a **Paso 11**.
- Si no, vaya a **Paso 13**.

Paso 11 Inicie sesión de nuevo en el portal del administrador de FusionInsight y seleccione **Cluster** > *Name of the desired cluster* > **Services** > **Storm** > **Nimbus** para comprobar si el estado de ejecución es **Normal**.

- En caso afirmativo, vaya a **Paso 12**.
- Si no, vaya a **Paso 13**.

Paso 12 Espere 30 segundos y compruebe si la alarma está desactivada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 13**.

Recopilación de información de error

Paso 13 En el FusionInsight Manager, elija **O&M** > **Log** > **Download**.

Paso 14 Seleccione los siguientes nodos en el clúster requerido en la lista desplegable **Service**:

- KrbServer

  NOTA

  Los registros de KrbServer no necesitan descargarse en modo normal.
- ZooKeeper
- Storm

Paso 15 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 16 Póngase en contacto con el y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.190 ALM-26052 El número de Supervisor disponible del servicio de Storm es menor que el umbral

Descripción

El sistema comprueba periódicamente el número de Supervisor disponibles cada 60 segundos y compara el número de Supervisor disponible con el umbral. Esta alarma se genera cuando el número de Supervisor disponible es menor que el umbral.

Puede cambiar el umbral en **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster*.

Esta alarma se borra cuando el número de Supervisor disponible es mayor o igual que el umbral.

Atributo

ID de alarma	Gravedad de la alarma	Borrado automáticamente
26052	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger condition	Especifica el umbral que activa la alarma. Si el valor del indicador actual excede este umbral, se genera la alarma.

Impacto en el sistema

No se pueden realizar tareas existentes en el clúster. El clúster puede recibir nuevas tareas de Storm, pero no puede realizar estas tareas.

Causas posibles

El estado de algunos Supervisores en el clúster es anormal.

Procedimiento

Comprobar el estado del supervisor.

Paso 1 Seleccione **Cluster** > *Name of the desired cluster* > **Services** > **Storm** > **Supervisor** para ir a la página de gestión de servicio de Storm.

Paso 2 En **Roles**, compruebe si existe cualquier instancia cuyo estado sea **Faulty** o **Restoring**.

- En caso afirmativo, vaya a **Paso 3**.
- Si no, vaya a **Paso 5**.

Paso 3 Seleccione las instancias de rol de supervisor cuyo estado es **Faulty** o **Restoring**, elija **More** > **Restart Instance**, y compruebe si las instancias se reinician correctamente.

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 5**.

Paso 4 Espere 30 segundos y compruebe si la alarma está desactivada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 5**.

NOTA

Los servicios se interrumpen cuando se está reiniciando el Supervisor. A continuación, los servicios se restauran después del reinicio.

Recopilar información de fallas.

Paso 5 En el portal del FusionInsight Manager, seleccione **O&M** > **Log** > **Download**.

Paso 6 Seleccione **Storm** y **ZooKeeper** en el clúster requerido en el cuadro de lista desplegable **Service**.

Paso 7 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 1 hora antes y después del tiempo de generación de alarma, respectivamente. A continuación, haga clic en **Download**.

Paso 8 Póngase en contacto con el y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.191 ALM-26053 El uso de Storm Slot supera el umbral

Descripción

El sistema comprueba el uso de la ranura cada 60 segundos y compara el uso real de la ranura con el umbral. Esta alarma se genera cuando el uso de ranura es mayor que el umbral.

Puede cambiar el umbral en **O&M** > **Alarm** > **Thresholds**.

Esta alarma se borra cuando el uso de ranura es menor o igual que el umbral.

Atributo

ID de alarma	Gravedad de la alarma	Borrado automáticamente
26053	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger condition	Especifica el umbral que activa la alarma. Si el valor del indicador actual excede este umbral, se genera la alarma.

Impacto en el sistema

No se pueden realizar nuevas tareas de Storm.

Causas posibles

- El estado de algunos Supervisores en el clúster es anormal.
- El estado de todos los Supervisores es normal, pero la capacidad de procesamiento es insuficiente.

Procedimiento

Comprobar el estado del supervisor.

Paso 1 Seleccione **Cluster** > *Name of the desired cluster* > **Services** > **Storm** > **Instance** para ir a la página de gestión de instancias de Storm.

Paso 2 Compruebe si existe alguna instancia cuyo estado sea **Faulty** o **Restoring**.

- En caso afirmativo, vaya a **Paso 3**.
- Si no, vaya a **Paso 5**.

Paso 3 Seleccione las instancias de rol de supervisor cuyo estado es **Faulty** o **Restoring**, elija **More** > **Restart Instance**, y compruebe si las instancias se reinician correctamente.

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 10**.

Paso 4 Espere varios minutos y compruebe si la alarma está desactivada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 5**.

Aumentar el número de espacios en cada Supervisor.

Paso 5 Inicie sesión en el portal del FusionInsight Manager, elija **Cluster** > *Name of the desired cluster* > **Services** > **Storm** > **Configurations** > **All Configurations**.

Paso 6 Aumente el número de puertos en el parámetro **supervisor.slots.ports** de cada rol Supervisor y reinicie la instancia.

Paso 7 Espere varios minutos y compruebe si la alarma está desactivada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 8**.

Paso 8 Realice la ampliación de la capacidad para Supervisor.

Paso 9 Espere varios minutos y compruebe si la alarma está desactivada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 10**.

  NOTA

  Los servicios se interrumpen cuando se está reiniciando el Supervisor. A continuación, los servicios se restauran después del reinicio.

Recopilar información de fallas.

Paso 10 En el portal del FusionInsight Manager, seleccione **O&M** > **Log** > **Download**.

Paso 11 Seleccione **Storm** y **ZooKeeper** en el clúster requerido en el cuadro de lista desplegable **Service**.

Paso 12 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 1 hora antes y después del tiempo de generación de alarma, respectivamente. A continuación, haga clic en **Download**.

Paso 13 Póngase en contacto con el y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.192 ALM-26054 El uso de memoria heap de Nimbus supera el umbral

Descripción

El sistema comprueba el uso de memoria heap de Storm Nimbus cada 30 segundos y compara el uso real con el umbral. La alarma se genera cuando el uso de memoria heap de Storm Nimbus excede el umbral (80% de la memoria máxima por defecto) durante 5 veces consecutivas.

Los usuarios pueden elegir **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster* > **Storm** > **Nimbus** para cambiar el umbral.

La alarma se borra cuando el uso de memoria heap es menor o igual que el umbral.

Atributo

ID de alarma	Gravedad de la alarma	Borrado automáticamente
26054	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el nombre del servicio para el que se genera la alarma.
RoleName	Especifica el nombre del rol para el que se genera la alarma.
HostName	Especifica el objeto (ID de host) para el que se genera la alarma.
Trigger Condition	Especifica el umbral que activa la alarma. Si el valor del indicador actual excede este umbral, se genera la alarma.

Impacto en el sistema

Cuando el uso de memoria heap de Storm Nimbus es demasiado alto, se producen GC frecuentes. Además, puede producirse un desbordamiento de memoria para que el servicio Yarn no esté disponible.

Causas posibles

La memoria heap de la instancia de Storm Nimbus en el nodo está sobreutilizada o la memoria heap se asigna de forma inapropiada. Como resultado, el uso excede el umbral.

Procedimiento

Comprobar el uso de la memoria heap.

Paso 1 En el portal del FusionInsight Manager, elija **O&M** > **Alarm** > **Alarms** > **Heap Memory Usage of Storm Nimbus Exceeds the Threshold** > **Location**. Compruebe el nombre de host de la instancia para la que se genera la alarma.

Paso 2 En el portal del FusionInsight Manager, elija **Cluster** > *Name of the desired cluster* > **Services** > **Storm** > **Instance**. Haga clic en la instancia para la que se genera la alarma para ir a la página de la instancia. Haga clic en el menú desplegable en el área del gráfico y elija **Customize** > **Nimbus** > **Heap Memory Usage of Nimbus**. Haga clic en **OK**.

Paso 3 Comprobar si la memoria heap usada de Nimbus alcanza el umbral (El valor predeterminado es el 80% de la memoria heap máxima) especificado para Nimbus.

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 6**.

Paso 4 En el portal del FusionInsight Manager, seleccione **Cluster** > *Name of the desired cluster* > **Services** > **Storm** > **Configurations** > **All Configurations** > **Nimbus** > **System**. Cambie el valor de **-Xmx** en **NIMBUS_GC_OPTS** según los requisitos del sitio y haga clic en **Save**. Haga clic en **OK**.

NOTA

- Se recomienda establecer **-Xms** y **-Xmx** en el mismo valor para evitar un impacto adverso en el rendimiento cuando JVM ajusta dinámicamente el tamaño de la memoria heap.
- El número de trabajadores crece a medida que aumenta la escala del clúster Storm. Puede aumentar el valor de **GC_OPTS** para Nimbus. El valor recomendado es el siguiente: Si el número de trabajadores es 20, establezca **-Xmx** en un valor mayor o igual a 1 GB. Si el número de trabajadores es superior a 100, establezca **-Xmx** en un valor mayor o igual a 5 GB.

Paso 5 Reinicie los servicios o instancias afectados y compruebe si la alarma está desactivada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 6**.

Recopilar información de fallas.

Paso 6 En el portal del FusionInsight Manager, seleccione **O&M** > **Log** > **Download**.

Paso 7 Seleccione el siguiente nodo en el clúster requerido en la lista desplegable **Service**.

- NodeAgent
- Storm

Paso 8 Haga clic en  en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 9 Póngase en contacto con el y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.193 ALM-27001 DBService no disponible

Descripción

El módulo de alarma comprueba el estado del servicio de DBService cada 30 segundos. Esta alarma se genera cuando el sistema detecta que el servicio DBService no está disponible.

Esta alarma se borra cuando se recupera el servicio DBService.

Atributo

ID de alarma	Gravedad de la alarma	Borrado automáticamente
27001	Crítica	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

El servicio de base de datos no está disponible y no puede proporcionar funciones de importación y consulta de datos para los servicios de capa superior, lo que da como resultado algunas excepciones de servicios.

Causas posibles

- La dirección IP flotante no existe.
- No hay una instancia de DBServer activa.
- Los procesos DBServer activo y en espera son anormales.

Procedimiento

Comprobar si la dirección IP flotante existe en el entorno del clúster.

Paso 1 En la página principal del FusionInsight Manager, elija **Cluster** > *Name of the desired cluster* > **Services** > **DBService** > **Instance**.

Paso 2 Compruebe si existe la instancia activa.

- En caso afirmativo, vaya a **Paso 3**.
- Si no, vaya a **Paso 9**.

Paso 3 Seleccione la instancia de DBServer activa y registre la dirección IP.

Paso 4 Inicie sesión en el host que corresponde a la dirección IP anterior como usuario **root** y ejecute el comando **ifconfig** para comprobar si existe la dirección IP flotante de DBService en el nodo.

- En caso afirmativo, vaya a **Paso 5**.
- Si no, vaya a **Paso 9**.

Paso 5 Ejecute el comando **ping** *floatip* para comprobar si la dirección IP flotante DBService se puede hacer ping correctamente.

- En caso afirmativo, vaya a **Paso 6**.
- Si no, vaya a **Paso 9**.

Paso 6 Inicie sesión en el host que corresponde a la dirección IP flotante de DBService como usuario **root** y ejecute el comando para eliminar la dirección IP flotante.

ifconfig *interface* **down**

Paso 7 En la página principal del FusionInsight Manager, elija **Cluster >** *Name of the desired cluster* > **Services** > **DBService** > **More** > **Restart Service** para reiniciar DBService y compruebe si DBService se reinicia correctamente.

- En caso afirmativo, vaya a **Paso 8**.
- Si no, vaya a **Paso 9**.

Paso 8 Espere unos 2 minutos y compruebe si la alarma está borrada en la lista de alarmas.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 14**.

Comprobar el estado de la instancia activa de DBServer.

Paso 9 Seleccione la instancia de DBServer cuyo estado de rol es anormal y registre la dirección IP.

Paso 10 En la página **Alarm** , compruebe si se produce **Process Fault** en la instancia DBServer en el host que corresponde a la dirección IP.

- En caso afirmativo, vaya a **Paso 11**.
- Si no, vaya a **Paso 14**.

Paso 11 Maneje la alarma según "ALM-12007 Falla de proceso".

Paso 12 Espere unos 5 minutos y compruebe si la alarma está borrada en la lista de alarmas.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 19**.

Comprobar el estado de los DBServers activos y en espera.

Paso 13 Inicie sesión en el host que corresponde a la dirección IP anterior como usuario **root** y ejecute el comando **su - omm** para cambiar a usuario **omm**.

Paso 14 Ejecute el comando **cd ${DBSERVER_HOME}** para ir al directorio de instalación del DBService.

Paso 15 Ejecute el comando **sh sbin/status-dbserver.sh** para ver el estado de los procesos de HA activos y en espera de DBService. Determine si el estado se puede ver correctamente.

```
HAMode
double

NodeName                 HostName             HAVersion
StartTime                HAActive             HAAllResOK
HARunPhase
10_5_89_12               host01               V100R001C01
2019-06-13 21:33:09      active               normal
Actived
10_5_89_66               host03               V100R001C01
2019-06-13 21:33:09      standby              normal
Deactived

NodeName                 ResName              ResStatus
ResHAStatus              ResType
10_5_89_12               floatip              Normal
Normal                   Single_active
10_5_89_12               gaussDB              Active_normal
Normal                   Active_standby
10_5_89_66               floatip              Stopped
Normal                   Single_active
10_5_89_66               gaussDB              Standby_normal
Normal                   Active_standby
```

- En caso afirmativo, vaya a **Paso 16**.
- Si no, vaya a **Paso 19**.

Paso 16 Compruebe si los procesos HA activo y en espera están en estado anormal.

- En caso afirmativo, vaya a **Paso 17**.
- Si no, vaya a **Paso 19**.

Paso 17 En FusionInsight Manager, elija **Cluster >** *Name of the desired cluster* > **Services** > **DBService** > **More** > **Restart Service** para reiniciar DBService y compruebe si el sistema muestra un mensaje que indica que el reinicio se ha realizado correctamente.

- En caso afirmativo, vaya a **Paso 18**.
- Si no, vaya a **Paso 19**.

Paso 18 Espere unos 2 minutos y compruebe si la alarma está borrada en la lista de alarmas.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 19**.

Recopilar información de fallas.

Paso 19 En FusionInsight Manager, elija **O&M** >**Log > Download**.

Paso 20 Seleccione **DBService** en el clúster requerido y **NodeAgent** en el **Service**.

Paso 21 Haga clic en  en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 1 hora antes y después del tiempo de generación de alarma, respectivamente. A continuación, haga clic en **Download**.

Paso 22 Póngase en contacto con el y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.194 ALM-27003 La interrupción del latido del corazón entre los nodos activo y en espera de DBService

Descripción

Esta alarma se genera cuando el nodo de DBService activo o en espera no recibe mensajes de latidos del nodo par durante 7 segundos.

Esta alarma se borra cuando se recupera el latido del corazón.

Atributo

ID de alarma	Gravedad de la alarma	Borrado automáticamente
27003	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Local DBService HA Name	Especifica un HA de DBService local.
Peer DBService HA Name	Especifica un HA de DBService del mismo nivel.

Impacto en el sistema

Durante la interrupción del latido de DBService, solo un nodo puede proporcionar el servicio. Si este nodo es defectuoso, no hay ningún nodo en espera disponible para la conmutación por error y el servicio no está disponible.

Causas posibles

El vínculo entre los nodos DBService activo y en espera es anormal.

Procedimiento

Comprobar si la red entre el servidor DBService activo y el servidor DBService en espera es normal.

Paso 1 En la lista de alarmas del Administrador de FusionInsight, haga clic en ⌄ en la fila donde se encuentra la alarma en la lista de alarmas en tiempo real y vea la dirección del servidor DBService en espera.

Paso 2 Inicie sesión en el servidor DBService activo como usuario **root**.

Paso 3 Ejecute el comando **ping** *standby DBService heartbeat IP address* para comprobar si el servidor DBService en espera es accesible.

- En caso afirmativo, vaya a **Paso 6**.
- Si no, vaya a **Paso 4**.

Paso 4 Póngase en contacto con el administrador de la red para comprobar si la red es defectuosa.

- En caso afirmativo, vaya a **Paso 5**.
- Si no, vaya a **Paso 6**.

Paso 5 Rectifique la falla de la red y compruebe si la alarma está borrada de la lista de alarmas.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 6**.

Recopilar información de fallas.

Paso 6 En el portal del FusionInsight Manager, elija **O&M** > **Log > Download**.

Paso 7 Seleccione los siguientes nodos en el clúster requerido desde el **Service**:

- DBService
- Controller
- NodeAgent

Paso 8 Haga clic en ✎ en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 9 Póngase en contacto con el y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.195 ALM-27004 Incoherencia de datos entre DBServices activos y en espera

Descripción

El sistema comprueba el estado de sincronización de datos entre el DBService activo y en espera cada 10 segundos. Esta alarma se genera cuando el estado de sincronización no se puede consultar durante seis veces consecutivas o cuando el estado de sincronización es anormal.

Esta alarma se borra cuando el estado de sincronización se vuelve normal.

Atributo

ID de alarma	Gravedad de la alarma	Borrado automáticamente
27004	Crítica	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Local DBService HA Name	Especifica el nombre HA del DBService local.
Peer DBService HA Name	Especifica el nombre HA del DBService del mismo nivel.
SYNC_PERCENT	Especifica el porcentaje de sincronización.

Impacto en el sistema

Cuando los datos no están sincronizados entre los DBServices activo y en espera, los datos pueden perderse o ser anormales si la instancia activa se vuelve anormal.

Causas posibles

- La red entre los nodos activo y en espera es inestable.
- El DBService en espera es anormal.
- El espacio en disco del nodo en espera está lleno.
- El uso de CPU del proceso de GaussDB en el nodo DBService activo es alto. Es necesario localizar la causa del error en función de los registros.

Procedimiento

Comprobar si la red entre los nodos activos y en espera es normal.

Paso 1 En FusionInsight Manager, seleccione **Cluster > Services > DBService > Instance** y compruebe la dirección IP del servicio de la instancia de DBServer en espera.

Paso 2 Inicie sesión en el nodo DBService activo como usuario **root**.

Paso 3 Ejecute el comando **ping** *Standby DBService heartbeat IP address* para comprobar si el nodo DBService en espera es accesible.

- En caso afirmativo, vaya a **Paso 6**.
- Si no, vaya a **Paso 4**.

Paso 4 Póngase en contacto con el administrador de la red para comprobar si la red es defectuosa.

- En caso afirmativo, vaya a **Paso 5**.
- Si no, vaya a **Paso 6**.

Paso 5 Rectifique la falla de la red y compruebe si la alarma está borrada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 6**.

Comprobar si el DBService en espera es normal.

Paso 6 Inicie sesión en el nodo DBService en espera como usuario **root**.

Paso 7 Ejecute el comando **su - omm** para cambiar a usuario **omm**.

Paso 8 Vaya al directorio **${DBSERVER_HOME}/sbin** y ejecute el comando **./status-dbserver.sh** para comprobar si el estado del recurso de GaussDB del DBService en espera es normal. En la salida del comando, compruebe si se muestra la siguiente información en la fila donde **ResName** es **gaussDB**:

Por ejemplo:

```
10_10_10_231 gaussDB Standby_normal Normal Active_standby
```

- En caso afirmativo, vaya a **Paso 9**.
- Si no, vaya a **Paso 16**.

Comprobar si el espacio de disco de nodo en espera está lleno. (Omita esta comprobación para versiones posteriores a MRS 3.1.2.)

Paso 9 Inicie sesión en el nodo DBService en espera como usuario **root**.

Paso 10 Ejecute el comando **su - omm** para cambiar a usuario **omm**.

Paso 11 Vaya al directorio **${DBSERVER_HOME}** y ejecute los siguientes comandos para obtener el directorio de datos de DBService:

cd ${DBSERVER_HOME}

source .dbservice_profile

echo ${DBSERVICE_DATA_DIR}

Paso 12 Ejecute el comando **df -h** para ver la información de uso de la partición del disco del sistema.

Paso 13 Compruebe si el espacio de directorio de datos de DBService está lleno.

- En caso afirmativo, vaya a **Paso 14**.
- Si no, vaya a **Paso 16**.

Paso 14 Amplíe la capacidad del disco.

Paso 15 Después de ampliar la capacidad del disco, espere 2 minutos y compruebe si la alarma está borrada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 16**.

Recopilar información de fallas.

Paso 16 En el portal del FusionInsight Manager, elija **O&M** > **Log > Download**.

Paso 17 En el área **Service**, seleccione **DBService** del clúster de destino y **OS**, **OS Statistics** y **OS Performance** en **OMS** y haga clic en **OK**.

Paso 18 Haga clic en  en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 19 Póngase en contacto con el y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.196 ALM-27005 El uso de conexiones de base de datos supera el umbral

Descripción

El sistema comprueba el uso del número de conexiones de base de datos de los nodos donde se encuentran las instancias de DBServer cada 30 segundos y compara el uso con el umbral.

Si el uso excede el umbral durante cinco veces consecutivas (este número es configurable, y 5 es el valor predeterminado) el sistema genera esta alarma. El umbral de uso predeterminado es 90%, y puede configurarlo en función de los requisitos del sitio.

El conteo de desencadenador es configurable. Esta alarma se borra en los siguientes escenarios:

- El conteo de desencadenadores es 1, y el uso del número de conexiones de base de datos es menor o igual que el umbral.
- El conteo de desencadenadores es mayor que 1, y el uso del número de conexiones de base de datos es menor o igual al 90% del umbral.

Atributo

ID de alarma	Gravedad de la alarma	Borrado automáticamente
27005	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger Condition	Especifica el umbral que activa la alarma. Si el valor del indicador actual excede este umbral, se genera la alarma.

Impacto en el sistema

Los servicios de capa superior pueden no conectarse a la base de datos de DBService, lo que afecta a los servicios.

Causas posibles

- Se utilizan demasiadas conexiones de base de datos.
- El número máximo de conexiones de base de datos no está configurado correctamente.
- El umbral de alarma o el recuento de disparos de alarma están configurados incorrectamente.

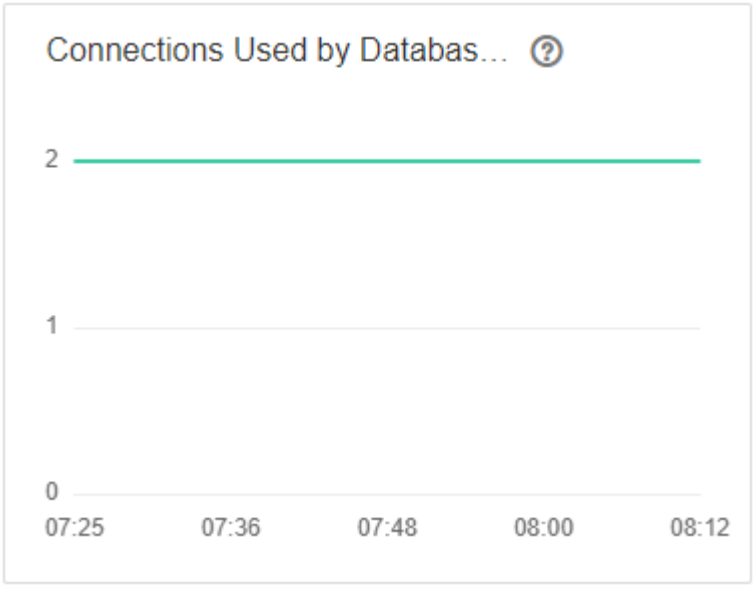
Procedimiento

Comprobar si se utilizan demasiadas conexiones de datos

Paso 1 En FusionInsight Manager, haga clic en DBService en la lista de servicios en el panel de navegación izquierdo. Se muestra la página de supervisión de DBService.

Paso 2 Observe el número de conexiones utilizadas por el usuario de la base de datos, como se muestra en **Figura 9-72**. En función del escenario de servicio, reduzca el número de conexiones de usuario de base de datos.

Figura 9-72 Número de conexiones utilizadas por los usuarios de la base de datos



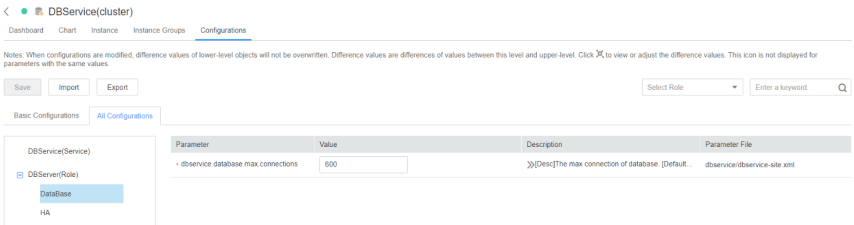
Paso 3 Espere 2 minutos y compruebe si la alarma se borra automáticamente.

- Si lo es, no se requiere ninguna otra acción.
- Si no es así, vaya a **Paso 4**.

Comprobar si el número máximo de conexiones de base de datos está configurado correctamente

Paso 4 Inicie sesión en el FusionInsight Manager y seleccione **Cluster** > *Name of the desired cluster* > **Services** > **DBService** > **Configurations**. En la página mostrada, seleccione la pestaña **All Configurations** y aumente el número máximo de conexiones de base de datos en función de los requisitos de servicio, como se muestra en **Figura 9-73**. Haga clic en **Save**. En el cuadro de diálogo **Save configuration** que se muestra, haga clic en **OK**.

Figura 9-73 Establecer el número máximo de conexiones de base de datos



Paso 5 Después de cambiar el número máximo de conexiones de base de datos, reinicie DBService (no reinicie los servicios de capa superior).

Procedimiento: Inicie sesión en el FusionInsight Manager y elija **Cluster** > *Name of the desired cluster* > **Services** > **DBService**. En la página mostrada, elija **More** > **Restart Service**. Ingrese la contraseña del usuario de inicio de sesión actual y haga clic en **OK**. No seleccione **Restart upper-layer services.**, haga clic en **OK**.

Paso 6 Después de reiniciar el servicio, espere 2 minutos y compruebe si la alarma está desactivada.

- Si lo es, no se requiere ninguna otra acción.
- Si no es así, vaya a **Paso 7**.

Comprobar si el umbral de alarma o el conteo de desencadenadores está configurado correctamente

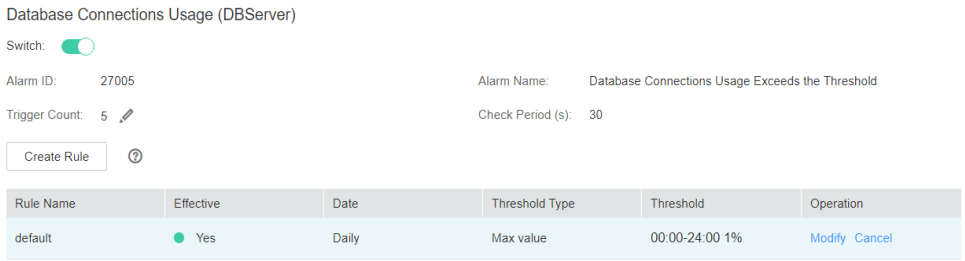
Paso 7 Inicie sesión en el FusionInsight Manager y cambie el umbral de alarma y el conteo de desencadenadores de alarma según el uso real de la conexión a la base de datos.

Elija **O&M**> **Alarm** > **Thresholds** > *Name of the desired cluster* > **DBService > Database > Database Connections Usage (DBServer)**. En el área **Database Connections Usage (DBServer)**, haga clic en el icono de lápiz situado junto a la pestaña **Trigger Count**. En el cuadro de diálogo mostrado, cambie el recuento de desencadenadores, como se muestra en **Figura 9-74**.

NOTA

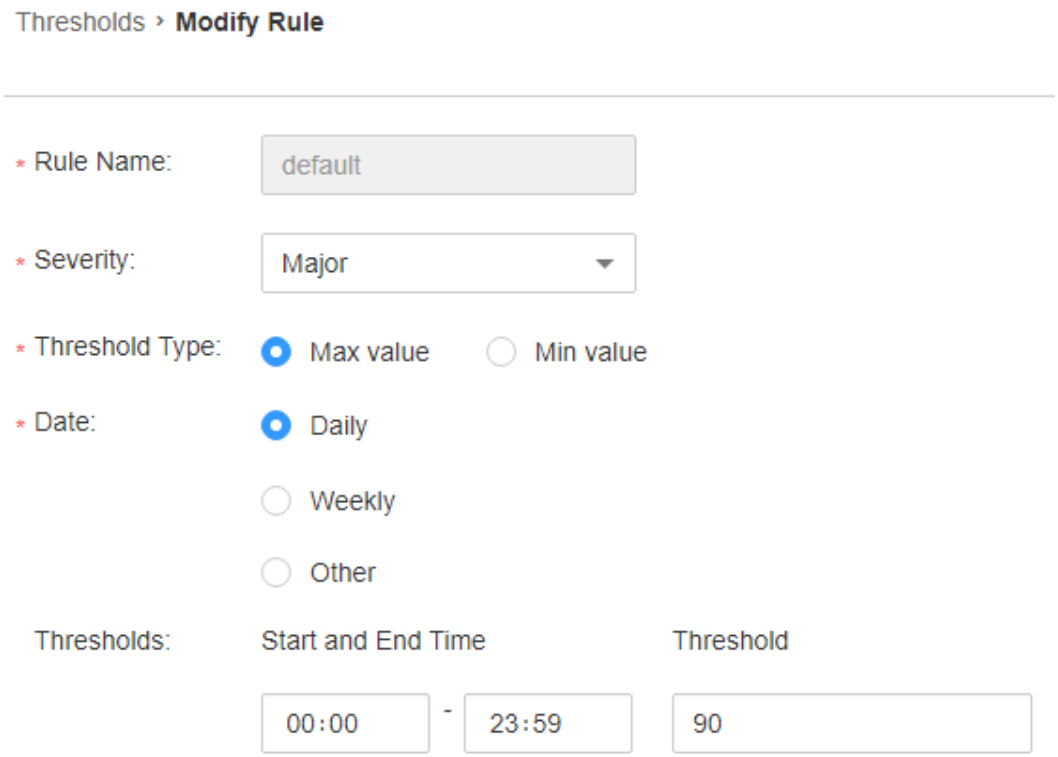
Trigger Count: Si el uso del número de conexiones de base de datos excede el umbral consecutivamente por más que el valor de este parámetro, se genera una alarma.

Figura 9-74 Configuración de trigger count de alarma



En función del uso real de la conexión a la base de datos, elija **O&M** >**Alarm** > **Thresholds** > *Name of the desired cluster* > **DBService > Database > Database Connections Usage (DBServer)**. En el área **Database Connections Usage (DBServer)**, haga clic en **Modify** en la columna **Operation**. En el cuadro de diálogo **Modify Rule**, modifique los parámetros necesarios y haga clic en **OK** como se muestra en **Figura 9-75**.

Figura 9-75 Establecer umbral de alarma



Paso 8 Espere 2 minutos y compruebe si la alarma se borra automáticamente.

- Si lo es, no se requiere ninguna otra acción.
- Si no es así, vaya a **Paso 9**.

Recopilar información de fallas.

Paso 9 En FusionInsight Manager, elija **O&M** > **Log** > **Download**.

Paso 10 Seleccione **DBService** en el clúster requerido en el **Service**.

Paso 11 Especifique el host para recopilar registros estableciendo el parámetro **Host** que es opcional. De forma predeterminada, se seleccionan todos los hosts.

Paso 12 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 13 Póngase en contacto con el y envíe los registros de fallas recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.197 ALM-27006 El uso de espacio en disco del directorio de datos supera el umbral

Descripción

El sistema comprueba el uso de espacio en disco del directorio de datos en el nodo DBServer activo cada 30 segundos y compara el uso del disco con el umbral. La alarma se genera cuando el uso de espacio en disco excede el umbral durante cinco veces consecutivas (el valor predeterminado). El número de veces consecutivas es configurable. El umbral de uso de espacio en disco del directorio de datos se establece en 80% de forma predeterminada, que también es configurable.

El valor de **hit number** es configurable. Cuando el valor se establece en **1** y el uso de espacio en disco es inferior o igual al umbral, la alarma se borra. Cuando el valor es mayor que 1 y el uso de espacio en disco es menor que 90% del umbral, la alarma se borra.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
27006	Importante	Sí

Parámetros

Nombre	Significado
ClusterName	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
PartitionName	Especifica la partición de disco donde se genera la alarma.
Trigger Condition	Especifica el umbral que activa la alarma. Si el valor del indicador real excede este umbral, se genera la alarma.

Impacto en el sistema

- Los procesos de servicio no están disponibles.

- Cuando el uso de espacio en disco del directorio de datos supera el 90%, la base de datos informa de la alarma "Base de datos entra en el modo de solo lectura" y entra en el modo de solo lectura, lo que puede causar la pérdida de datos de servicio.

Causas posibles

- El umbral de alarma está configurado incorrectamente.
- El volumen de datos de la base de datos es demasiado grande o la configuración del disco no puede cumplir con los requisitos de servicio, lo que provoca un uso excesivo del disco.

Procedimiento

Comprobar si el umbral está configurado correctamente.

Paso 1 En FusionInsight Manager, seleccione **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster* > **DBService** > **Database** > **Disk Space Usage of the Data Directory** para comprobar si el umbral de alarma es adecuado (el valor predeterminado 80% es un valor adecuado).

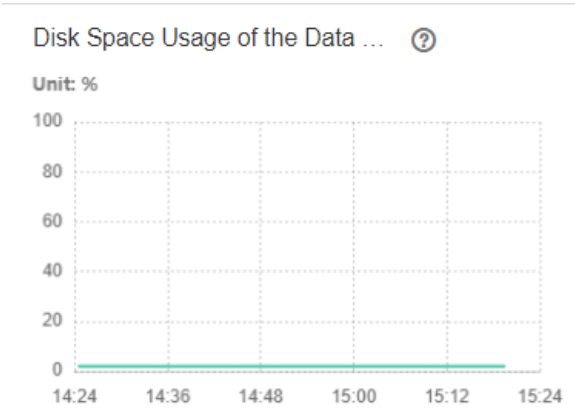
- En caso afirmativo, vaya a **Paso 3**.
- Si no, vaya a **Paso 2**.

Paso 2 Cambie el umbral de alarma en función de la situación real del servicio.

Paso 3 Elija **Cluster** > *Name of the desired cluster* > **Services** > **DBService**. En la página **Dashboard**, vea el gráfico **Disk Space Usage of the Data Directory** y compruebe si el uso de espacio en disco del directorio de datos es inferior al umbral.

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 5**.

Figura 9-76 Uso del espacio en disco del directorio de datos



Paso 4 Espere 2 minutos y compruebe si la alarma se borra automáticamente.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 5**.

Comprobar si archivos grandes se escriben incorrectamente en el disco.

Paso 5 Inicie sesión en el nodo DBService activo como usuario **omm**.

Paso 6 Ejecute los siguientes comandos para ver los archivos cuyo tamaño excede los 500 MB en el directorio de datos y compruebe si hay archivos grandes escritos incorrectamente en el directorio:

source $DBSERVER_HOME/.dbservice_profile

find "$DBSERVICE_DATA_DIR"/../ -type f -size +500M

- En caso afirmativo, vaya a **Paso 7**.
- Si no, vaya a **Paso 8**.

Paso 7 Maneje los archivos de gran tamaño en función del escenario real y comprobar si la alarma se borra 2 minutos más tarde.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 8**.

Recopilar información de fallas.

Paso 8 En FusionInsight Manager, elija **O&M** > **Log** > **Download**.

Paso 9 Expanda la lista desplegable **Service** y seleccione **DBService** para el clúster de destino.

Paso 10 Especifique el host para recopilar registros estableciendo el parámetro **Host** que es opcional. De forma predeterminada, se seleccionan todos los hosts.

Paso 11 Haga clic en  en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 12 Póngase en contacto con el y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.198 ALM-27007 La base de datos entra en el modo de solo lectura

Descripción

El sistema comprueba el uso de espacio en disco del directorio de datos en el nodo DBServer activo cada 30 segundos. La alarma se genera cuando el uso de espacio en disco supera el 90%.

La alarma se borra cuando el uso de espacio en disco es inferior al 80%.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
27007	Crítica	Sí

Parámetros

Nombre	Significado
ClusterName	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
Trigger Condition	Especifica el umbral que activa la alarma. Si el valor del indicador real excede este umbral, se genera la alarma.

Impacto en el sistema

La base de datos entra en el modo de solo lectura, causando la pérdida de datos de servicio.

Causas posibles

La configuración del disco no puede cumplir los requisitos de servicio. El uso del disco alcanza el límite superior.

Procedimiento

Comprobar si el uso del espacio en disco alcanza el límite superior.

Paso 1 En FusionInsight Manager, elija **Cluster** > *Name of the desired cluster* > **Services** > **DBService**.

Paso 2 En la página **Dashboard**, vea el gráfico **Disk Space Usage of the Data Directory** y compruebe si el uso de espacio en disco del directorio de datos supera el 90%.

- En caso afirmativo, vaya a **Paso 3**.
- Si no, vaya a **Paso 13**.

Paso 3 Inicie sesión en el nodo de gestión activo de DBServer como usuario **omm** y ejecute los siguientes comandos para comprobar si la base de datos entra en el modo de solo lectura:

source $DBSERVER_HOME/.dbservice_profile

gsql -U omm -W *password* **-d postgres -p 20051**

show default_transaction_read_only;

> **NOTA**
>
> En los comandos anteriores, *password* indica la contraseña del usuario **omm** de la base de datos de DBService (Puede ver la contraseña inicial del usuario omm en **Lista de cuenta de usuario**.). Puede ejecutar el comando **\q** para salir de la base de datos.

Comprueba si el valor de **default_transaction_read_only** es de **on**.

```
POSTGRES=# show default_transaction_read_only;
 default_transaction_read_only
-------------------------------
 on
(1 row)
```

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 13**.

Paso 4 Ejecute los siguientes comandos para abrir el archivo **dbservice.properties**:

source $DBSERVER_HOME/.dbservice_profile

vi ${DBSERVICE_SOFTWARE_DIR}/tools/dbservice.properties

Paso 5 Cambie el valor de **gaussdb_readonly_auto** a **OFF**.

Paso 6 Ejecute el siguiente comando para abrir el archivo **postgresql.conf**:

vi ${DBSERVICE_DATA_DIR}/postgresql.conf

Paso 7 Elimine **default_transaction_read_only = on**.

Paso 8 Ejecute el siguiente comando para que la configuración surta efecto:

gs_ctl reload -D ${DBSERVICE_DATA_DIR}

Paso 9 Inicie sesión en FusionInsight Manager y elija **O&M** > **Alarm** > **Alarms**. A la derecha de la alarma "Database Enters the Read-Only Mode", haga clic en **Clear** en la columna **Operation**. En el cuadro de diálogo que se muestra, haga clic en **OK** para borrar manualmente la alarma.

Paso 10 Inicie sesión en el nodo de gestión activo de DBServer como usuario **omm** y ejecute los siguientes comandos para ver los archivos cuyo tamaño supera los 500 MB en el directorio de datos y comprobar si hay archivos grandes escritos incorrectamente en el directorio:

source $DBSERVER_HOME/.dbservice_profile

find "$DBSERVICE_DATA_DIR"/../ -type f -size +500M

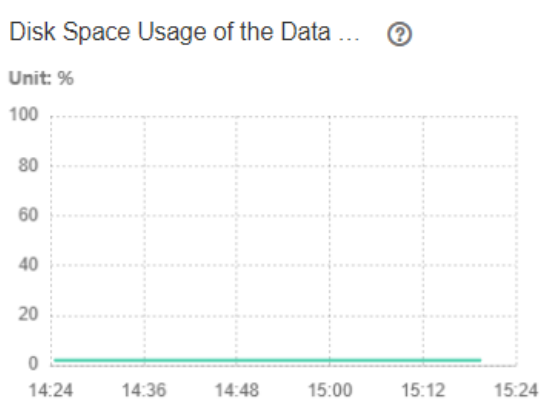
- En caso afirmativo, vaya a **Paso 11**.
- Si no, vaya a **Paso 13**.

Paso 11 Maneje los archivos que están escritos incorrectamente en el directorio según el escenario real.

Paso 12 Inicie sesión en el FusionInsight Manager y elija **Cluster** > *Name of the desired cluster* > **Services** > **DBService**. En la página **Dashboard**, vea el gráfico **Disk Space Usage of the Data Directory** y compruebe si el uso de espacio en disco es inferior al 80%.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 13**.

Figura 9-77 Uso del espacio en disco del directorio de datos



Recopilar información de fallas.

Paso 13 En FusionInsight Manager, elija **O&M** > **Log** > **Download**.

Paso 14 Expanda la lista desplegable **Service** y seleccione **DBService** para el clúster de destino.

Paso 15 Especifique el host para recopilar registros estableciendo el parámetro **Host** que es opcional. De forma predeterminada, se seleccionan todos los hosts.

Paso 16 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 17 Póngase en contacto con el y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.199 ALM-29000 Servicio Impala no disponible

Descripción

El módulo de alarma comprueba el estado del servicio Impala cada 30 segundos. Esta alarma se genera si el servicio Impala es anormal.

Esta alarma se borra después de que el servicio de Impala se recupere.

Atributo

ID de alarma	Severidad de alarma	Borrado automáticamente
29000	Crítica	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

Cuando el servicio Impala es anormal, no puede realizar operaciones de clúster en Impala a través de FusionInsight Manager. Las funciones del servicio Impala no están disponibles.

Causas posibles

- El servicio Hive es anormal.
- El servicio KrbServer es anormal.
- El proceso de Impala es anormal.

Procedimiento

Comprobar si los servicios de los que depende Impala son normales.

Paso 1 En FusionInsight Manager, seleccione **Cluster** > **Services** para comprobar si Hive y KrbServer están detenidos.

- En caso afirmativo, inicie los servicios parados y vaya a **Paso 2**.
- Si no, vaya a **Paso 3**.

Paso 2 En FusionInsight Manager, seleccione **O&M** > **Alarm** > **Alarms**. En la lista de alarmas, compruebe si la alarma Serivcio Impala no disponible está desactivada.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 3**.

Paso 3 En FusionInsight Manager, seleccione **O&M** > **Alarm** > **Alarms**. En la lista de alarmas, compruebe si ALM-16004 Servicio Hive no está disponible y ALM-25500 Servicio KrbServer no está disponible.

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 5**.

Paso 4 Rectifique la falla siguiendo el procedimiento de manejo de ALM-16004 Servicio Hive no disponible o ALM-25500 Servicio KrbServer no disponible. Luego, verifique si la alarma se rectificó.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 5**.

Comprobar si el proceso Impala es normal.

Paso 5 En FusionInsight Manager, seleccione **O&M** > **Alarm** > **Alarms**. Compruebe si existe ALM-12007 Falla de proceso en la lista de alarma.

- En caso afirmativo, vaya a **Paso 6**.
- Si no, vaya a **Paso 7**.

Paso 6 Rectifique la falla haciendo referencia al método de manejo de ALM-12007 Falla de proceso, y a continuación, compruebe si la alarma está borrada.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 7**.

Recopilar información de fallas.

Paso 7 En FusionInsight Manager, elija **O&M** > **Log** > **Download**.

Paso 8 Expanda la lista desplegable **Service** y seleccione **Impala** para el clúster de destino.

Paso 9 Haga clic en  en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 1 hora antes y después del tiempo de generación de alarma, respectivamente. A continuación, haga clic en **Download**.

Paso 10 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar el fallo que activa la alarma, la alarma se borra automáticamente.

Información relacionada

Ninguna

9.200 ALM-29004 El uso de memoria de proceso Impalad supera el umbral

Descripción

El sistema comprueba el uso de memoria del proceso Impalad cada 30 segundos. Esta alarma se genera cuando el sistema detecta que el uso de memoria excede el umbral predeterminado (80%).

Esta alarma se borra automáticamente cuando el sistema detecta que el uso de memoria del proceso cae por debajo del umbral.

Atributo

ID de alarma	Severidad de alarma	Borrado automáticamente
29004	Menor	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger Condition	Especifica el umbral para activar la alarma.

Impacto en el sistema

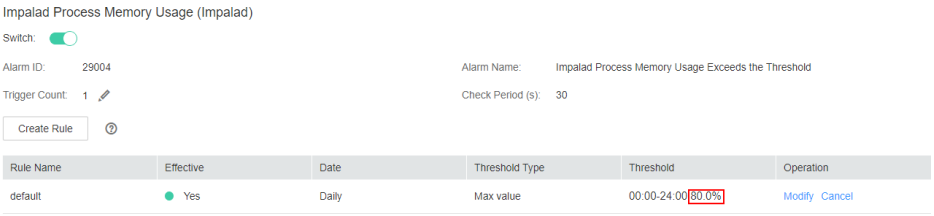
El uso de la memoria es demasiado alto. Algunas tareas de consulta pueden fallar debido a una memoria insuficiente.

Causas posibles

El proceso Impalad está ejecutando un gran número de tareas de consulta.

Procedimiento

Paso 1 En FusionInsight Manager, seleccione **O&M** > **Alarm** > **Thresholds** > **Impala** > **CPU and Memory** > **Impalad Process Memory Usage (Impalad)** para comprobar el umbral.



Paso 2 Si el umbral de alarma es inferior al 80%, aumente el umbral de alarma según sea necesario y compruebe si la alarma está borrada.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 3**.

Paso 3 Si el umbral es superior al 80%, compruebe si existe un gran número de tareas de consulta simultáneas cuando se genera la alarma. Un gran número de tareas de consulta simultáneas hará que el uso de memoria aumente considerablemente. Una vez completadas las tareas, la alarma se borra automáticamente. Durante este período, algunas tareas pueden fallar al ejecutarse o cancelarse debido a una memoria insuficiente. En este caso, inténtalo de nuevo.

NOTA

Si el uso de memoria siempre excede el umbral, es posible que sea necesario ampliar la capacidad del clúster.

----Fin

Eliminación de alarmas

La alarma se borra automáticamente una vez completadas las tareas simultáneas de ráfaga.

Información relacionada

Ninguna

9.201 ALM-29005 Número de conexiones de Impalad JDBC supera el umbral

Descripción

El sistema comprueba el número de conexiones de cliente al nodo Impalad cada 30 segundos. Esta alarma se genera cuando el número de conexiones de cliente excede el umbral personalizado (60 por defecto).

Esta alarma se borra automáticamente cuando el número de conexiones de cliente es menor que el umbral.

Atributo

ID de alarma	Severidad de alarma	Borrado automáticamente
29005	Grave	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger Condition	Especifica el umbral para activar la alarma.

Impacto en el sistema

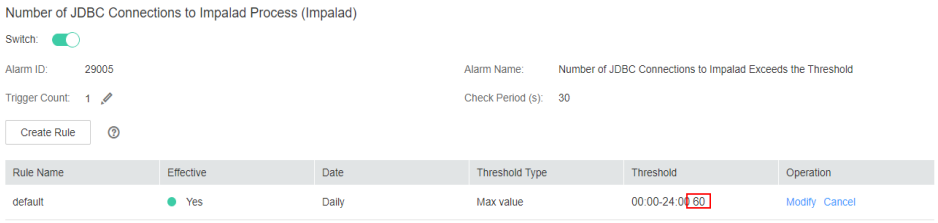
Las nuevas conexiones de cliente pueden estar bloqueadas o incluso fallar.

Causas posibles

El número de conexiones de cliente mantenidas por el servicio Impalad es demasiado grande o el umbral es demasiado pequeño.

Procedimiento

Paso 1 En FusionInsight Manager, seleccione **O&M** > **Alarm** > **Thresholds** > **Impala** > **Connections** > **Number of JDBC Connections to Impalad Process** para comprobar el umbral configurado.

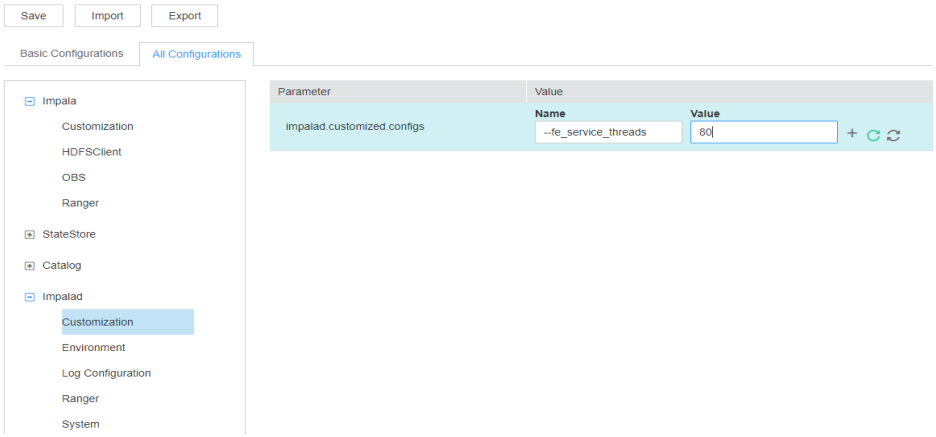


Paso 2 Compruebe el número de aplicaciones JDBC conectadas a Impalad y detenga las aplicaciones inactivas. Compruebe si la alarma se borra automáticamente.

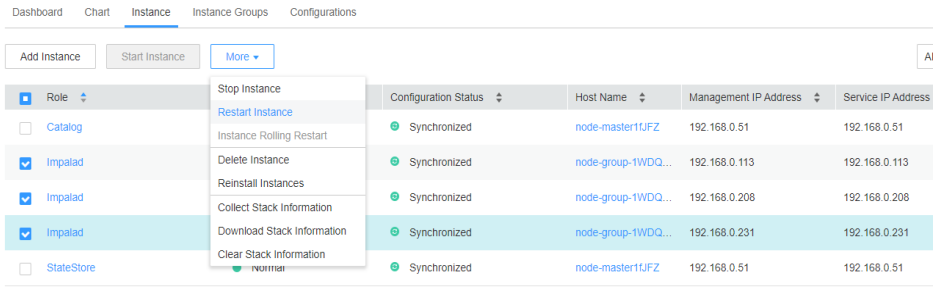
- En caso afirmativo, no es necesario hacer nada más.

- Si no, vaya a **Paso 3** para cambiar el número de conexiones de cliente simultáneas.

Paso 3 En FusionInsight Manager, seleccione **Cluster** > **Impala** > **Configurations** > **All Configurations** > **Impalad** > **Customization**. Agregue el parámetro personalizado **--fe_service_threads**. El valor predeterminado de este parámetro es **64**. Cambie el valor según sea necesario y haga clic en **Save**.



Paso 4 Una vez completadas las tareas de consulta en todos los clientes, haga clic en la pestaña **Instance**. Seleccione todas las instancias de Impalad y reinícielas.



Paso 5 Una vez finalizado el reinicio, se borra la alarma. Ejecute la aplicación que utiliza JDBC para conectarse a Impalad de nuevo.

----Fin

Eliminación de alarmas

Después de rectificar el fallo que activa la alarma, la alarma se borra automáticamente.

Información relacionada

Ninguna

9.202 ALM-29006 Número de conexiones de Impalad ODBC supera el umbral

Descripción

El sistema comprueba el número de conexiones de cliente al nodo Impalad cada 30 segundos. Esta alarma se genera cuando el número de conexiones de cliente excede el umbral personalizado (60 por defecto).

Esta alarma se borra automáticamente cuando el número de conexiones de cliente es menor que el umbral.

Atributo

ID de alarma	Severidad de alarma	Borrado automáticamente
29006	Grave	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger Condition	Especifica el umbral para activar la alarma.

Impacto en el sistema

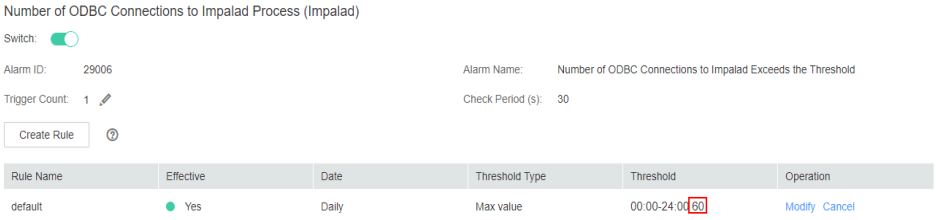
Las nuevas conexiones de cliente pueden estar bloqueadas o incluso fallar.

Causas posibles

El número de conexiones de cliente mantenidas por el servicio Impalad es demasiado grande o el umbral es demasiado pequeño.

Procedimiento

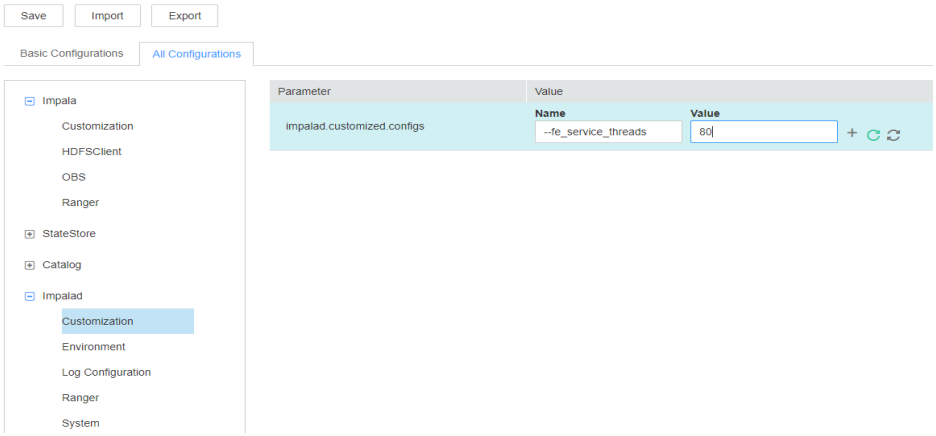
Paso 1 En FusionInsight Manager, seleccione **O&M** > **Alarm** > **Thresholds** > **Impala** > **Connections** > **Number of ODBC Connections to Impalad Process (Impalad)** para comprobar el umbral.



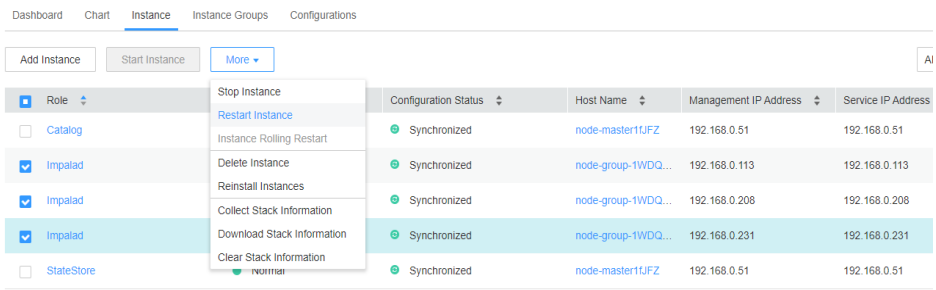
Paso 2 Compruebe el número de aplicaciones ODBC conectadas a Impalad y detenga las aplicaciones inactivas. Compruebe si la alarma se borra automáticamente.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 3** para cambiar el número de conexiones simultáneas soportadas por Impalad.

Paso 3 En FusionInsight Manager, seleccione **Cluster** > **Impala** > **Configurations** > **All Configurations** > **Impalad** > **Customization**. Agregue el parámetro personalizado **--fe_service_threads**. El valor predeterminado de este parámetro es **64**. Cambie el valor según sea necesario y haga clic en **Save**.



Paso 4 Una vez completadas las tareas de consulta en todos los clientes, haga clic en la pestaña **Instance**. Seleccione todas las instancias de Impalad y reinícielas.



Paso 5 Una vez finalizado el reinicio, se borra la alarma. Ejecute la aplicación que utiliza ODBC para conectarse a Impalad de nuevo.

----Fin

Eliminación de alarmas

Después de rectificar el fallo que activa la alarma, la alarma se borra automáticamente.

Información relacionada

Ninguna

9.203 ALM-29100 Servicio Kudu no disponible

Descripción

El sistema comprueba el estado del servicio Kudu cada 60 segundos. Esta alarma se genera cuando el sistema detecta que todas las instancias de Kudu son anormales y considera que el servicio de Kudu no está disponible.

Esta alarma se borra cuando al menos una instancia de Kudu se vuelve normal y el sistema considera que se restaura el servicio de instancia de Kudu.

Atributo

ID de alarma	Severidad de alarma	Borrado automáticamente
29100	Crítica	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
Trigger Condition	Especifica el umbral para activar la alarma.

Impacto en el sistema

Los usuarios no pueden usar el servicio Kudu.

Causas posibles

Algunos casos de Kudu son anormales.

Procedimiento

Gestionar las excepciones de la instancia Kudu.

Paso 1 En FusionInsight Manager, seleccione **O&M** > **Alarm** > **Alarms**. En la página mostrada, busque la alarma ALM-29100 Servicio Kudu no disponible.

Paso 2 En la columna **Location Information**, registre el nombre de host y el nombre de rol.

Paso 3 Elija **Cluster** > **Services** > **Kudu** > **Instance**. Haga clic en el nombre de rol correspondiente al nombre de host en **Paso 2** para restaurar la instancia. Luego, verifique si la alarma se rectificó.

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 5**.

Paso 4 Elija **O&M** > **Alarm** > **Alarms** y compruebe si la alarma está desactivada.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 5**.

Recopilar información de fallas.

Paso 5 En FusionInsight Manager, elija **O&M** > **Log** > **Download**.

Paso 6 En el área **Service**, seleccione los siguientes nodos del clúster deseado.

- Kudu

Paso 7 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 8 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar el fallo que activa la alarma, la alarma se borra automáticamente.

Información relacionada

Ninguna

9.204 ALM-29104 El uso de la memoria de proceso Tserver supera el umbral

Descripción

El sistema comprueba el uso de memoria del proceso Kudu Tserver cada 60 segundos. Esta alarma se genera cuando el sistema detecta que el uso de memoria del proceso Kudu Tserver excede el umbral.

Esta alarma se borra cuando el uso de memoria del proceso Tserver se vuelve normal y el sistema considera que el servicio de instancia Kudu se recupera.

Atributo

ID de alarma	Severidad de alarma	Borrado automáticamente
29104	Crítica	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
Trigger Condition	Especifica el umbral para activar la alarma.

Impacto en el sistema

Los usuarios no pueden usar el servicio Kudu.

Causas posibles

El uso de memoria de una instancia de KuduTserver es demasiado alto.

Procedimiento

Gestionar las excepciones de la instancia Kudu.

Paso 1 En FusionInsight Manager, seleccione **O&M** > **Alarm** > **Alarms**. En la página mostrada, localice la alarma ALM-29104 El uso de la memoria de proceso del servidor Tserver supera el umbral.

Paso 2 Elija **O&M** > **Alarm** > **Threshold Configuration** > **Kudu**. Localice el umbral de alarma y compárelo con el elemento de monitoreo de memoria de la instancia Kudu del clúster para comprobar si el uso de memoria excede el umbral. Si el uso de memoria excede el umbral, rectifique la falla o cambie el umbral.

Paso 3 Elija **O&M** > **Alarm** y compruebe si la alarma está desactivada.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya al paso 4.

Recopilar información de fallas.

Paso 4 En FusionInsight Manager, elija **O&M** > **Log** > **Download**.

Paso 5 En el área **Service**, seleccione los siguientes nodos del clúster deseado.

- Kudu

Paso 6 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 7 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar el fallo que activa la alarma, la alarma se borra automáticamente.

Información relacionada

Ninguna

9.205 ALM-29106 El uso de la CPU del proceso Tserver supera el umbral

Descripción

El sistema comprueba el estado del servicio Kudu cada 60 segundos. Esta alarma se genera cuando el sistema detecta que el uso de CPU del proceso Kudu Tserver es demasiado alto.

Esta alarma se borra cuando el uso de la CPU del proceso Tserver se vuelve normal y el sistema considera que el servicio de instancia Kudu se recupera.

Atributo

ID de alarma	Severidad de alarma	Borrado automáticamente
29106	Crítica	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.

Nombre	Significado
Trigger Condition	Especifica el umbral para activar la alarma.

Impacto en el sistema

Los usuarios no pueden usar el servicio Kudu.

Causas posibles

El uso de CPU de una instancia de KuduTserver es demasiado alto.

Procedimiento

Gestionar las excepciones de la instancia Kudu.

Paso 1 En FusionInsight Manager, elija **O&M** >**Alarm**. En la página mostrada, compruebe si se genera ALM-29106 Uso de CPU de proceso Tserver supera el umbral.

- En caso afirmativo, vaya a **2**.
- Si no, vaya al paso **4**.

Paso 2 Elija **O&M** > **Alarm** > **Thresholds** > **Kudu**. Localice el umbral de alarma y compruebe si el uso de CPU de la instancia Kudu del clúster excede el umbral. En caso afirmativo, rectifique la falla o cambie el umbral.

Paso 3 Elija **O&M** > **Alarm** y compruebe si la alarma está desactivada.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya al paso **4**.

Recopilar información de fallas.

Paso 4 En FusionInsight Manager, elija **O&M** > **Log** > **Download**.

Paso 5 En el área **Service**, seleccione los siguientes nodos del clúster deseado.

- Kudu

Paso 6 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 7 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar el fallo que activa la alarma, la alarma se borra automáticamente.

Información relacionada

Ninguna

9.206 ALM-29107 El uso de la memoria de proceso de Tserver supera el umbral

Descripción

El sistema comprueba el estado del servicio Kudu cada 60 segundos. Esta alarma se genera cuando el uso de memoria del proceso Kudu Tserver excede el umbral.

Esta alarma se borra cuando el uso de memoria del proceso Tserver se vuelve normal y el sistema considera que el servicio de instancia Kudu se recupera.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
29107	Crítica	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
Trigger Condition	Especifica el umbral para activar la alarma.

Impacto en el sistema

Los usuarios no pueden usar el servicio Kudu.

Causas posibles

El uso de memoria de la instancia KuduTserver es demasiado alto.

Procedimiento

Gestionar las excepciones de la instancia Kudu.

Paso 1 En FusionInsight Manager, elija **O&M** >**Alarm**. En la página mostrada, localice la alarma ALM-29107 El uso de la memoria de proceso de Tserver supera el umbral y vea la fuente de la alarma.

Paso 2 Elija **O&M** > **Alarm** > **Threshold Configuration** > **Kudu**, encuentre el umbral de la alarma, compare el uso de memoria de la instancia KuduTserver en el clúster con el umbral y encuentre el nodo cuyo uso de memoria excede el umbral.

Agregue nodos o reprograme trabajos para reducir el uso de memoria del nodo Tserver o cambie el umbral.

Paso 3 Elija **O&M** > **Alarm** y compruebe si la alarma está desactivada.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **4**.

Recopilar información de fallas.

Paso 4 En FusionInsight Manager, seleccione **O&M**. En el panel de navegación de la izquierda, elija **Log** > **Download**.

Paso 5 En el área **Service**, seleccione los siguientes nodos del clúster deseado.

- Kudu

Paso 6 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 7 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

Información relacionada

Ninguna

9.207 ALM-38000 Servicio Kafka no disponible

Descripción

El sistema comprueba el estado del servicio Kafka cada 30 segundos. Esta alarma se genera cuando el servicio Kafka no está disponible.

Esta alarma se borra cuando se recupera el servicio Kafka.

Atributo

ID de alarma	Gravedad de la alarma	Borrado automáticamente
38000	Crítica	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

El clúster no puede proporcionar el servicio de Kafka y los usuarios no pueden realizar nuevas tareas de Kafka.

Causas posibles

- El servicio KrbServer es anormal.(Omita este paso si se utiliza el modo normal.)
- El servicio ZooKeeper es anormal o no responde.
- La instancia de Broker en el clúster de Kafka es anormal.

Procedimiento

Verificar el estado del servicio KrbServer. (Omita este paso si se usa el modo normal).

Paso 1 En el portal del FusionInsight Manager, elija **Cluster** > *Name of the desired cluster* > **Services > KrbServer**.

Paso 2 Compruebe si el estado de ejecución del servicio KrbServer es de tipo **Normal**.

- En caso afirmativo, vaya a **Paso 5**.
- Si no, vaya a **Paso 3**.

Paso 3 Rectifique la falla siguiendo los pasos indicados en el documento **ALM-25500 Servicio KrbServer no disponible**.

Paso 4 Realice **Paso 2** de nuevo.

Verificar el estado del clúster de ZooKeeper.

Paso 5 Compruebe si el estado de ejecución del servicio ZooKeeper es de tipo **Normal**.

- En caso afirmativo, vaya a **Paso 8**.
- Si no, vaya a **Paso 6**.

Paso 6 Si el servicio ZooKeeper se detiene, inícielo, si no, rectifique la falla siguiendo los pasos indicados en el documento **ALM-13000 Servicio ZooKeeper no disponible**.

Paso 7 Realice **Paso 5** de nuevo.

Comprobar el estado de Broker.

Paso 8 Seleccione **Cluster** > *Name of the desired cluster* > **Services** > **Kafka** > **Instance** para ir a la página de instancias de Kafka.

Paso 9 Compruebe si todas las instancias de **Roles** se están ejecutando correctamente.

- En caso afirmativo, vaya a **Paso 11**.
- Si no, vaya a **Paso 10**.

Paso 10 Seleccione todas las instancias de Broker, elija **More** > **Restart Instance** y compruebe si las instancias se reinician correctamente.

- En caso afirmativo, vaya a **Paso 11**.
- Si no, vaya a **Paso 13**.

Paso 11 Elija **Cluster** > *Name of the desired cluster* > **Services** > **Kafka** para comprobar si el estado de ejecución es de tipo **Normal**.

- En caso afirmativo, vaya a **Paso 12**.
- Si no, vaya a **Paso 13**.

Paso 12 Espere 30 segundos y compruebe si la alarma está desactivada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 13**.

Recopilación de información de error

Paso 13 En el portal de FusionInsight Manager, seleccione **O&M** > **Log** > **Download**.

Paso 14 Seleccione **Kafka** en el clúster requerido en la lista desplegable **Service**.

Paso 15 Haga clic en  en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 16 Póngase en contacto con el y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.208 ALM-38001 Capacidad de disco Kafka insuficiente

Descripción

El sistema comprueba el uso del disco Kafka cada 60 segundos y compara el uso real del disco con el umbral. El uso del disco tiene un umbral predeterminado. Esta alarma se genera cuando el uso del disco es mayor que el umbral.

Puede cambiar el umbral en **O&M** > **Alarm** > **Thresholds**. En la lista de servicios, elija **Kafka > Disk > Broker Disk Usage (Broker)** y cambie el umbral.

Cuando el **Trigger Count** es 1, esta alarma se borra cuando el uso del disco Kafka es menor o igual al umbral. Cuando el **Trigger Count** es mayor que 1, esta alarma se borra cuando el uso del disco Kafka es menor o igual al 90% del umbral.

Atributo

ID de alarma	Gravedad de la alarma	Borrado automáticamente
38001	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
PartitionName	Especifica la partición de disco donde se genera la alarma.
Trigger Condition	Especifica el umbral que activa la alarma. Si el valor del indicador actual excede este umbral, se genera la alarma.

Impacto en el sistema

Las operaciones de escritura de datos Kafka se ven afectadas.

Causas posibles

- La configuración (como el número y el tamaño) de los discos para almacenar datos de Kafka no puede cumplir con el requisito del tráfico de servicio actual, debido a lo cual el uso del disco alcanza el límite superior.
- El tiempo de retención de datos es demasiado largo, debido a lo cual el uso del disco de datos alcanza el límite superior.
- El plan de servicio no distribuye los datos de manera uniforme, debido a lo cual el uso de algunos discos alcanza el límite superior.

Procedimiento

Verificar la configuración del disco de datos de Kafka.

Paso 1 En el portal del Administrador FusionInsight y haga clic en **O&M** > **Alarm** > **Alarms**.

Paso 2 En la lista de alarmas, localice la alarma y obtenga **HostName** de **Location**.

Paso 3 Haga clic en **Cluster** > *Name of the desired cluster* > **Hosts**.

Paso 4 En la lista de hosts, haga clic en el nombre de host obtenido en **Paso 2**.

Paso 5 Compruebe si el área **Disk** contiene el nombre de la partición en la alarma.

- En caso afirmativo, vaya a **Paso 6**.
- En caso negativo, borre manualmente la alarma y no se requiere ninguna operación adicional.

Paso 6 Compruebe si el uso de la partición de disco contenida en la alarma alcanza el 100% en el área **Disk**.

- En caso afirmativo, maneje la alarma siguiendo las instrucciones en **Información relacionada**.
- Si no, vaya a **Paso 7**.

Comprobar la duración del almacenamiento de datos de Kafka.

Paso 7 Seleccione **Cluster** > *Name of the desired cluster* > **Services** > **Kafka** > **Configurations**.

Paso 8 Compruebe si el valor del parámetro **disk.adapter.enable** está establecido en **true**.

- En caso afirmativo, vaya a **Paso 10**.
- Si no, vaya a **Paso 9**.

Paso 9 Establezca el valor de **disk.adapter.enable** en **true**. Compruebe si el valor de **adapter.topic.min.retention.hours** está configurado correctamente.

- En caso afirmativo, vaya a **Paso 10**.
- En caso negativo, ajuste el período de retención de datos en función de los requisitos de servicio.

AVISO

Si la función de adaptación automática del disco está habilitada, se eliminan algunos datos históricos de temas especificados. Si no se puede ajustar el período de retención de algunos temas, haga clic en **All Configurations** y agregue los temas al valor del parámetro **disk.adapter.topic.blacklist**.

Paso 10 Espere 10 minutos y compruebe si el uso de discos defectuosos se reduce.

- En caso afirmativo, espere hasta que se borre la alarma.
- Si no, vaya a **Paso 11**.

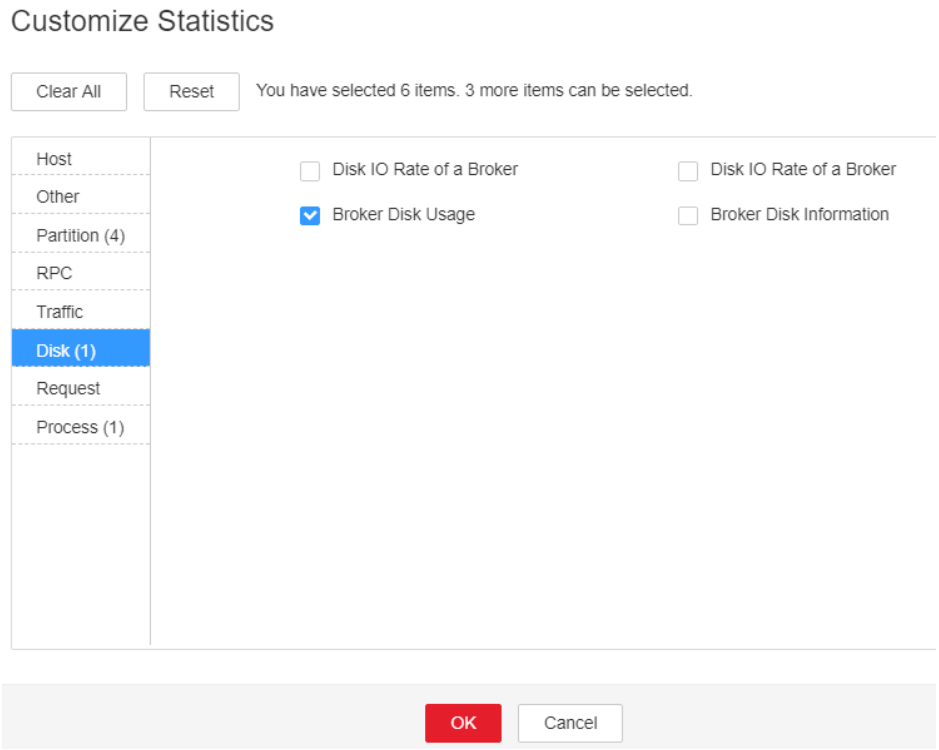
Comprobar el plan de datos de Kafka.

Paso 11 En el área **Instance**, haga clic en **Broker**. En el área **Real Time** de Broker, haga clic en el menú desplegable en el área Chart y elija **Customize** para personalizar los elementos de monitoreo.

Paso 12 En el cuadro de diálogo, seleccione **Disk** > **Broker Disk Usage** y haga clic en **OK**.

Se muestra la información de uso del disco Kafka.

Figura 9-78 Uso del disco del broker



Paso 13 Vea la información en **Paso 12** para comprobar si existe solo la partición de disco para la que se genera la alarma en **Paso 2**.

- En caso afirmativo, vaya a **Paso 14**.
- Si no, vaya a **Paso 15**.

Paso 14 Realice la planificación del disco y monte un nuevo disco. Vaya a la página **Instance Configurations** del nodo para el que se genera la alarma, modifique **log.dirs** y agregue otros directorios de disco y reinicie la instancia de Kafka.

Paso 15 Determine si se debe acortar el tiempo de retención de datos configurado en Kafka según los requisitos de servicio y el tráfico de servicio.

- En caso afirmativo, vaya a **Paso 16**.
- Si no, vaya a **Paso 17**.

Paso 16 Inicie sesión en el Administrador de FusionInsight, seleccione **Cluster** > *Name of the desired cluster* > **Services** > **Kafka** > **Configurations**, y haga clic en **All Configurations**. En el cuadro de búsqueda de la derecha, escriba **log.retention.hours**. El valor del parámetro indica el tiempo de retención de datos predeterminado del tema. Puede cambiar el valor a uno más pequeño.

NOTA

- Para un tema cuyo tiempo de retención de datos se configura solo, la modificación del tiempo de retención de datos en la página Kafka Service Configuration no tiene efecto.
- Para modificar el tiempo de retención de datos de un tema, utilice la interfaz de línea de comandos (CLI) del cliente Kafka para configurar el tema.

  Ejemplo: **kafka-topics.sh --zookeeper "***ZooKeeper IP address***:2181/kafka" --alter --topic "***Topic bane***" --config retention.ms= "***retention time***"**

Paso 17 Compruebe si el uso de algunos discos alcanza el límite superior debido a una configuración poco razonable de las particiones de algunos temas. Por ejemplo, el número de particiones configuradas para un tema con un volumen de datos grande es menor que el número de discos. En este caso, los datos no se asignan uniformemente a los discos.

NOTA

Si no sabe qué temas tienen una gran cantidad de datos de servicio, realice los siguientes pasos:

1. Inicie sesión en un nodo de instancia en función de la información de nodo host obtenida en **Paso 2**.
2. Vaya al directorio de datos (directorio especificado por **log.dirs** antes de la modificación en **Paso 14**).
3. Ejecute el siguiente comando para comprobar si hay un tema con una partición que use un gran espacio en disco.

   du -h --max-depth=1 ./

- En caso afirmativo, vaya a **Paso 18**.
- Si no, vaya a **Paso 19**.

Paso 18 En la CLI del cliente Kafka, ejecute el siguiente comando para realizar la expansión de la capacidad de la partición para el tema:

kafka-topics.sh --zookeeper "*ZooKeeper IP address***:2181/kafka" --alter --topic "***Topic name***" --partitions="***New number of partitions***"**

NOTA

- Se recomienda establecer el nuevo número de particiones en un múltiplo del número de discos de datos de Kafka.
- El paso puede no borrar rápidamente la alarma, y es necesario modificar el tiempo de retención de datos en **Paso 11** para equilibrar gradualmente la asignación de datos.

Paso 19 Determine si se debe realizar la ampliación de la capacidad.

NOTA

Se recomienda realizar la ampliación de la capacidad de Kafka cuando el uso actual del disco supera el 80%.

- En caso afirmativo, vaya a **Paso 20**.
- Si no, vaya a **Paso 21**.

Paso 20 Amplíe la capacidad del disco y compruebe si la alarma se borra después de la ampliación de la capacidad.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 22**.

Paso 21 Verifique si la alarma se ha borrado.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 22**.

Recopilar información de fallas.

Paso 22 En el portal de FusionInsight Manager, seleccione **O&M** > **Log** > **Download**.

Paso 23 Seleccione **Kafka** en el clúster requerido en la lista desplegable **Service**.

Paso 24 Haga clic en  en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 25 Póngase en contacto con el y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Paso 1 Inicie sesión en el Administrador de FusionInsight, elija **Cluster** > *Name of the desired cluster* > **Services** > **Kafka** > **Instance**, detenga la instancia del Broker cuyo estado es **Restoring**, registrar la dirección IP de gestión del nodo donde se encuentra la instancia del Broker y registrar **broker.id**. El valor se puede obtener mediante el siguiente método: Haga clic en el nombre del rol. En la página **Configurations**, seleccione **All Configurations** y busque el parámetro **broker.id**.

Paso 2 Inicie sesión en la dirección IP de gestión grabada como usuario **root** y ejecute el comando **df -lh** para ver el directorio montado cuyo uso del disco es 100%, por ejemplo, **${BIGDATA_DATA_HOME}/kafka/data1**.

Paso 3 Vaya al directorio, ejecute el comando **du -sh *** para ver el tamaño de cada archivo en el directorio, compruebe si existen archivos distintos de **kafka-logs** y determine si estos archivos se pueden eliminar o migrar.

- En caso afirmativo, vaya a **Paso 8**.
- Si no, vaya a **Paso 4**.

Paso 4 Vaya al directorio **kafka-logs**, ejecute el comando **du -sh *** y seleccione la carpeta de partición que desea mover. La regla de nombre es **Topic name-Partition ID**. Registre el tema y la partición.

Paso 5 Modifique los archivos **recovery-point-offset-checkpoint** y **replication-offset-checkpoint** del directorio **kafka-logs** de la misma manera.

1. Disminuya el número en la segunda línea del archivo. (Para quitar varios directorios, el número deducido es igual al número de archivos que se van a quitar.)
2. Elimine la línea de la partición que se va a eliminar. (La estructura de línea es "Topic name Partition ID Offset". Guarde los datos antes de eliminarlos. Posteriormente, el contenido debe agregarse al archivo del mismo nombre en el directorio de destino.)

Paso 6 Modifique los archivos **recovery-point-offset-checkpoint** y **replication-offset-checkpoint** en el directorio de datos de destino. Por ejemplo, **${BIGDATA_DATA_HOME}/kafka/data2/kafka-logs** de la misma manera.

- Aumente el número en la segunda línea del archivo. (Para mover varios directorios, el número agregado es igual al número de archivos que se van a mover.)
- Agregue la partición que desea mover al final del archivo. (La estructura de línea es "Topic name Partition ID Offset". Puede copiar los datos de línea guardados en **Paso 5**.)

Paso 7 Mueva la partición al directorio de destino. Después de mover la partición, ejecute el comando **chown omm:wheel -R** *Partition directory* para modificar el grupo de propietarios de directorios para la partición.

Paso 8 Inicie sesión en FusionInsight Manager y elija **Cluster** > *Name of the desired cluster* > **Services** > **Kafka** > **Instance** para iniciar la instancia del Broker.

Paso 9 Espere de 5 a 10 minutos y compruebe si el estado de salud de la instancia de Broker es de **Normal**.

- En caso afirmativo, resuelva el problema de insuficiencia de capacidad de disco de acuerdo con el método de manejo de "ALM-38001 Espacio en disco de Kafka insuficiente" después de que se elimine la alarma.
- Si no, póngase en contacto con el .

----Fin

9.209 ALM-38002 El uso de memoria heap de Kafka supera el umbral

Descripción

El sistema comprueba el estado del servicio Kafka cada 30 segundos. La alarma se genera cuando el uso de memoria heap de una instancia de Kafka supera el umbral (95% de la memoria máxima) durante 10 veces consecutivas.

Cuando el **Trigger Count** es 1, esta alarma se borra cuando el uso de memoria heap es menor o igual que el umbral. Cuando el **Trigger Count** es mayor que 1, esta alarma se borra cuando el uso de memoria heap es menor o igual al 90% del umbral.

Atributo

ID de alarma	Gravedad de la alarma	Borrado automáticamente
38002	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el nombre del servicio para el que se genera la alarma.

Nombre	Significado
RoleName	Especifica el nombre del rol para el que se genera la alarma.
HostName	Especifica el objeto (ID de host) para el que se genera la alarma.
Trigger Condition	Especifica el umbral que activa la alarma. Si el valor del indicador actual excede este umbral, se genera la alarma.

Impacto en el sistema

Si la memoria heap de Kafka disponible es insuficiente, se produce un desbordamiento de memoria y el servicio se interrumpe.

Causas posibles

La memoria heap de la instancia de Kafka se utiliza en exceso o la memoria heap se asigna de forma inapropiada.

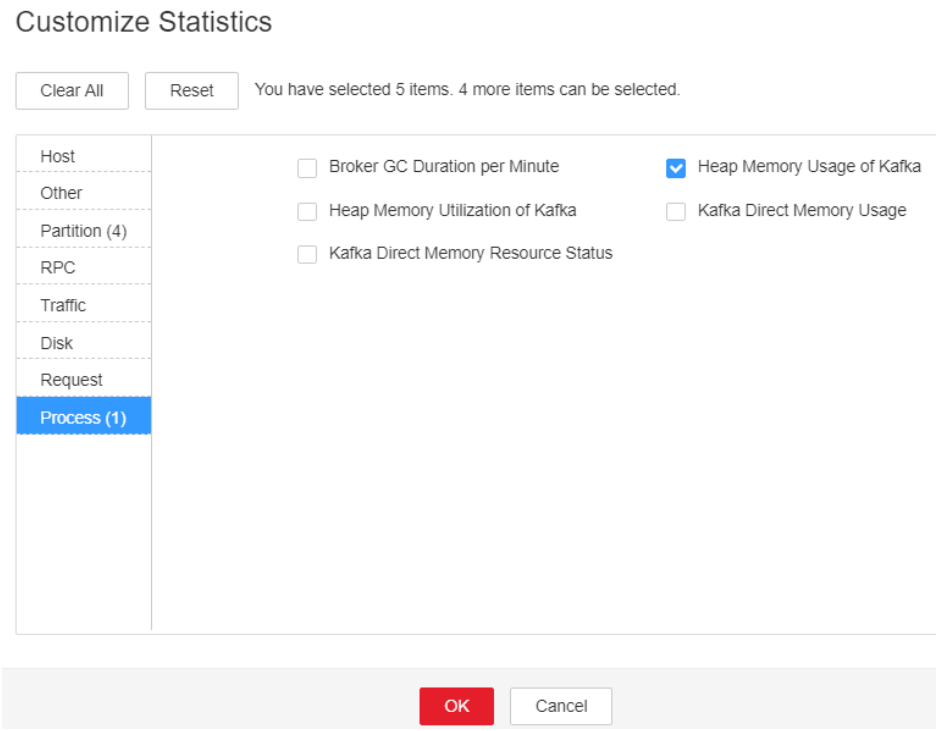
Procedimiento

Comprobar el uso de memoria heap.

Paso 1 En el portal del FusionInsight Manager, elija **O&M** > **Alarm** > **Alarms** > **Kafka Heap Memory Usage Exceeds the Threshold** > **Location**. Compruebe el nombre de host de la instancia involucrada en esta alarma.

Paso 2 En el portal del FusionInsight Manager, seleccione **Cluster** > *Name of the desired cluster* > **Services** > **Kafka** > **Instance**. Haga clic en la instancia para la que se genera la alarma para ir a la página de la instancia. Haga clic en la lista desplegable en la esquina superior derecha del área del gráfico, elija **Customize** > **Process** > **Heap Memory Usage of Kafka** y haga clic en **OK**.

Figura 9-79 Uso de memoria heap de Kafka



Paso 3 Compruebe si la memoria heap usada de Kafka alcanza el 95% de la memoria heap máxima especificada para Kafka.

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 6**.

Comprobar el tamaño de la memoria heap configurado para Kafka.

Paso 4 En el portal del FusionInsight Manager, seleccione **Cluster** > *Name of the desired cluster* > **Services** > **Kafka** > **Configurations** > **All Configurations**> **Broker(Role)** > **Environment**. Aumente el valor de **KAFKA_HEAP_OPTS** haciendo referencia a la Nota.

Figura 9-80 KAFKA_HEAP_OPTS

Parameter	Value
KAFKA_HEAP_OPTS	-Xmx6G -Xms6G

NOTA

- Se recomienda establecer **-Xmx** y **-Xms** en el mismo valor.
- Se recomienda ver **Uso de memoria heap de Kafka** haciendo referencia a **Paso 2** y establecer el valor de **KAFKA_HEAP_OPTS** en el doble del valor de **Memoria heap usada por Kafka.**

Paso 5 Verifique si la alarma se ha borrado.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 6**.

Recopilar información de fallas.

Paso 6 En el portal de FusionInsight Manager, seleccione **O&M** > **Log** > **Download**.

Paso 7 Seleccione **Kafka** en el clúster requerido en la lista desplegable **Service**.

Paso 8 Haga clic en  en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 9 Póngase en contacto con el y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.210 ALM-38004 El uso de memoria directa de Kafka supera el umbral

Descripción

El sistema comprueba el uso de memoria directa del servicio Kafka cada 30 segundos. Esta alarma se genera cuando el uso de memoria directa de una instancia de Kafka supera el umbral (80% de la memoria máxima) durante 10 veces consecutivas.

Cuando el **Trigger Count** es 1, esta alarma se borra cuando el uso de memoria directa es menor o igual al umbral. Cuando el **Trigger Count** es mayor que 1, esta alarma se borra cuando el uso de memoria directa es menor o igual al 90% del umbral.

Atributo

ID de alarma	Gravedad de la alarma	Borrado automáticamente
38004	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.

Nombre	Significado
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger Condition	Especifica el umbral que activa la alarma. Si el valor del indicador actual excede este umbral, se genera la alarma.

Impacto en el sistema

Si la memoria directa disponible del servicio Kafka es insuficiente, se produce un desbordamiento de memoria y el servicio se interrumpe.

Causas posibles

La memoria directa de la instancia de Kafka se sobreutiliza o la memoria directa se asigna de forma inapropiada.

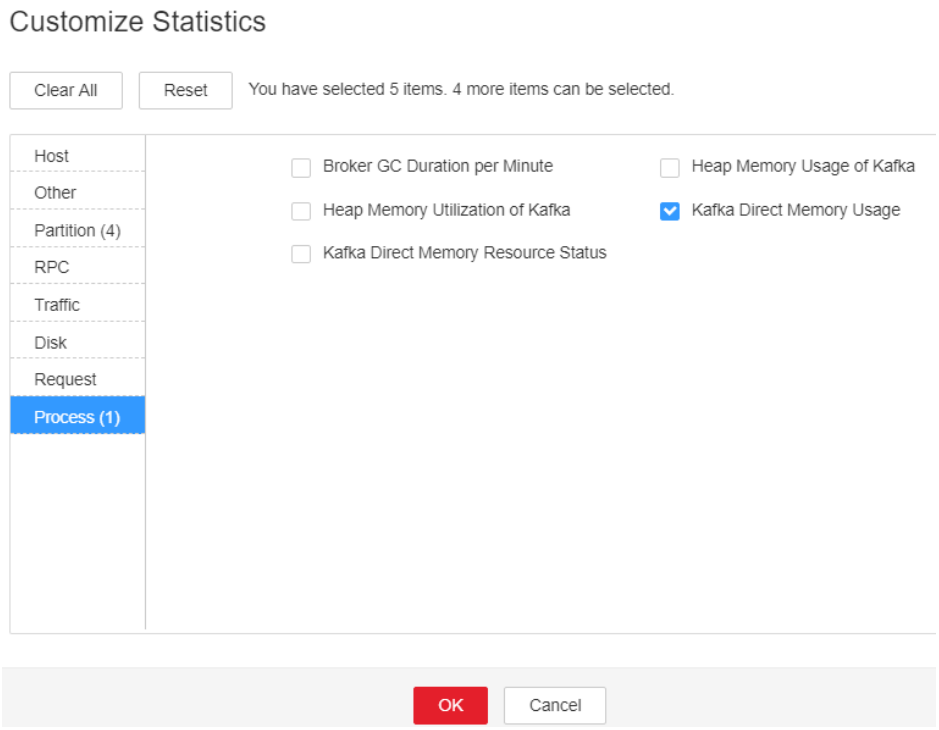
Procedimiento

Comprobar el uso de la memoria directa.

Paso 1 En el portal del FusionInsight Manager, elija **O&M** > **Alarm** > **Alarms** > **Kafka Direct Memory Usage Exceeds the Threshold** > **Location** para comprobar el nombre de host de la instancia para que se genera la alarma.

Paso 2 En el portal del FusionInsight Manager, seleccione **Cluster** > *Name of the desired cluster* > **Services** > **Kafka** > **Instance**. Haga clic en la instancia para la que se genera la alarma para ir a la página de la instancia. Haga clic en el menú desplegable en el área Chart y elija **Customize** > **Process** > **Kafka Direct Memory Usage** y haga clic en **OK**.

Figura 9-81 Uso de memoria directa de Kafka



Paso 3 Compruebe si la memoria directa utilizada de Kafka alcanza el 80% de la memoria directa máxima especificada para Kafka.

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 7**.

Verificar el tamaño de memoria directa configurado para Kafka.

Paso 4 En el portal del FusionInsight Manager, elija **Cluster** > *Name of the desired cluster* > **Services** > **Kafka** > **Configurations** > **All Configurations** > **Broker(Role)** > **Environment** para aumentar el valor de **-Xmx** configurado en el parámetro **KAFKA_HEAP_OPTS** haciendo referencia a la Nota.

NOTA

- Se recomienda establecer **-Xmx** y **-Xms** en el mismo valor.
- Se recomienda ver **Kafka Direct Memory Usage** haciendo referencia a **Paso 2** y establecer el valor de **KAFKA_HEAP_OPTS** en el doble del valor de **Direct Memory Used by Kafka.**

Paso 5 Guarde la configuración y reinicie el servicio Kafka.

Paso 6 Verifique si la alarma se ha borrado.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 7**.

Recopilar información de fallas.

Paso 7 En el portal de FusionInsight Manager, seleccione **O&M** > **Log** > **Download**.

Paso 8 Seleccione **Kafka** en el clúster requerido en la lista desplegable **Service**.

Paso 9 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 10 Póngase en contacto con el y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.211 ALM-38005 La duración de GC del proceso de Broker supera el umbral

Descripción

El sistema comprueba la duración de la recolección de basura (GC) del proceso del Broker cada 60 segundos. Esta alarma se genera cuando la duración de GC excede el umbral (12 segundos por defecto) durante 3 veces consecutivas.

Cuando el **Trigger Count** es 1, esta alarma se borra cuando la duración de GC es menor o igual que el umbral. Cuando el **Trigger Count** es mayor que 1, esta alarma se borra cuando la duración de GC es menor que o igual al 90% del umbral.

Atributo

ID de alarma	Gravedad de la alarma	Borrado automáticamente
38005	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.

Nombre	Significado
HostName	Especifica el host para el que se genera la alarma.
Trigger Condition	Especifica el umbral que activa la alarma. Si el valor del indicador actual excede este umbral, se genera la alarma.

Impacto en el sistema

Una larga duración de GC del proceso de Broker puede interrumpir los servicios.

Causas posibles

La duración de GC de Kafka del nodo es demasiado larga o la memoria heap se asigna de forma inapropiada. Como resultado, los GC ocurren con frecuencia.

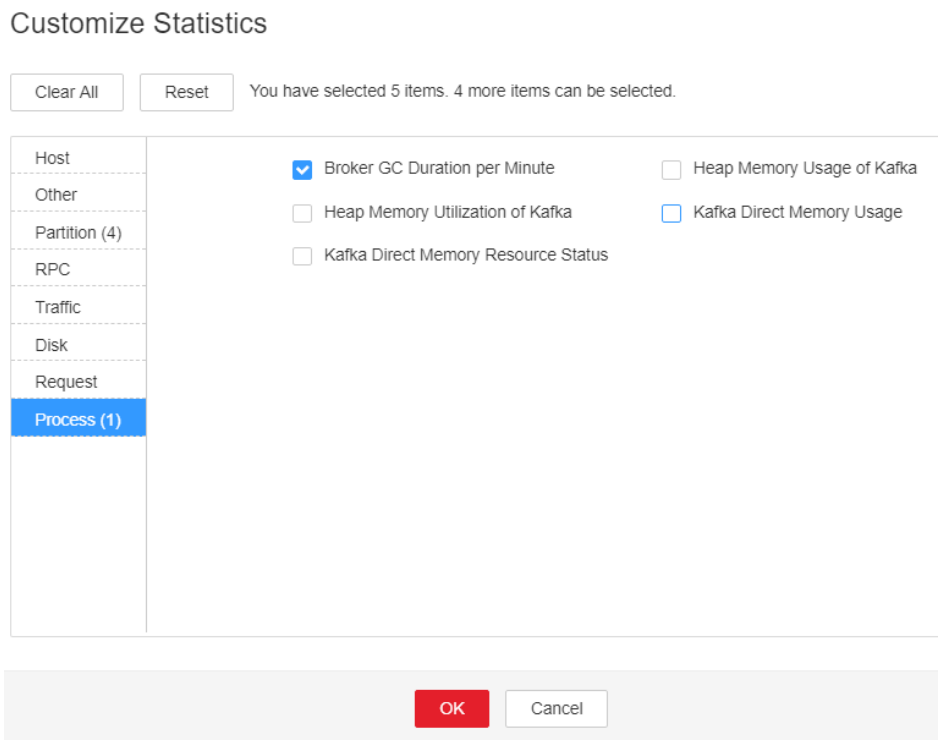
Procedimiento

Comprobar la duración del GC.

Paso 1 En el portal del administrador FusionInsight, elija **O&M** > **Alarm** > **Alarms** > **GC Duration of the Broker Process Exceeds the Threshold** > **Location**. Compruebe el nombre de host de la instancia involucrada en esta alarma.

Paso 2 En el portal del FusionInsight Manager, seleccione **Cluster** > *Name of the desired cluster* > **Services** > **Kafka** > **Instance**. Haga clic en la instancia para la que se genera la alarma para ir a la página de la instancia. Haga clic en la lista desplegable en la esquina superior derecha del área del gráfico, elija **Customize** > **Process** > **Broker GC Duration per Minute** y haga clic en **OK**.

Figura 9-82 Duración de GC de Broker por minuto



Paso 3 Compruebe si la duración del GC del proceso del Broker recopilado cada minuto supera el umbral (12 segundos por defecto).

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 7**.

Verificar el tamaño de memoria directa configurado para Kafka.

Paso 4 En el portal del FusionInsight Manager, elija **Cluster** > *Name of the desired cluster* > **Services** > **Kafka** > **Configurations** > **All Configurations** > **Broker(Role)** > **Environment** para aumentar el valor de **-Xmx** configurado en el parámetro **KAFKA_HEAP_OPTS** haciendo referencia a la Nota.

NOTA

- Se recomienda establecer **-Xmx** y **-Xms** en el mismo valor.
- Se recomienda establecer el valor de **KAFKA_HEAP_OPTS** en el doble del valor de **Direct Memory Used by Kafka.**

  En el portal del FusionInsight Manager, seleccione **Cluster** > *Name of the desired cluster* > **Services** > **Kafka** > **Instance**. Haga clic en la instancia para la que se genera la alarma para ir a la página de la instancia. Haga clic en la lista desplegable en la esquina superior derecha del área del gráfico y elija **Customize** > **Process** > **Kafka Direct Memory Resource Status** para comprobar el valor de **Direct Memory Used by Kafka**.

Paso 5 Guarde la configuración y reinicie el servicio Kafka.

Paso 6 Verifique si la alarma se ha borrado.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 7**.

Recopilar información de fallas.

Paso 7 En el portal de FusionInsight Manager, seleccione **O&M** > **Log** > **Download**.

Paso 8 Seleccione **Kafka** en el clúster requerido en la lista desplegable **Service**.

Paso 9 Haga clic en  en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 10 Póngase en contacto con el y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.212 ALM-38006 El porcentaje de Partition de Kafka que no están completamente sincronizadas supera el umbral

Descripción

El sistema comprueba el porcentaje de Partition de Kafka que no están completamente sincronizadas con el número total de Partition cada 60 segundos. Esta alarma se genera cuando el porcentaje excede el umbral (50% por defecto) durante 3 veces consecutivas.

Cuando el **Trigger Count** es 1, esta alarma se borra cuando el porcentaje es menor o igual al umbral. Cuando el **Trigger Count** es mayor que 1, esta alarma se borra cuando el porcentaje es menor o igual al 90% del umbral.

Atributo

ID de alarma	Gravedad de la alarma	Borrado automáticamente
38006	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.

Nombre	Significado
RoleName	Especifica el rol para el que se genera la alarma.
Trigger Condition	Especifica el umbral que activa la alarma. Si el valor del indicador actual excede este umbral, se genera la alarma.

Impacto en el sistema

Demasiadas Partitions de Kafka que no están completamente sincronizadas afectan a la confiabilidad del servicio. Además, los datos pueden perderse cuando se conmutan Leader.

Causas posibles

Algunos nodos en los que reside la instancia del Broker son anormales o dejan de ejecutarse. Como resultado, las réplicas de algunas Partitions en Kafka están fuera del conjunto de réplicas in-sync (ISR).

Procedimiento

Comprobar instancias de Broker.

Paso 1 En el portal del FusionInsight Manager, seleccione **Cluster** > *Name of the desired cluster* > **Services** > **Kafka** > **Instance**. Se muestra la página de instancias de Kafka.

Paso 2 Compruebe si existen nodos defectuosos entre todos los nodos del Broker.

- En caso afirmativo, registre el nombre de host del nodo y vaya a **Paso 3**.
- Si no, vaya a **Paso 5**.

Paso 3 En el portal del FusionInsight Manager, haga clic en **O&M** > **Alarm** > **Alarms** para comprobar si la falla descrita en **Paso 2** existe en la información de alarma y manejar la alarma basándose en los métodos correspondientes.

Paso 4 En el portal del FusionInsight Manager, seleccione **Cluster** > *Name of the desired cluster* > **Services** > **Kafka** > **Instance**. Se muestra la página de instancias de Kafka.

Paso 5 Compruebe si existen nodos detenidos entre todas las instancias del Broker.

- En caso afirmativo, vaya a **Paso 6**.
- Si no, vaya a **Paso 7**.

Paso 6 Seleccione todas las instancias de Broker detenidas y haga clic en **Start Instance**.

Paso 7 Verifique si la alarma se ha borrado.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 8**.

Recopilar información de fallas.

Paso 8 En el portal de FusionInsight Manager, seleccione **O&M** > **Log** > **Download**.

Paso 9 Seleccione **Kafka** en el clúster requerido en la lista desplegable **Service**.

Paso 10 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 11 Póngase en contacto con el y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.213 ALM-38007 El estado del usuario predeterminado de Kafka es anormal

Descripción

El sistema comprueba el usuario predeterminado de Kafka cada 60 segundos. Esta alarma se genera cuando el sistema detecta que el estado del usuario es anormal.

Trigger Count está establecido en **1**. Esta alarma se borra cuando el estado de usuario se vuelve normal.

Atributo

ID de alarma	Gravedad de la alarma	Borrado automáticamente
38007	Crítica	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.

Nombre	Significado
HostName	Especifica el nombre de host para el que se genera la alarma.
Trigger Condition	Especifica la condición de que el estado de usuario predeterminado de Kafka es anormal.

Impacto en el sistema

Si el estado de usuario predeterminado de Kafka es anormal, la sincronización de metadatos entre Brokers y la interacción entre Kafka y ZooKeeper se verá afectada, lo que afectará a la producción de servicios, el consumo y la creación y eliminación de temas.

Causas posibles

- El servicio Sssd es anormal.
- Algunas instancias de Broker dejan de ejecutarse.

Procedimiento

Compruebe si el servicio Sssd es anormal.

Paso 1 En el portal del FusionInsight Manager, elija **O&M** > **Alarm** > **Alarms** > **Status of Kafka Default User Is Abnormal** > **Location** para comprobar el nombre de host de la instancia para la que se genera la alarma.

Paso 2 Encuentre la información del host en la información de alarma e inicie sesión en el host.

Paso 3 Ejecute el comando **id -Gn kafka** y compruebe si se muestra "No such user" en la salida del comando.

- En caso afirmativo, registre el nombre de host del nodo y vaya a **Paso 4**.
- Si no, vaya a **Paso 6**.

Paso 4 En la página de inicio del FusionInsight Manager, seleccione **O&M** > **Alarm** > **Alarms**. Compruebe si hay **Sssd Service Exception** en la información de alarma. Si lo hay, maneje la alarma basándose en la información de alarma.

Verifique el estado de ejecución de la instancia de Broker.

Paso 5 En la página principal del FusionInsight Manager, elija **Cluster** > *Name of the desired cluster* > **Services** > **Kafka** > **Instance**. Se muestra la página de instancia de Kafka.

Paso 6 Compruebe si hay nodos detenidos en todas las instancias del Broker.

- En caso afirmativo, vaya a **Paso 7**.
- Si no, vaya a **Paso 8**.

Paso 7 Seleccione todas las instancias de Broker detenidas y haga clic en **Start Instance**.

Paso 8 Verifique si la alarma se ha borrado.

- De ser así, no se requiere ninguna acción adicional.

- Si no, vaya a **Paso 9**.

Recopilar información de fallas.

Paso 9 En FusionInsight Manager, elija **O&M** > **Log** > **Download**.

Paso 10 En el área **Service** , seleccione **Kafka** en el clúster requerido.

Paso 11 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 12 Póngase en contacto con el y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.214 ALM-38008 Estado anormal del directorio de datos de Kafka

Descripción

El sistema comprueba el estado del directorio de datos Kafka cada 60 segundos. Esta alarma se genera cuando el sistema detecta que el estado de un directorio de datos es anormal.

Trigger Count está establecido en **1**. Esta alarma se borra cuando el estado del directorio de datos se vuelve normal.

Atributo

ID de alarma	Gravedad de la alarma	Borrado automáticamente
38008	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.

Nombre	Significado
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el nombre de host para el que se genera la alarma.
DirName	Especifica el nombre del directorio para el que se genera la alarma.
Trigger Condition	Especifica la condición de que el estado del directorio de datos Kafka es anormal.

Impacto en el sistema

Si el estado del directorio de datos Kafka es anormal, las réplicas actuales de todas las particiones en el directorio de datos se ponen fuera de línea, y el estado del directorio de datos de múltiples nodos es anormal al mismo tiempo. Como resultado, es posible que algunas particiones no estén disponibles.

Causas posibles

- El permiso del directorio de datos está alterado.
- El disco donde se encuentra el directorio de datos está defectuoso.

Procedimiento

Verificar el permiso en el directorio de datos defectuoso.

Paso 1 Encuentre la información del host en la información de alarma e inicie sesión en el host.

Paso 2 En la información de alarma, compruebe si el directorio de datos y sus subdirectorios pertenecen al grupo omm:wheel.

- En caso afirmativo, registre el nombre de host del nodo y vaya a **Paso 4**.
- Si no, vaya a **Paso 3**.

Paso 3 Restaurar el grupo propietario del directorio de datos y sus subdirectorios a omm:wheel.

- En caso afirmativo, vaya a **Paso 6**.
- Si no, vaya a **Paso 5**.

Comprobar si el disco donde se encuentra el directorio de datos está defectuoso.

Paso 4 En el directorio de nivel superior del directorio de datos, cree y elimine archivos como usuario **omm**. Compruebe si la lectura/escritura de datos en el disco es normal.

Paso 5 Reemplace o repare el disco donde se encuentra el directorio de datos para asegurarse de que la lectura/escritura de datos en el disco sea normal.

Paso 6 En la página principal del FusionInsight Manager, elija **Cluster** > *Name of the desired cluster* > **Services** > **Kafka** > **Instance**. En la página de instancia de Kafka que se muestra, reinicie la instancia del Broker en el host registrado en **Paso 2**.

Paso 7 Una vez iniciado el Broker, compruebe si la alarma está desactivada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 8**.

Recopilar información de fallas.

Paso 8 En FusionInsight Manager, elija **O&M** > **Log** > **Download**.

Paso 9 En el área **Service** , seleccione **Kafka** en el clúster requerido.

Paso 10 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 11 Póngase en contacto con el y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.215 ALM-38009 E/S ocupado de disco de Broker (Aplicable a versiones posteriores a MRS 3.1.0)

NOTA

Esta sección se aplica a las versiones posteriores a MRS 3.1.0.

Descripción

El sistema comprueba el estado de E/S de cada disco de Kafka cada 60 segundos. Esta alarma se genera cuando la E/S de disco de un directorio de datos de Kafka en un broker supera el umbral (80% por defecto).

Su **Trigger Count** es **3**. Esta alarma se borra cuando la E/S del disco es inferior al umbral (80% por defecto).

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
38009	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
DataDirectoryName	Especifica el nombre del directorio de datos de Kafka con E/S de disco frecuentes.

Impacto en el sistema

La partición de disco tiene E/S frecuentes. Es posible que los datos no se escriban en el topic de Kafka para el que se genera la alarma.

Causas posibles

- Hay muchas réplicas configuradas para el topic.
- El parámetro para los mensajes del productor de escritura por lotes está configurado de forma inadecuada. El tráfico de servicio de este tema es demasiado pesado y la configuración de Partition actual no es apropiada.

Procedimiento

Comprobar el número de réplicas de topic.

Paso 1 En FusionInsight Manager, seleccione **O&M** > **Alarm** > **Alarms**. Busque la fila que contiene esta alarma, haga clic en ⌄ y vea el nombre de host de **Location**.

Paso 2 En FusionInsight Manager, elija **Cluster**, haga clic en el nombre del clúster deseado, elija **Services** > **Kafka** > **KafkaTopic Monitor**, busque el tema para el que se genera la alarma y compruebe el número de réplicas.

Paso 3 Reduzca los factores de replicación del topic (por ejemplo, reducir a **3**) si el número de réplicas es mayor que 3.

Ejecute el siguiente comando en el cliente de FusionInsight para volver a planificar las réplicas de los topics de Kafka:

kafka-reassign-partitions.sh --zookeeper *{zk_host}:{port}*/**kafka --reassignment-json-file** *{manual assignment json file path}* **--execute**

Por ejemplo:

/opt/client/Kafka/kafka/bin/kafka-reassign-partitions.sh --zookeeper 10.149.0.90:2181,10.149.0.91:2181,10.149.0.92:2181/kafka --reassignment-json-file expand-cluster-reassignment.json --execute

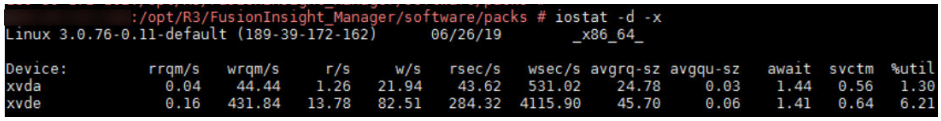
> **NOTA**
>
> En el archivo **expand-cluster-reassignment.json**, describa los brokers a los que se migran las Partitions del Topic en el siguiente formato: {"partitions":[{"topic": "*topicName*","partition": 1,"replicas": [1,2,3] }],"version":1}

Paso 4 Observe durante un período de tiempo y compruebe si la alarma está desactivada. Si la alarma persiste, vaya a **Paso 5**.

Comprobar el plan de Partition de Topic.

Paso 5 En la página **KafkaTopic Monitor**, vea **Topic Input Traffic** en el área **Topic Traffic** de cada Topic, obtenga el Topic con el mayor valor y compruebe Partition de este Topic, así como la información sobre el host de estas Partitions.

Paso 6 Inicie sesión en el host consultado en **Paso 5** y ejecute el comando **iostat -d -x** para comprobar el valor **%util** de cada disco.

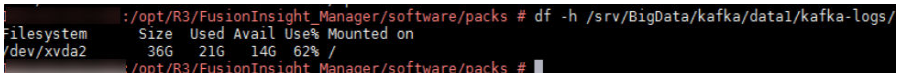


- Si el valor **%util** de cada disco excede el umbral (**80%** predeterminado), expanda la capacidad del disco de Kafka. Después de la ampliación de capacidad, vuelva a planificar las particiones del tema haciendo referencia a **Paso 3**.
- Si los valores **%util** de los discos varían mucho, compruebe la configuración de la partición de disco de Kafka. Por ejemplo, compruebe el valor de **log.dirs** en el archivo **${BIGDATA_HOME}/FusionInsight_HD_/1_14_Broker/etc/server.properties**.

  Ejecute el siguiente comando para ver la información **Filesystem**:

  df -h *log.dirs value*

  El resultado del comando es el siguiente.

- Si la partición donde se encuentra el sistema de archivos coincide con la partición con un valor **%util** alto, planifique particiones de Kafka en discos inactivos, configure **log.dirs** como un directorio de disco inactivo y vuelva a planificar Partition de Topic haciendo referencia a **Paso 3**. Asegúrese de que Partition de topic estén distribuidas uniformemente en cada disco.

Paso 7 Observe durante un período de tiempo y compruebe si la alarma está desactivada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, repita **Paso 5** a **Paso 6** tres veces. A continuación, vaya a **Paso 8**.

Paso 8 Observe durante un período de tiempo y compruebe si la alarma está desactivada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 9**.

Recopilar información de fallas.

Paso 9 En FusionInsight Manager, seleccione **O&M**. En el panel de navegación de la izquierda, elija **Log** > **Download**.

Paso 10 Expanda la lista desplegable **Service** y seleccione **Kafka** para el clúster de destino.

Paso 11 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 12 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

Información relacionada

Ninguna

9.216 ALM-38009 Sobrecarga de Kafka Topic (aplicable a MRS 3.1.0 y versiones anteriores)

NOTA

Esta sección se aplica a MRS 3.1.0 o anterior.

Descripción

El sistema comprueba el estado de sobrecarga de cada topic de Kafka cada 60 segundos. Esta alarma se genera cuando el porcentaje de particiones de un topic en el disco sobrecargado excede el umbral (40% de forma predeterminada).

Su **Trigger Count** es **1**. Esta alarma se borra cuando el porcentaje de particiones de un topic en el disco sobrecargado es inferior al umbral (40% de forma predeterminada).

Un disco sobrecargado se refiere al disco cuyo uso de E/S de una partición de disco es superior al 80%.

Por ejemplo:

Las particiones del Topic A se distribuyen en tres brokers. Los usos de E/S de las particiones de disco en dos brokers son superiores al 80%.

El porcentaje de particiones en el disco sobrecargado es 2/3, mayor que 40%, se genera esta alarma.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
38009	Grave	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
TopicName	Especifica el tema Kafka para el que se genera la alarma.

Impacto en el sistema

La partición de disco tiene E/S frecuentes. Es posible que los datos no se escriban en el topic de Kafka para el que se genera la alarma.

Causas posibles

- Hay muchas réplicas configuradas para el topic.
- El parámetro para los mensajes del productor de escritura por lotes está configurado de forma inadecuada. El tráfico de servicio de este tema es demasiado pesado y la configuración de Partition actual no es apropiada.

Procedimiento

Comprobar el número de réplicas de topic.

Paso 1 En FusionInsight Manager, seleccione **O&M** > **Alarm** > **Alarms**. Busque la fila que contiene esta alarma, haga clic en ⌄ y vea el nombre de host de **Location**.

Paso 2 En FusionInsight Manager, elija **Cluster**, haga clic en el nombre del clúster deseado, elija **Services** > **Kafka** > **KafkaTopic Monitor**, busque el tema para el que se genera la alarma y compruebe el número de réplicas.

Paso 3 Reduzca los factores de replicación del topic (por ejemplo, reducir a **3**) si el número de réplicas es mayor que 3.

Ejecute el siguiente comando en el cliente de FusionInsight para volver a planificar las réplicas de los topics de Kafka:

kafka-reassign-partitions.sh --zookeeper *{zk_host}:{port}*/**kafka --reassignment-json-file** *{manual assignment json file path}* **--execute**

Por ejemplo:

/opt/client/Kafka/kafka/bin/kafka-reassign-partitions.sh --zookeeper 10.149.0.90:2181,10.149.0.91:2181,10.149.0.92:2181/kafka --reassignment-json-file expand-cluster-reassignment.json --execute

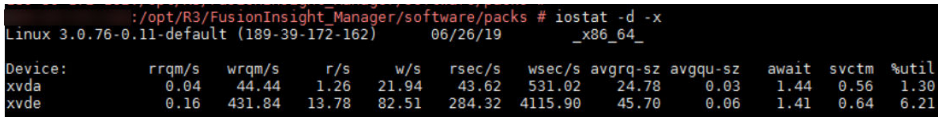
> **NOTA**
>
> En el archivo **expand-cluster-reassignment.json**, describa los brokers a los que se migran las Partitions del Topic en el siguiente formato: {"partitions":[{"topic": "*topicName*","partition": 1,"replicas": [1,2,3] }],"version":1}

Paso 4 Observe durante un período de tiempo y compruebe si la alarma está desactivada. Si la alarma persiste, vaya a **Paso 5**.

Comprobar el plan de Partition de Topic.

Paso 5 En la página **KafkaTopic Monitor**, vea **Topic Input Traffic** en el área **Topic Traffic** de cada Topic, obtenga el Topic con el mayor valor y compruebe Partition de este Topic, así como la información sobre el host de estas Partitions.

Paso 6 Inicie sesión en el host consultado en **Paso 5** y ejecute el comando **iostat -d -x** para comprobar el valor **%util** de cada disco.

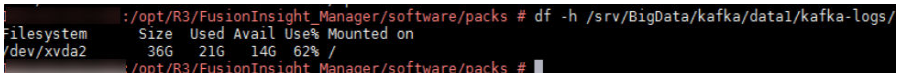


- Si el valor **%util** de cada disco excede el umbral (**80%** predeterminado), expanda la capacidad del disco de Kafka. Después de la ampliación de capacidad, vuelva a planificar las particiones del tema haciendo referencia a **Paso 3**.
- Si los valores **%util** de los discos varían mucho, compruebe la configuración de la partición de disco de Kafka. Por ejemplo, compruebe el valor de **log.dirs** en el archivo **${BIGDATA_HOME}/FusionInsight_HD_/1_14_Broker/etc/server.properties**.

  Ejecute el siguiente comando para ver la información **Filesystem**:

  df -h *log.dirs value*

  El resultado del comando es el siguiente.

- Si la partición donde se encuentra el sistema de archivos coincide con la partición con un valor **%util** alto, planifique particiones de Kafka en discos inactivos, configure **log.dirs** como un directorio de disco inactivo y vuelva a planificar Partition de Topic haciendo referencia a **Paso 3**. Asegúrese de que Partition de topic estén distribuidas uniformemente en cada disco.

Paso 7 Observe durante un período de tiempo y compruebe si la alarma está desactivada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, repita **Paso 5** a **Paso 6** tres veces. A continuación, vaya a **Paso 8**.

Paso 8 Observe durante un período de tiempo y compruebe si la alarma está desactivada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 9**.

Recopilar información de fallas.

Paso 9 En FusionInsight Manager, seleccione **O&M**. En el panel de navegación de la izquierda, elija **Log** > **Download**.

Paso 10 Expanda la lista desplegable **Service** y seleccione **Kafka** para el clúster de destino.

Paso 11 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 12 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

Información relacionada

Ninguna

9.217 ALM-38010 Topics con réplica única

Descripción

El sistema comprueba el número de réplicas de cada topic cada 60 segundos en el nodo donde reside el Controller de Kafka. Esta alarma se genera cuando hay una réplica para un topic.

Atributo

ID de alarma	Gravedad de la alarma	Borrado automáticamente
38010	Advertencia	No

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
TopicName	Especifica la lista de topics para los que se genera la alarma.

Impacto en el sistema

Existe el riesgo de punto único de falla (SPOF) para los temas con una sola réplica. Cuando el nodo donde reside la réplica se vuelve anormal, el partition no tiene un leader y los servicios del topic se ven afectados.

Causas posibles

- El número de réplicas del topic está configurado incorrectamente.

Procedimiento

Comprobar el número de réplicas para el topic.

Paso 1 En FusionInsight Manager, seleccione **O&M** > **Alarm** > **Alarms**, haga clic en ⌄ de esta alarma y vea la lista **TopicName** en **Location**.

Paso 2 Compruebe si es necesario agregar réplicas para el topic para el que se genera la alarma.

- En caso afirmativo, vaya a **Paso 3**.
- Si no, vaya a **Paso 5**.

Paso 3 En el cliente de FusionInsight, vuelva a planificar las réplicas de topic y describa la distribución de particiones del topic en el archivo **add-replicas-reassignment.json** con el siguiente formato: {"partitions":[{"topic": "*topic name*","partition": 1,"replicas": [1,2] }],"version":1}. A continuación, ejecute el siguiente comando para agregar réplicas:

kafka-reassign-partitions.sh --zookeeper *{zk_host}:{port}*/**kafka --reassignment-json-file** *{manual assignment json file path}* **--execute**

Por ejemplo:

/opt/client/Kafka/kafka/bin/kafka-reassign-partitions.sh --zookeeper 192.168.0.90:2181,192.168.0.91:2181,192.168.0.92:2181/kafka --reassignment-json-file add-replicas-reassignment.json --execute

Paso 4 Ejecute el siguiente comando para comprobar el progreso de la ejecución de la tarea:

kafka-reassign-partitions.sh --zookeeper *{zk_host}:{port}*/**kafka --reassignment-json-file** *{manual assignment json file path}* **--verify**

Por ejemplo:

/opt/client/Kafka/kafka/bin/kafka-reassign-partitions.sh --zookeeper 192.168.0.90:2181,192.168.0.91:2181,192.168.0.92:2181/kafka --reassignment-json-file add-replicas-reassignment.json --verify

Paso 5 Después de completar las operaciones de manejo o de confirmar que la alarma no tiene impacto, borre manualmente la alarma en FusionInsight Manager.

Paso 6 Después de un período de tiempo, compruebe si la alarma está desactivada.

- Si lo es, no se requiere ninguna otra acción.
- Si no es así, vaya a **Paso 7**.

Recopilar información de fallas.

Paso 7 En FusionInsight Manager, elija **O&M** > **Log** > **Download**.

Paso 8 En el área **Service** , seleccione **Kafka** en el clúster requerido.

Paso 9 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 10 Póngase en contacto con el y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Si la alarma no tiene impacto, borre la alarma manualmente.

Información relacionada

Ninguna

9.218 ALM-38011 El uso de conexión de usuario en el Broker supera el umbral

Descripción

El sistema comprueba el número de conexiones de cada usuario en Broker cada 30 segundos. Esta alarma se genera cuando el uso de conexión de un usuario en el Broker excede el umbral (80% por defecto) durante 5 veces consecutivas.

El número de veces que se realiza el suavizado es de **5**. Esta alarma se borra cuando el uso de conexión de un usuario en el Broker es menor que el umbral.

La alarma se puede borrar automáticamente. Sin embargo, si el número de conexiones de un usuario se convierte repentinamente en **0** y no se crea ninguna conexión, la alarma no se puede borrar automáticamente. Necesita borrarlo manualmente.

Atributo

ID de alarma	Gravedad de la alarma	Borrado automáticamente
38011	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.

Nombre	Significado
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
UserName	Especifica el nombre de usuario para el que se genera la alarma.

Impacto en el sistema

Si el número de conexiones de un usuario es excesivo, el usuario no puede crear nuevas conexiones al Broker.

Causas posibles

- El número de conexiones (creadas por un usuario) utilizadas por el cliente excede el umbral preestablecido.
- El umbral para el uso de la conexión no cumple con los requisitos de servicio.

Procedimiento

Comprobar el número de conexiones establecidas por un mismo usuario en el cliente.

Paso 1 En la página de inicio del FusionInsight Manager, elija **O&M** > **Alarm** > **Alarms** > **User Connection Usage on Broker Exceeds the Threshold**. Compruebe el nombre de host y el nombre de usuario de la instancia de Broker para la que se genera la alarma en el **Location**.

Paso 2 En la página principal del FusionInsight Manager, elija **Cluster** > *Name of the desired cluster* > **Services** > **Kafka** > **Instance**. Haga clic en la instancia para la que se genera la alarma para ir a la página de la instancia. Haga clic en la lista desplegable en la esquina superior derecha del área del gráfico, elija **Customize > Other**, y seleccione **User Connection Usage on Broker**, **Maximum Number of User Connections on Broker**, y **Number of User Connections on Broker** para ver el número de conexiones de usuario actuales en el Broker.

Paso 3 Observe el número de conexiones en tiempo real del usuario de alarma actual y compruebe si existen los datos de monitorización en tiempo real del usuario actual.

- En caso afirmativo, vaya a **Paso 4**.
- Si no, el usuario actual ha desconectado todas las conexiones. Es necesario borrar la alarma manualmente, y no se requiere ninguna acción adicional.

  NOTA

  Después de que el usuario de alarma desconecta todas las conexiones, los datos de monitorización del usuario desaparecen. En este caso, la alarma no se borrará automáticamente. Necesita borrarlo manualmente.

Paso 4 Compruebe si el usuario está autorizado por el lado del servicio.

En caso afirmativo, vaya a **Paso 7**.

Si no, vaya a **Paso 5**.

Paso 5 Ejecute el siguiente comando en el cliente para limitar el número de conexiones del usuario. Hay dos reglas de configuración basadas en los siguientes comandos:

1. Para el Broker y el usuario específicos, ejecute el siguiente comando:

   kafka-configs.sh --bootstrap-server <*broker ip:port*> **--alter --add-config 'max.connections.per.user.overrides=[**<*username*>**:**<*connection.number*>**]' --entity-type brokers --entity-name** <*broker.id*> **--command-config Kafka/kafka/config/producer.properties**

   NOTA

   Para usuarios no autorizados, confirme con el lado del servicio para reducir el número máximo de conexiones de un usuario no autorizado o establezca el número máximo de conexiones a **0**.

   En el comando, debe especificar la dirección IP y el número de puerto del Broker, establecer los valores de los elementos de configuración y especificar **brokerId** y **username**. En este caso, el usuario se refiere al usuario autorizado de Kerberos.

   La configuración actualizada mediante la herramienta de línea de comandos puede tener efecto dinámicamente. La configuración no es válida después de reiniciar el servicio. Para que la configuración surta efecto después del reinicio, elija **Cluster** > *Name of the desired cluster* > **Services** > **Kafka** > **Configurations** > **All Configurations**> **Broker** > **Server** en la página de inicio de FusionInsight Manager y actualice la configuración a **max.connections.per.user.overrides**.

2. Para el uso específico y el Broker predeterminado (es decir, todas las instancias del Broker en el clúster), ejecute el siguiente comando:

   kafka-configs.sh --bootstrap-server <*broker ip:port*> **--alter --add-config 'max.connections.per.user.overrides=[**<*username*>**:**<*connection.number*>**]' --entity-type brokers ---entity-default --command-config Kafka/kafka/config/client.properties**

   Ejemplo:

   kafka-configs.sh --bootstrap-server 10.153.3.26:21007 --alter --add-config 'max.connections.per.user.overrides=[showcase:4]' --entity-type brokers --entity-name 1 --command-config Kafka/kafka/config/client.properties

Paso 6 Comprueba si el número máximo de conexiones es de **0** y si el número de conexiones del usuario actual disminuye o permanece inalterado según **Paso 2**.

- En caso afirmativo, borre manualmente la alarma y no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 7**.

Paso 7 Compruebe si el número de conexiones en tiempo real y el uso de la conexión del usuario actual aumentan drásticamente cuando se comparan con los datos históricos, y si han excedido el número máximo especificado de conexiones.

- En caso afirmativo, vaya a **Paso 8**.
- Si no, vaya a **Paso 9**.

NOTA

Si hay un aumento obvio después de la comparación y el número máximo de conexiones ha alcanzado el valor preestablecido, las conexiones del usuario pueden ser anormales. Es necesario confirmarlo con la parte de servicio.

Comprobar si el número de conexiones de usuario cumple con los requisitos del servicio.

Paso 8 Compruebe si el número de conexiones del usuario cumple con los requisitos de servicio.

- En caso afirmativo, vaya a **Paso 9**.
- En caso negativo, póngase en contacto con la parte de servicio para rectificar la falla.

NOTA

Si el número de conexiones de usuario es anormal, póngase en contacto con la parte de servicio para rectificar la falla de los siguientes aspectos:

- Compruebe si se agregan nuevos servicios para que el número de conexiones de usuario aumente considerablemente.
- Compruebe si se producen fugas en el mango en el código del lado de servicio.

Paso 9 Considere si se debe aumentar el número máximo de conexiones del usuario.

- En caso afirmativo, vaya a **Paso 10**.
- Si no, vaya a **Paso 12**.

Paso 10 Aumente el número máximo de conexiones en función de los requisitos de servicio. Establezca el número de conexiones del usuario en el cliente Kafka. Para obtener más información, consulte **Paso 5**.

Paso 11 Espere varios minutos y luego compruebe si la alarma se borra automáticamente.

- En caso afirmativo, vaya a **Paso 12**.
- Si no, vaya a **Paso 2**.

Paso 12 Determine si desea agregar el usuario a la lista blanca en función de los requisitos de servicio del lado del servicio.

- En caso afirmativo, vaya a **Paso 13**.
- Si no, vaya a **Paso 15**.

NOTA

Para agregar un usuario a la lista blanca, debe reiniciar el servicio Kafka. Sin embargo, esta operación causará una interrupción del servicio y afectará al funcionamiento del servicio. Por lo tanto, debe confirmar con el lado de servicio antes de realizar esta operación.

Paso 13 En la página principal del FusionInsight Manager, elija **Cluster** > *Name of the desired cluster* > **Services** > **Kafka** > **Configurations** > **All Configurations** > **Broker(Role)** > **Server** a agregar el usuario al elemento de configuración **max.connections.per.user.whitelist**.

Paso 14 Reinicie el servicio para que la modificación surta efecto. Además, es necesario borrar manualmente la alarma, y no s e requiere ninguna acción adicional.

Recopilar información de fallas.

Paso 15 En la página de inicio del FusionInsight Manager, seleccione **O&M** > **Log** > **Download**.

Paso 16 Expanda la lista desplegable **Service** y seleccione **Kafka** para el clúster de destino.

Paso 17 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 18 Póngase en contacto con el y envíe los registros de fallas recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.219 ALM-43001 Servicio Spark2x no disponible

Descripción

El sistema comprueba el estado del servicio Spark2x cada 300 segundos. Esta alarma se genera cuando el servicio Spark2x no está disponible.

Esta alarma se borra cuando se recupera el servicio Spark2x.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
43001	Crítica	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

Las tareas de Spark enviadas por los usuarios no se pueden ejecutar.

Causas posibles

- El servicio KrbServer es anormal.
- El servicio LdapServer es anormal.
- ZooKeeper es anormal.
- HDFS es anormal.
- Yarn es anormal.
- El servicio Hive correspondiente es anormal.

- El paquete de ensamblaje de Spark2x es anormal.

Procedimiento

Si la alarma es un paquete de ensamblaje de Spark2x anormal, el paquete Spark es anormal. Espera unos 10 minutos. La alarma se borra automáticamente.

Comprobar si existen alarmas de indisponibilidad del servicio en los servicios de los que depende.

Paso 1 En FusionInsight Manager, seleccione **O&M**. En el panel de navegación de la izquierda, elija **Alarm** > **Alarms**.

Paso 2 Compruebe si existen las siguientes alarmas en la lista de alarmas:

- ALM-25500 Servicio KrbServer no disponible
- ALM-25000 Servicio LdapServer no disponible
- ALM-13000 Servicio ZooKeeper no disponible
- ALM-14000 Servicio HDFS no disponible
- ALM-18000 Servicio de Yarn no disponible
- ALM-16004 Servicio Hive no disponible
- En caso afirmativo, vaya a **Paso 3**.
- Si no, vaya a **Paso 4**.

Paso 3 Manejar las alarmas basándose en los métodos de solución de problemas proporcionados en la ayuda de alarma.

Después de que se desactive la alarma, espere unos minutos y compruebe si la alarma GuardianService no disponible está despejado.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 4**.

Recopilar información de fallas.

Paso 4 En FusionInsight Manager, elija **O&M** > **Log** > **Download**.

Paso 5 En el área **Service**, seleccione los siguientes nodos del clúster deseado. (Hive es el servicio específico de Hive determinado basado en el **ServiceName** en la información de ubicación de la alarma).

- KrbServer
- LdapServer
- ZooKeeper
- HDFS
- Yarn
- Hive

Paso 6 Haga clic en  en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 7 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

Información relacionada

Ninguna

9.220 ALM-43006 El uso de memoria heap del proceso JobHistory2x supera el umbral

Descripción

El sistema comprueba el estado del proceso JobHistory2x cada 30 segundos. La alarma se genera cuando el uso de memoria heap de un proceso JobHistory2x excede el umbral (95% de la memoria máxima).

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
43006	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el nombre del servicio para el que se genera la alarma.
RoleName	Especifica el nombre del rol para el que se genera la alarma.
HostName	Especifica el objeto (ID de host) para el que se genera la alarma.
Trigger Condition	Especifica el umbral que activa la alarma. Si el valor del indicador actual excede este umbral, se genera la alarma.

Impacto en el sistema

Si la memoria heap de procesos de JobHistory2x disponible es insuficiente, se produce un desbordamiento de memoria y el servicio se interrumpe.

Causas posibles

La memoria no heap del proceso de JobHistory2x se utiliza en exceso o la memoria heap se asigna de forma inadecuada.

Procedimiento

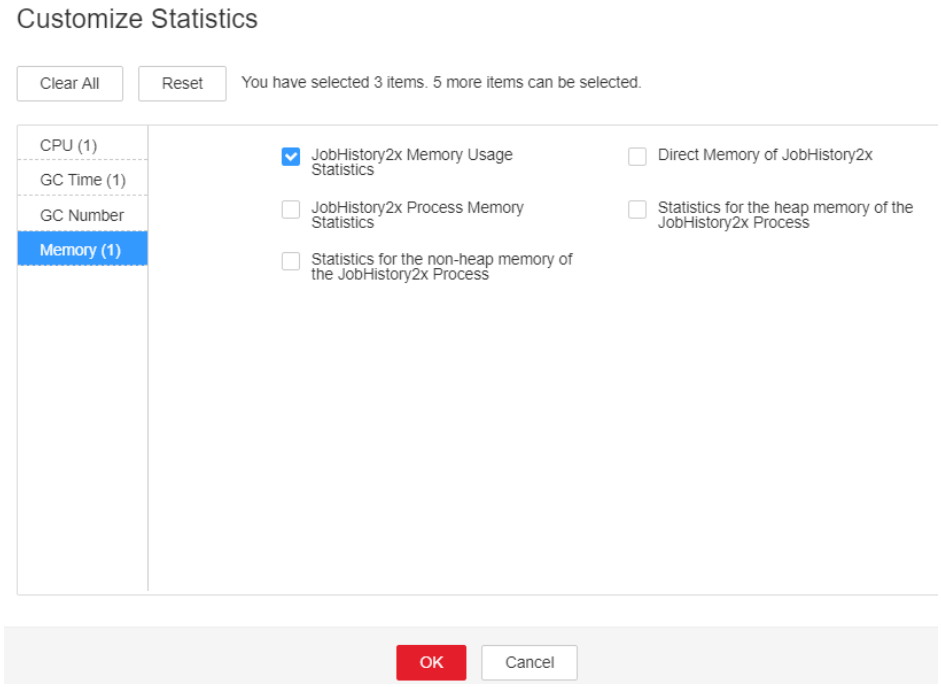
Comprobar el uso de memoria heap.

Paso 1 En el portal del Administrador FusionInsight, seleccione **O&M > Alarm > Alarms** y elija la alarma cuyo **ID** es **43006**. Compruebe el **RoleName** en **Location** y confirme la dirección IP de **HostName**.

Paso 2 En el portal del Administrador FusionInsight, elija **Cluster >** *Name of the desired cluster* **> Services** > **Spark2x** > **Instance** y haga clic en JobHistory2x para el que se genera la alarma para ir a la página **Dashboard**. Haga clic en el menú desplegable en el área Chart y elija **Customize** > **Memory > JobHistory2x Memory Usage Statistics** en el cuadro de lista desplegable en la esquina superior derecha y haga clic en **OK**. Compruebe si la memoria heap utilizada del proceso de JobHistory2x alcanza el umbral (el valor predeterminado es 95%) de la memoria heap máxima especificada para JobHistory2x.

- En caso afirmativo, vaya a **Paso 3**.
- Si no, vaya a **Paso 7**.

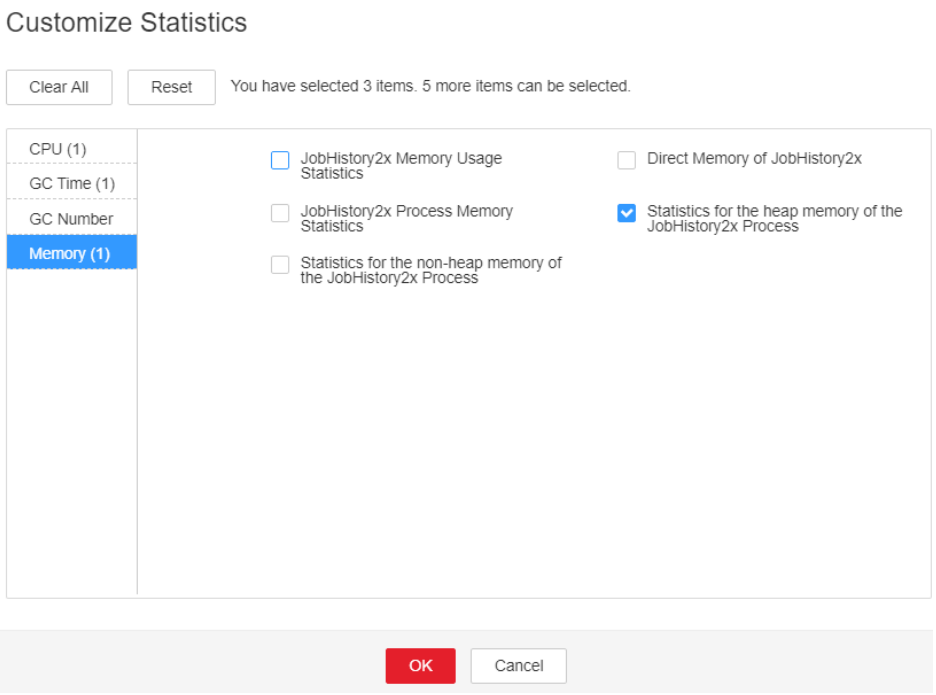
Figura 9-83 Estadísticas de uso de memoria de JobHistory2x



Paso 3 En la página de inicio del FusionInsight Manager, seleccione **Cluster** > *Name of the desired cluster* > **Services** > **Spark2x** > **Instance**. Haga clic en **JobHistory2x** por la que se informa que la alarma va a la página **Dashboard**, haga clic en la lista desplegable en la esquina

superior derecha del área del gráfico, elija **Customize** > **Memory > Statistics for the heap memory of the JobHistory2x Process** y haga clic en **OK**. Con base en el tiempo de generación de alarma, compruebe los valores de la memoria heap utilizada del proceso de JobHistory2x en el período correspondiente y obtenga el valor máximo.

Figura 9-84 Estadísticas para la memoria heap del proceso de JobHistory2x



Paso 4 En el portal de FusionInsight Manager, elija **Cluster >** *Name of the desired cluster* **> Services** > **Spark2x** > **Configurations** y haga clic en **All Configurations**. Elija **JobHistory2x** > **Default**. El valor predeterminado de **SPARK_DAEMON_MEMORY** es 4GB. Puede cambiar el valor de acuerdo con las siguientes reglas: Relación entre el uso máximo de memoria de pila de JobHistory2x y el **Threshold** del **JobHistory2x Heap Memory Usage Statistics (JobHistory2x)** en el período de alarma. Si esta alarma se genera ocasionalmente después de ajustar el valor del parámetro, aumente el valor en 0.5 veces. Si la alarma se notifica con frecuencia después de ajustar el valor del parámetro, aumente el valor en 1 vez.

NOTA

En la página de inicio del Administrador FusionInsight, elija **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster* **> Spark2x** > **Memory** >**JobHistory2x Heap Memory Usage Statistics (JobHistory2x)** para ver **Threshold**.

Paso 5 Reinicie todas las instancias de JobHistory2x.

Paso 6 Después de 10 minutos, compruebe si la alarma está borrada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 7**.

Recopilar información de fallas.

Paso 7 En el portal del FusionInsight Manager, elija **O&M** > **Log > Download**.

Paso 8 Seleccione **Spark2x** en el clúster requerido en el **Service**.

Paso 9 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 10 Póngase en contacto con el y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.221 ALM-43007 El uso de memoria no heap del proceso JobHistory2x supera el umbral

Descripción

El sistema comprueba el estado del proceso JobHistory2x cada 30 segundos. La alarma se genera cuando el uso de memoria sin pila de un proceso JobHistory2x excede el umbral (95% de la memoria máxima).

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
43007	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el nombre del servicio para el que se genera la alarma.
RoleName	Especifica el nombre del rol para el que se genera la alarma.
HostName	Especifica el objeto (ID de host) para el que se genera la alarma.
Trigger Condition	Especifica el umbral que activa la alarma. Si el valor del indicador actual excede este umbral, se genera la alarma.

Impacto en el sistema

Si la memoria no heap de JobHistory2x Process disponible es insuficiente, se produce un desbordamiento de memoria y el servicio se rompe.

Causas posibles

La memoria no heap del proceso JobHistory2x se utiliza en exceso o la memoria no heap se asigna de forma inadecuada.

Procedimiento

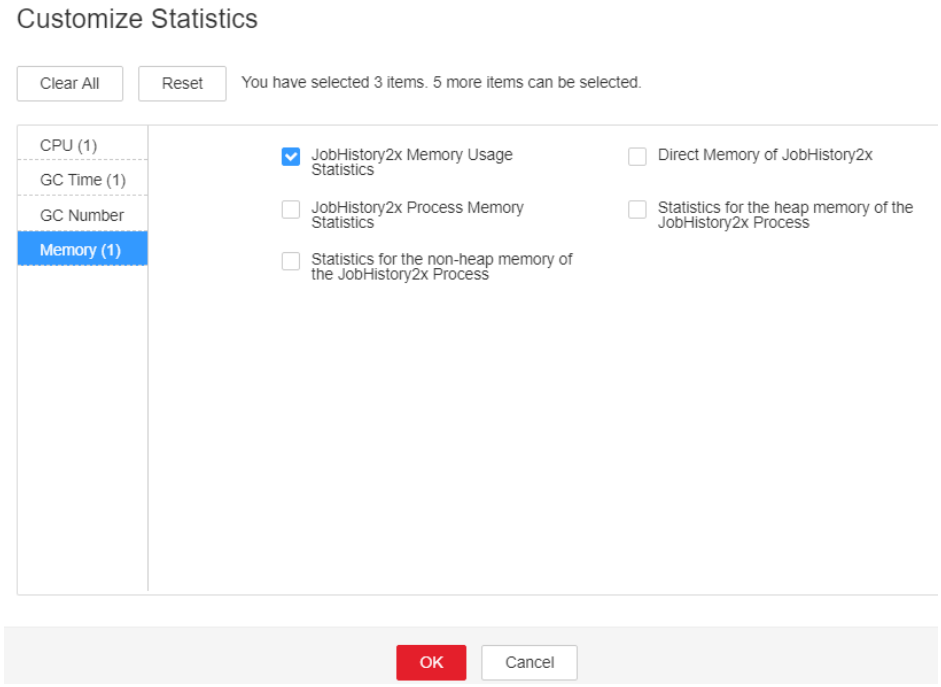
Verificar el uso de memoria no heap.

Paso 1 En el portal del FusionInsight Manager, seleccione **O&M > Alarm > Alarms** and select the alarm whose **ID** is **43007**. Compruebe el **RoleName** en **Location** y confirme la dirección IP de **HostName**.

Paso 2 En el portal del Administrador FusionInsight, elija **Cluster >** *Name of the desired cluster* **> Services** > **Spark2x** > **Instance** y haga clic en JobHistory2x para el que se genera la alarma para ir a la página **Dashboard**. Haga clic en el menú desplegable en el área Gráfico y elija **Customize** > **Memory** > **JobHistory2x Memory Usage Statistics** en el cuadro de lista desplegable en la esquina superior derecha y haga clic en **OK**. Compruebe si la memoria no heap utilizada del proceso JobHistory2x alcanza el umbral (el valor predeterminado es 95%) de la memoria máxima no heap especificada para JobHistory2x.

- En caso afirmativo, vaya a **Paso 3**.
- Si no, vaya a **Paso 7**.

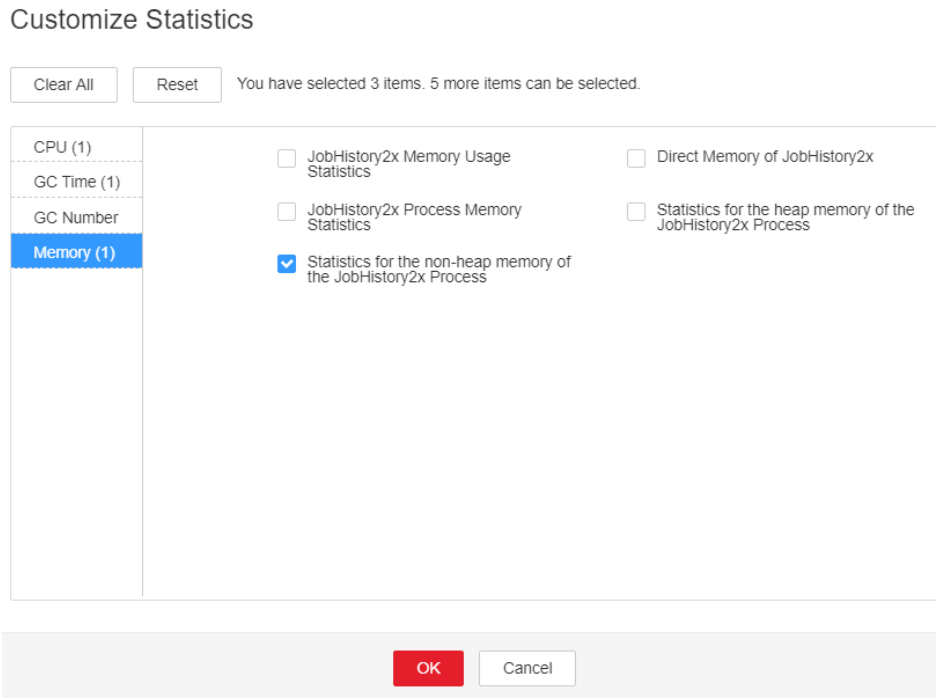
Figura 9-85 Estadísticas de uso de memoria de JobHistory2x



Paso 3 En la página de inicio del FusionInsight Manager, seleccione **Cluster** > *Name of the desired cluster* > **Services** > **Spark2x** > **Instance**. Haga clic en **JobHistory2x** por la que se informa que la alarma va a la página **Dashboard** y haga clic en la lista desplegable en la esquina

superior derecha del área del gráfico, elija **Customize** > **Memory > Statistics for the non-heap memory of the JobHistory2x Process** y haga clic en **OK**. Basado en el tiempo de generación de alarma, compruebe los valores de la memoria no heap utilizada del proceso JobHistory2x en el período correspondiente y obtenga el valor máximo.

Figura 9-86 Estadísticas para la memoria no heap del proceso JobHistory2x



Paso 4 En el portal de FusionInsight Manager, elija **Cluster >** *Name of the desired cluster* **> Services** > **Spark2x** > **Configurations** y haga clic en **All Configurations**. Elija **JobHistory2x** > **Default**. Puede cambiar el valor de **-XX:MaxMetaspaceSize** en **SPARK_DAEMON_JAVA_OPTS** de acuerdo con las siguientes reglas: Proporción del uso de memoria no heap de JobHistory2x con el umbral de estadísticas de uso de memoria no heap de **JobHistory2x Non-Heap Memory Usage Statistics (JobHistory2x)** en el período de alarma.

NOTA

En la página de inicio del FusionInsight Manager, elija **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster* **> Spark2x** > **Memory** >**JobHistory2x Non-Heap Memory Usage Statistics (JobHistory2x)** para ver **Threshold**.

Paso 5 Reinicie todas las instancias de JobHistory2x.

Paso 6 Después de 10 minutos, compruebe si la alarma está borrada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 7**.

Recopilar información de fallas.

Paso 7 En el portal del FusionInsight Manager, elija **O&M** > **Log > Download**.

Paso 8 Seleccione **Spark2x** en el clúster requerido en el **Service**.

Paso 9 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 10 Póngase en contacto con el y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.222 ALM-43008 El uso de memoria directa del proceso de JobHistory2x supera el umbral

Descripción

El sistema comprueba el estado del proceso JobHistory2x cada 30 segundos. La alarma se genera cuando el uso directo de memoria de un proceso de JobHistory2x excede el umbral (95% de la memoria máxima).

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
43008	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el nombre del servicio para el que se genera la alarma.
RoleName	Especifica el nombre del rol para el que se genera la alarma.
HostName	Especifica el objeto (ID de host) para el que se genera la alarma.
Trigger Condition	Especifica el umbral que activa la alarma. Si el valor del indicador actual excede este umbral, se genera la alarma.

Impacto en el sistema

Si la memoria directa de JobHistory2x Process disponible es insuficiente, se produce un desbordamiento de memoria y el servicio se interrumpe.

Causas posibles

La memoria directa del proceso de JobHistory2x se utiliza en exceso o la memoria directa se asigna de forma inapropiada.

Procedimiento

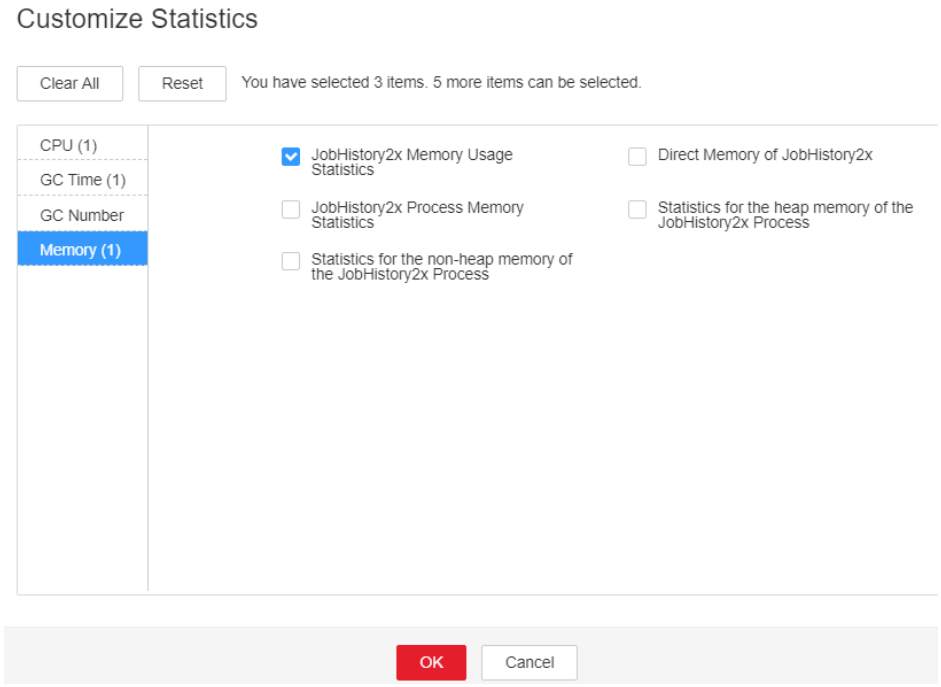
Comprobar el uso de memoria directa.

Paso 1 En el portal del Administrador FusionInsight, seleccione **O&M > Alarm > Alarms** y seleccione la alarma cuyo **ID** es **43008**. Compruebe el **RoleName** en **Location** y confirme la dirección IP de **HostName**.

Paso 2 En el portal del Administrador FusionInsight, elija **Cluster >** *Name of the desired cluster* **> Services** > **Spark2x** > **Instance** y haga clic en JobHistory2x para el que se genera la alarma para ir a la página **Dashboard**. Haga clic en el menú desplegable en el área Gráfico y elija **Customize** > **Memory** > **JobHistory2x Memory Usage Statistics** en el cuadro de lista desplegable en la esquina superior derecha y haga clic en **OK**. Compruebe si la memoria directa utilizada del proceso JobHistory2x alcanza el umbral (el valor predeterminado es 95%) de la memoria directa máxima especificada para JobHistory2x.

- En caso afirmativo, vaya a **Paso 3**.
- Si no, vaya a **Paso 7**.

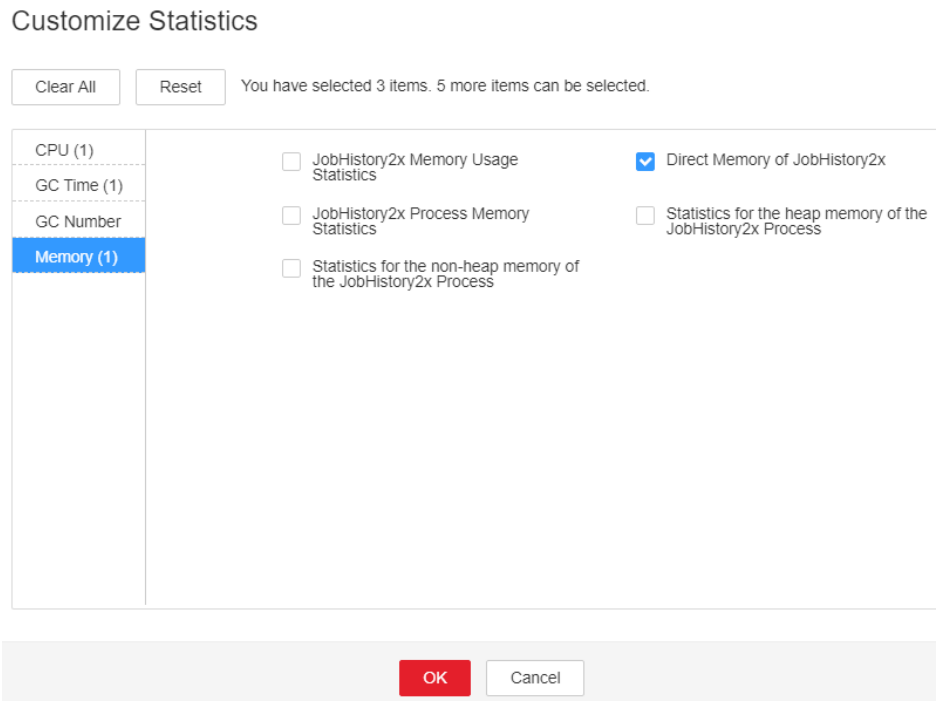
Figura 9-87 Estadísticas de uso de memoria de JobHistory2x



Paso 3 En la página de inicio del FusionInsight Manager, seleccione **Cluster** > *Name of the desired cluster* > **Services** > **Spark2x** > **Instance**. Haga clic en **JobHistory2x** por la que se informa que la alarma va a la página **Dashboard** y haga clic en la lista desplegable en la esquina

superior derecha del área del gráfico, elija **Customize** > **Memory > Direct Memory of JobHistory2x** y haga clic en **OK**. En base al tiempo de generación de alarma, compruebe los valores de la memoria directa utilizada del proceso JobHistory2x en el período correspondiente y obtenga el valor máximo.

Figura 9-88 Memoria directa del JobHistory2x



Paso 4 En el portal de FusionInsight Manager, elija **Cluster >** *Name of the desired cluster* **> Services** > **Spark2x** > **Configurations** y haga clic en **All Configurations**. Elija **JobHistory2x** > **Default**. El valor predeterminado de **-XX:MaxDirectMemorySize** en **SPARK_DAEMON_JAVA_OPTS** es de 512 MB. Puede cambiar el valor de acuerdo con las siguientes reglas: Relación entre el uso máximo de memoria directa del JobHistory2x y el **Threshold** del **JobHistory2x Direct Memory Usage Statistics (JobHistory2x)** en el período de alarma. Si esta alarma se genera ocasionalmente después de ajustar el valor del parámetro, aumente el valor en 0.5 veces. Si la alarma se notifica con frecuencia después de ajustar el valor del parámetro, aumente el valor en 1 vez. Se recomienda que el valor sea menor o igual que el valor de **SPARK_DAEMON_MEMORY**.

NOTA

En la página de inicio del Administrador FusionInsight, elija **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster* **> Spark2x** > **Memory** >**JobHistory2x Direct Memory Usage Statistics (JobHistory2x)** para ver **Threshold**.

Paso 5 Reinicie todas las instancias de JobHistory2x.

Paso 6 Después de 10 minutos, compruebe si la alarma está borrada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 7**.

Recopilar información de fallas.

Paso 7 En el portal del FusionInsight Manager, elija **O&M** > **Log > Download**.

Paso 8 Seleccione **Spark2x** en el clúster requerido en el **Service**.

Paso 9 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 10 Póngase en contacto con el y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.223 ALM-43009 Tiempo de GC de proceso de JobHistory2x excede el umbral

Descripción

El sistema comprueba el tiempo de recolección de basura (GC) del proceso JobHistory2x cada 60 segundos. Esta alarma se genera cuando el tiempo GC detectado excede el umbral (excede 5 segundos durante tres comprobaciones consecutivas). Para cambiar el umbral, elija **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster* > **Spark2x** > **GC Time** > **Total GC time in milliseconds (JobHistory2x)**. Esta alarma se borra cuando el tiempo de JobHistory2x GC es menor o igual que el umbral.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
43009	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el nombre del servicio para el que se genera la alarma.
RoleName	Especifica el nombre del rol para el que se genera la alarma.

Nombre	Significado
HostName	Especifica el objeto (ID de host) para el que se genera la alarma.
Trigger Condition	Especifica el umbral que activa la alarma. Si el valor del indicador actual excede este umbral, se genera la alarma.

Impacto en el sistema

Si el tiempo de GC excede el umbral, JobHistory2x puede ejecutarse con bajo rendimiento.

Causas posibles

La memoria de JobHistory2x se utiliza en exceso, la memoria heap se asigna de forma inapropiada. Como resultado, los GC ocurren con frecuencia.

Procedimiento

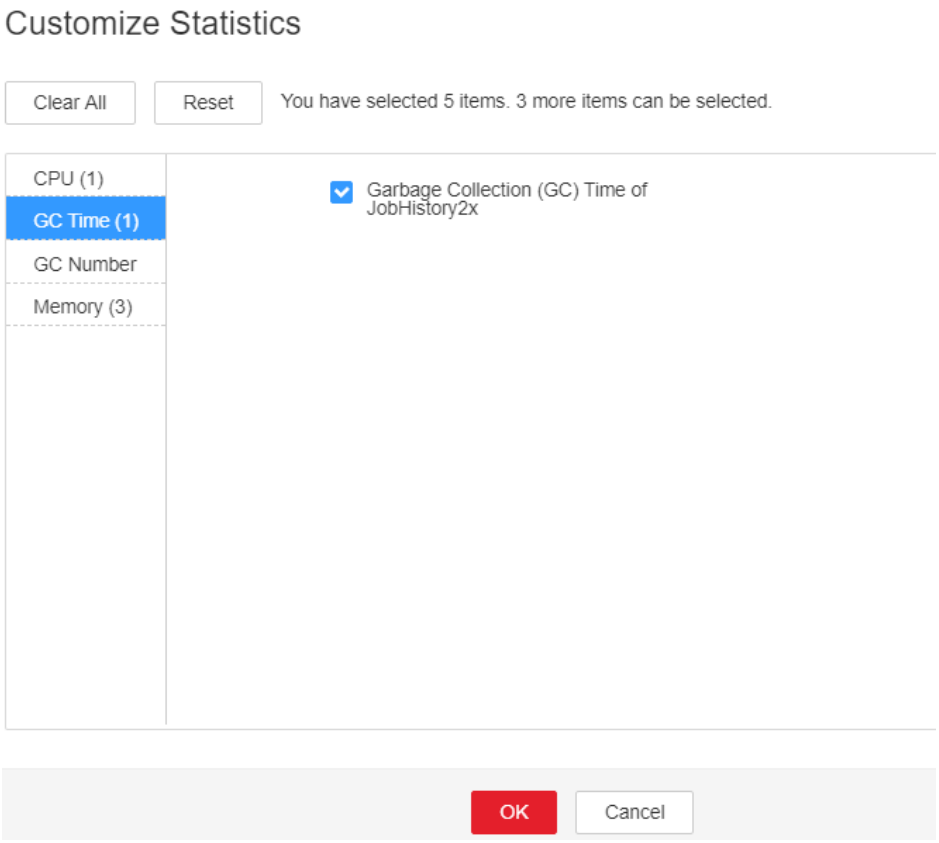
Comprobar el tiempo de GC.

Paso 1 En el portal del Administrador FusionInsight, seleccione **O&M > Alarm > Alarms** y seleccione la alarma cuyo **ID** es **43009**. Compruebe el **RoleName** en **Location** y confirme la dirección IP de **HostName**.

Paso 2 En el portal del Administrador FusionInsight, elija **Cluster >** *Name of the desired cluster* **> Services** > **Spark2x** > **Instance** y haga clic en JobHistory2x para el que se genera la alarma para ir a la página **Dashboard**. Haga clic en el menú desplegable en el área Chart y elija **Customize** > **GC Time** > **Garbage Collection (GC) Time of JobHistory2x** en el cuadro de lista desplegable en la esquina superior derecha y haga clic en **OK** para comprobar si el tiempo de GC es más largo que el umbral (valor predeterminado: 12 segundos).

- En caso afirmativo, vaya a **Paso 3**.
- Si no, vaya a **Paso 6**.

Figura 9-89 Tiempo de Recolección de basura (GC) de JobHistory2x



Paso 3 En el portal de FusionInsight Manager, elija **Cluster >** *Name of the desired cluster* **> Services > Spark2x > Configurations** y haga clic en **All Configurations**. Elija **JobHistory2x > Default**. El valor predeterminado de **SPARK_DAEMON_MEMORY** es 4 GB. Puede cambiar el valor de acuerdo con las siguientes reglas: Si esta alarma se genera ocasionalmente, aumente el valor en 0.5 veces. Si la alarma se informa con frecuencia, aumente el valor en 1 vez.

Paso 4 Reinicie todas las instancias de JobHistory2x.

Paso 5 Después de 10 minutos, compruebe si la alarma está borrada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 6**.

Recopilar información de fallas.

Paso 6 En la interfaz del FusionInsight Manager de los clústeres activos y en espera, seleccione **O&M > Log > Download**.

Paso 7 Seleccione **Spark2x** en el clúster requerido en el **Service**.

Paso 8 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 9 Póngase en contacto con el y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.224 ALM-43010 El uso de memoria heap del proceso JDBCServer2x supera el umbral

Descripción

El sistema comprueba el estado del proceso JDBCServer2x cada 30 segundos. La alarma se genera cuando el uso de memoria heap de un proceso JDBCServer2x excede el umbral (95% de la memoria máxima).

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
43010	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el nombre del servicio para el que se genera la alarma.
RoleName	Especifica el nombre del rol para el que se genera la alarma.
HostName	Especifica el objeto (ID de host) para el que se genera la alarma.
Trigger Condition	Especifica el umbral que activa la alarma. Si el valor del indicador actual excede este umbral, se genera la alarma.

Impacto en el sistema

Si la memoria heap de procesos JDBCServer2x disponible es insuficiente, se produce un desbordamiento de memoria y el servicio se interrumpe.

Causas posibles

La memoria heap del proceso JDBCServer2x se utiliza en exceso o la memoria heap se asigna de forma inadecuada.

Procedimiento

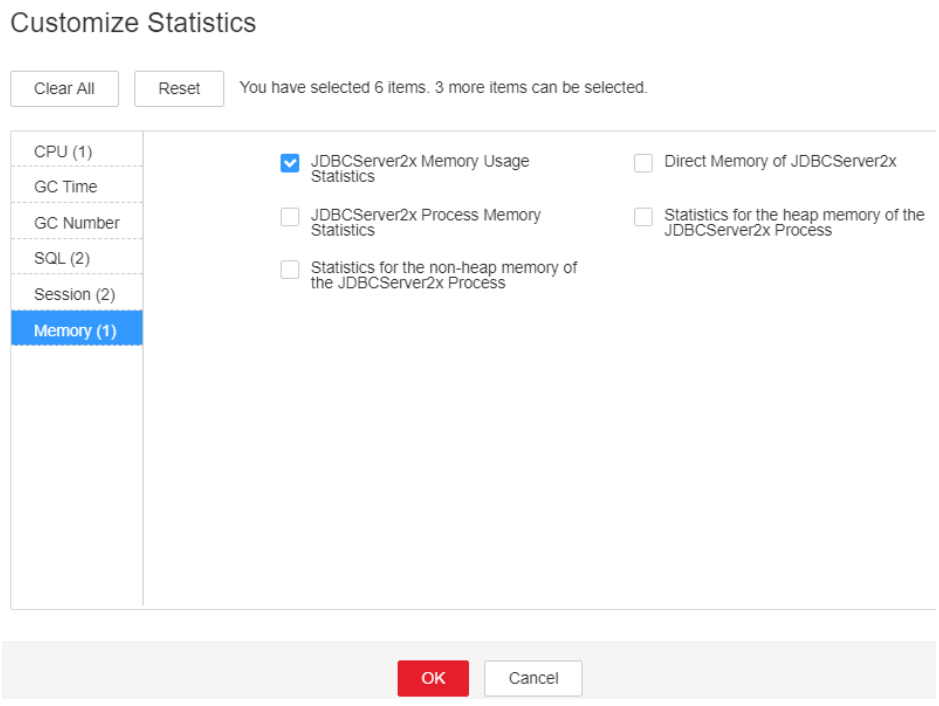
Comprobar el uso de memoria heap.

Paso 1 En el portal del Administrador FusionInsight, seleccione **O&M > Alarm > Alarms** y seleccione la alarma cuyo **ID** es **43010**. Compruebe el **RoleName** en **Location** y confirme la dirección IP de **HostName**.

Paso 2 En el portal del FusionInsight Manager, elija **Cluster >** *Name of the desired cluster* **> Services** > **Spark2x** > **Instance** y haga clic en el JDBCServer2x para el que se genera la alarma para ir a la página **Dashboard**. Haga clic en el menú desplegable en el área Chart y elija **Customize** > **Memory** > **JDBCServer2x Memory Usage Statistics** en el cuadro de lista desplegable en la esquina superior derecha y haga clic en **OK**. Compruebe si la memoria heap usada del proceso JDBCServer2x alcanza el umbral (valor predeterminado es 95%) de la memoria heap máxima especificada para JDBCServer2x.

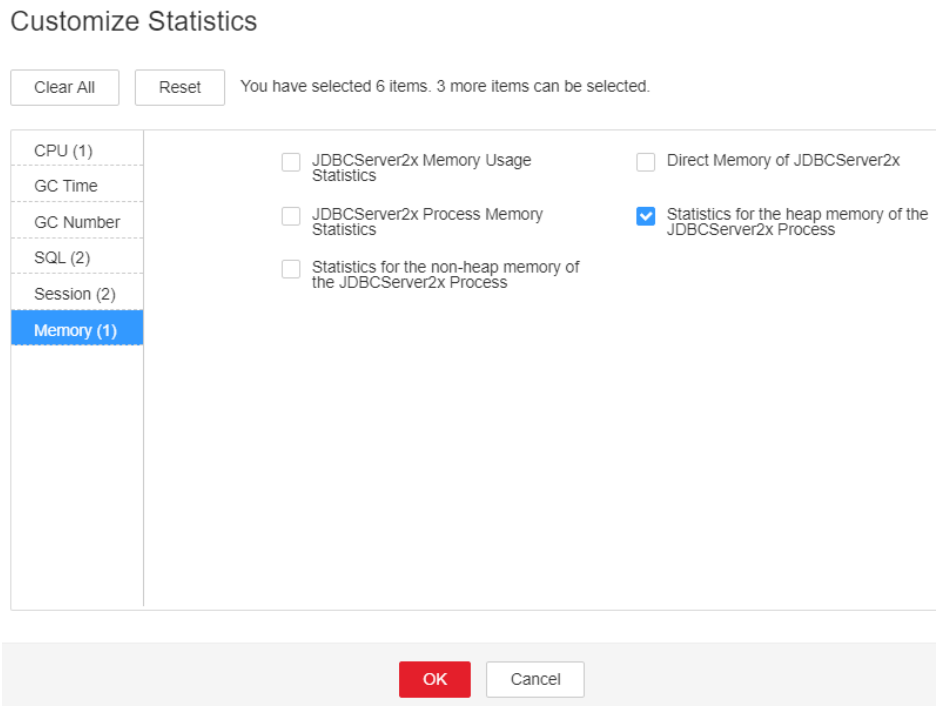
- En caso afirmativo, vaya a **Paso 3**.
- Si no, vaya a **Paso 7**.

Figura 9-90 Estadísticas de uso de memoria de JDBCServer2x



Paso 3 En la página de inicio del FusionInsight Manager, seleccione **Cluster** > *Name of the desired cluster* > **Services** > **Spark2x** > **Instance**. Haga clic en **JDBCServer2x** por la que se informa que la alarma va a la página **Dashboard** y haga clic en la lista desplegable en la esquina superior derecha del área del gráfico, elija **Customize** > **Memory > Statistics for the heap memory of the JDBCServer2x Process** y haga clic en **OK**. En función del tiempo de generación de alarma, compruebe los valores de la memoria heap usada del proceso JDBCServer2x en el período correspondiente y obtenga el valor máximo.

Figura 9-91 Estadísticas para la memoria heap del proceso JDBCServer2x



Paso 4 En el portal de FusionInsight Manager, elija **Cluster >** *Name of the desired cluster* **> Services** > **Spark2x** > **Configurations** y haga clic en **All Configurations**. Elija **JDBCServer2x** > **Tuning**. El valor predeterminado de **SPARK_DRIVER_MEMORY** es 4 GB. Puede cambiar el valor de acuerdo con las siguientes reglas: Relación entre el uso máximo de memoria heap de JobHistory2x y el **Threshold** del **JDBCServer2x Heap Memory Usage Statistics (JDBCServer2x)** en el período de alarma. Si esta alarma se genera ocasionalmente después de ajustar el valor del parámetro, aumente el valor en 0.5 veces. Si la alarma se notifica con frecuencia después de ajustar el valor del parámetro, aumente el valor en 1 vez. En el caso de un gran volumen de servicio y alta simultaneidad, agregue instancias.

NOTA

En la página de inicio del FusionInsight Manager, elija **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster* **> Spark2x** > **Memory** >**JDBCServer2x Heap Memory Usage Statistics (JDBCServer2x)** para ver **Threshold**.

Paso 5 Reinicie todas las instancias de JDBCServer2x.

Paso 6 Después de 10 minutos, compruebe si la alarma está borrada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 7**.

Recopilar información de fallas.

Paso 7 En el portal del FusionInsight Manager, elija **O&M** > **Log > Download**.

Paso 8 Seleccione **Spark2x** en el clúster requerido en el **Service**.

Paso 9 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 10 Póngase en contacto con el y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.225 ALM-43011 El uso de memoria no heap del proceso de JDBCServer2x supera el umbral

Descripción

El sistema comprueba el estado del proceso JDBCServer2x cada 30 segundos. La alarma se genera cuando el uso de memoria no heap de un proceso JDBCServer2x excede el umbral (95% de la memoria máxima).

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
43011	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el nombre del servicio para el que se genera la alarma.
RoleName	Especifica el nombre del rol para el que se genera la alarma.
HostName	Especifica el objeto (ID de host) para el que se genera la alarma.
Trigger Condition	Especifica el umbral que activa la alarma. Si el valor del indicador actual excede este umbral, se genera la alarma.

Impacto en el sistema

Si la memoria no heap de proceso de JDBCServer2x disponible es insuficiente, se produce un desbordamiento de memoria y el servicio se interrumpe.

Causas posibles

La memoria no heap del proceso JDBCServer2x se utiliza en exceso o la memoria no heap se asigna de forma inadecuada.

Procedimiento

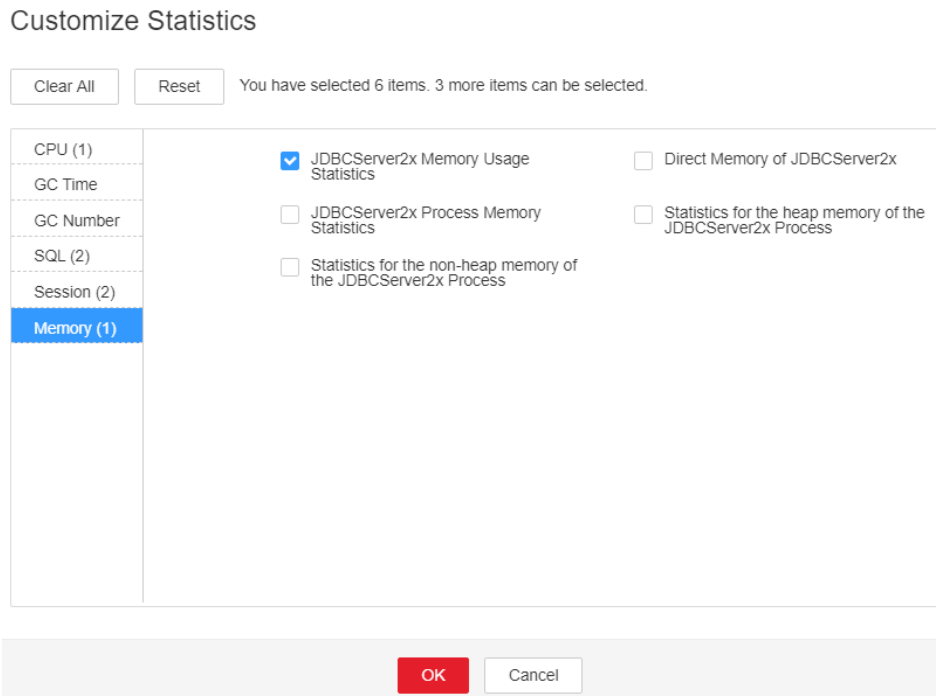
Verificar el uso de memoria no heap.

Paso 1 En el portal del FusionInsight Manager, seleccione **O&M > Alarm > Alarms** y seleccione la alarma cuyo **ID** es **43011**. Compruebe el **RoleName** en **Location** y confirme la dirección IP de **HostName**.

Paso 2 En el portal del FusionInsight Manager, elija **Cluster >** *Name of the desired cluster* **> Services** > **Spark2x** > **Instance** y haga clic en el JDBCServer2x para el que se genera la alarma para ir a la página **Dashboard**. Haga clic en el menú desplegable en el área Chart y elija **Customize** > **Memory** > **JDBCServer2x Memory Usage Statistics** en el cuadro de lista desplegable en la esquina superior derecha y haga clic en **OK**. Compruebe si la memoria no heap utilizada del proceso de JDBCServer2x alcanza el umbral (valor predeterminado es 95%) de la memoria no heap máxima especificada para JDBCServer2x.

- En caso afirmativo, vaya a **Paso 3**.
- Si no, vaya a **Paso 7**.

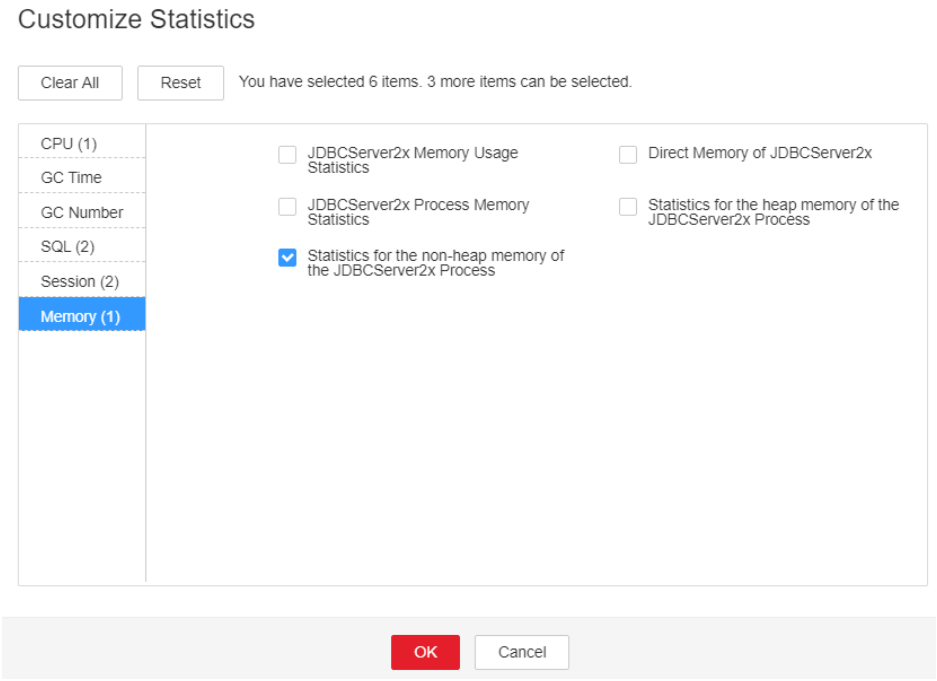
Figura 9-92 Estadísticas de uso de memoria de JDBCServer2x



Paso 3 En la página de inicio del FusionInsight Manager, seleccione **Cluster** > *Name of the desired cluster* > **Services** > **Spark2x** > **Instance**. Haga clic en **JDBCServer2x** por la que se informa

que la alarma va a la página **Dashboard** y haga clic en la lista desplegable en la esquina superior derecha del área del gráfico, elija **Customize** > **Memory > Statistics for the non-heap memory of the JDBCServer2x Process** y haga clic en **OK**. En base al tiempo de generación de alarma, compruebe los valores de la memoria no heap utilizada del proceso JDBCServer2x en el período correspondiente y obtenga el valor máximo.

Figura 9-93 Estadísticas para la memoria no heap del proceso JDBCServer2x



Paso 4 En el portal de FusionInsight Manager, elija **Cluster >** *Name of the desired cluster* **> Services** > **Spark2x** > **Configurations** y haga clic en **All Configurations**. Elija **JDBCServer2x** > **Tuning**. Puede cambiar el valor de **-XX: MaxMetaspaceSize** en **spark.driver.extraJavaOptions** de acuerdo con las siguientes reglas: La relación entre el valor máximo de la memoria no heap utilizada por JDBCServer2x y **Threshold** de **JDBCServer2x Non-Heap Memory Usage Statistics (JDBCServer2x)** en el período de alarma.

NOTA

En la página de inicio del FusionInsight Manager, elija **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster* **> Spark2x** > **Memory** > **JDBCServer2x Non-Heap Memory Usage Statistics (JDBCServer2x)** para ver **Threshold**.

Paso 5 Reinicie todas las instancias de JDBCServer2x.

Paso 6 Después de 10 minutos, compruebe si la alarma está borrada.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 7**.

Recopilar información de fallas.

Paso 7 En el portal del FusionInsight Manager, elija **O&M** > **Log >Download**.

Paso 8 Seleccione **Spark2x** en el clúster requerido en el **Service**.

Paso 9 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 10 Póngase en contacto con el y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.226 ALM-43012 El uso de memoria heap directa del proceso de JDBCServer2x supera el umbral

Descripción

El sistema comprueba el estado del proceso JDBCServer2x cada 30 segundos. La alarma se genera cuando el uso de memoria directa de un proceso de JDBCServer2x excede el umbral (95% de la memoria máxima).

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
43012	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el nombre del servicio para el que se genera la alarma.
RoleName	Especifica el nombre del rol para el que se genera la alarma.
HostName	Especifica el objeto (ID de host) para el que se genera la alarma.
Trigger Condition	Especifica el umbral que activa la alarma. Si el valor del indicador actual excede este umbral, se genera la alarma.

Impacto en el sistema

Si la memoria heap directa del proceso de JDBCServer2x disponible es insuficiente, se produce un desbordamiento de memoria y el servicio se interrumpe.

Causas posibles

La memoria heap directa del proceso JDBCServer2x se utiliza en exceso o la memoria heap directa se asigna de forma inadecuada.

Procedimiento

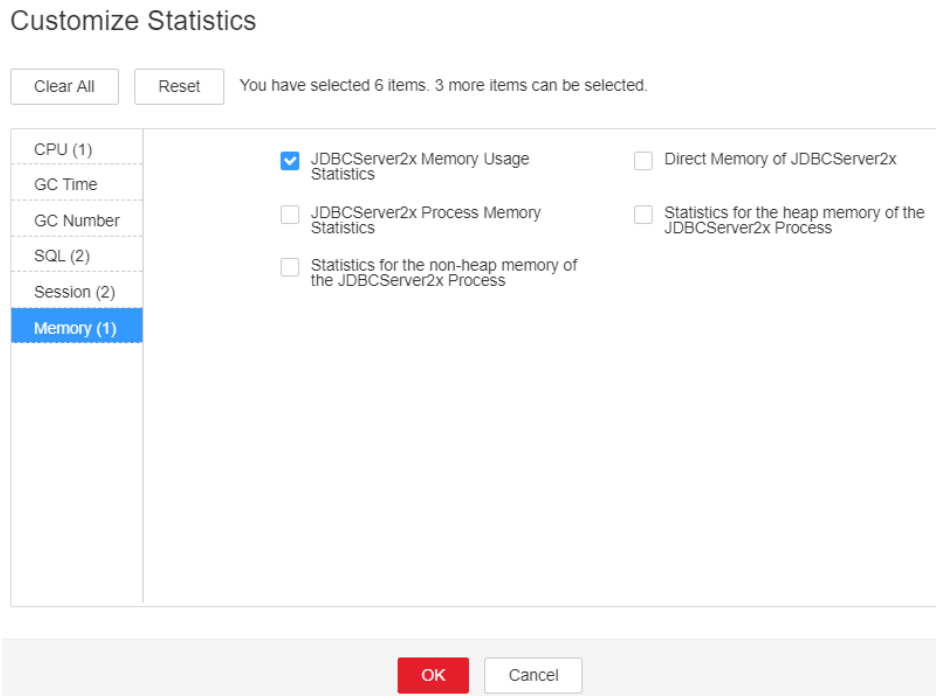
Comprobar el uso de memoria heap directa.

Paso 1 En el portal del administrador FusionInsight, seleccione **O&M > Alarm > Alarms** y seleccione la alarma cuyo **ID** es **43012**. Compruebe el **RoleName** en **Location** y confirme la dirección IP de **HostName**.

Paso 2 En el portal del FusionInsight Manager, elija **Cluster >** *Name of the desired cluster* **> Services** > **Spark2x** > **Instance** y haga clic en el JDBCServer2x para el que se genera la alarma para ir a la página **Dashboard**. Haga clic en el menú desplegable en el área Chart y elija **Customize** > **Memory** > **JDBCServer2x Memory Usage Statistics** en el cuadro de lista desplegable en la esquina superior derecha y haga clic en **OK**. Compruebe si la memoria heap directa utilizada del proceso JDBCServer2x alcanza el umbral (valor predeterminado es 95%) de la memoria heap directa máxima especificada para JDBCServer2x.

- En caso afirmativo, vaya a **Paso 3**.
- Si no, vaya a **Paso 7**.

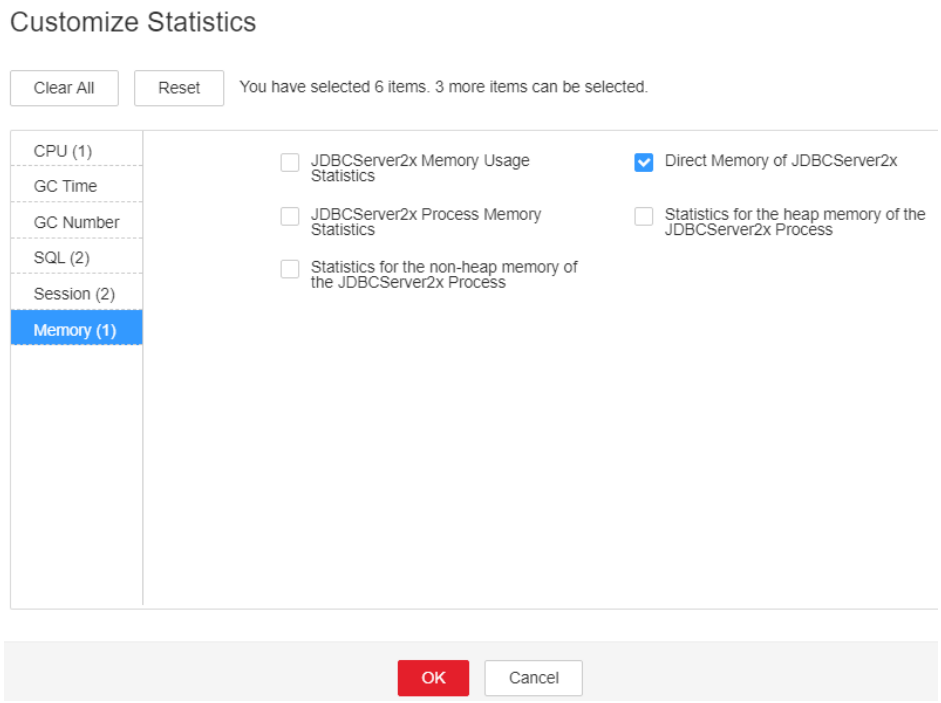
Figura 9-94 Estadísticas de uso de memoria de JDBCServer2x



Paso 3 En la página de inicio del FusionInsight Manager, seleccione **Cluster** > *Name of the desired cluster* > **Services** > **Spark2x** > **Instance**. Haga clic en **JDBCServer2x** por el cual se informa

que la alarma va a la página **Dashboard** y haga clic en la lista desplegable en la esquina superior derecha del área del chart, elija **Customize** > **Memory > Direct Memory of JDBCServer2x** y haga clic en **OK**. En función del tiempo de generación de alarma, compruebe los valores de la memoria directa utilizada del proceso JDBCServer2x en el período correspondiente y obtenga el valor máximo.

Figura 9-95 Memoria directa de JDBCServer2x



Paso 4 En el portal de FusionInsight Manager, elija **Cluster >** *Name of the desired cluster* **> Services** > **Spark2x** > **Configurations** y haga clic en **All Configurations**. Elija **JDBCServer2x** > **Tuning**. El valor predeterminado de **-XX:MaxDirectMemorySize** en **spark.driver.extraJavaOptions** es de 512 MB. Puede cambiar el valor de acuerdo con las siguientes reglas: Relación entre el uso máximo de memoria directa del JDBCServer2x y el **Threshold** del **JDBCServer2x Direct Memory Usage Statistics (JDBCServer2x)** en el período de alarma. Si esta alarma se genera ocasionalmente después de ajustar el valor del parámetro, aumente el valor en 0.5 veces. Si la alarma se notifica con frecuencia después de ajustar el valor del parámetro, aumente el valor en 1 vez. En el caso de un gran volumen de servicio y una alta simultaneidad de servicio, se recomienda agregar instancias.

NOTA

En la página de inicio del FusionInsight Manager, elija **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster* **> Spark2x** > **Memory** >**JDBCServer2x Direct Memory Usage Statistics (JDBCServer2x)** para ver **Threshold**.

Paso 5 Reinicie todas las instancias de JDBCServer2x.

Paso 6 Después de 10 minutos, compruebe si la alarma está borrada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 7**.

Recopilar información de fallas.

Paso 7 En el portal del FusionInsight Manager, elija **O&M** > **Log > Download**.

Paso 8 Seleccione **Spark2x** en el clúster requerido en el **Service**.

Paso 9 Haga clic en  en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 10 Póngase en contacto con el y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.227 ALM-43013 El tiempo de GC de proceso de JDBCServer2x supera el umbral

Descripción

El sistema comprueba el tiempo de recogida de basura (GC) del proceso JDBCServer2x cada 60 segundos. Esta alarma se genera cuando el tiempo GC detectado excede el umbral (excede 5 segundos durante tres comprobaciones consecutivas). Para cambiar el umbral, elija **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster* > **Spark2x** > **GC Time** > **Total GC time in milliseconds (JDBCServer2x)**. Esta alarma se borra cuando el tiempo de GC de JDBCServer2x es más corto o igual que el umbral.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
43013	Importante	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el nombre del servicio para el que se genera la alarma.
RoleName	Especifica el nombre del rol para el que se genera la alarma.

Nombre	Significado
HostName	Especifica el objeto (ID de host) para el que se genera la alarma.
Trigger Condition	Genera una alarma cuando el valor real del indicador excede el umbral especificado.

Impacto en el sistema

Si el tiempo de GC excede el umbral, JDBCServer2x puede ejecutarse con bajo rendimiento.

Causas posibles

La memoria de JDBCServer2x se utiliza en exceso, la memoria heap se asigna de forma inapropiada. Como resultado, los GC ocurren con frecuencia.

Procedimiento

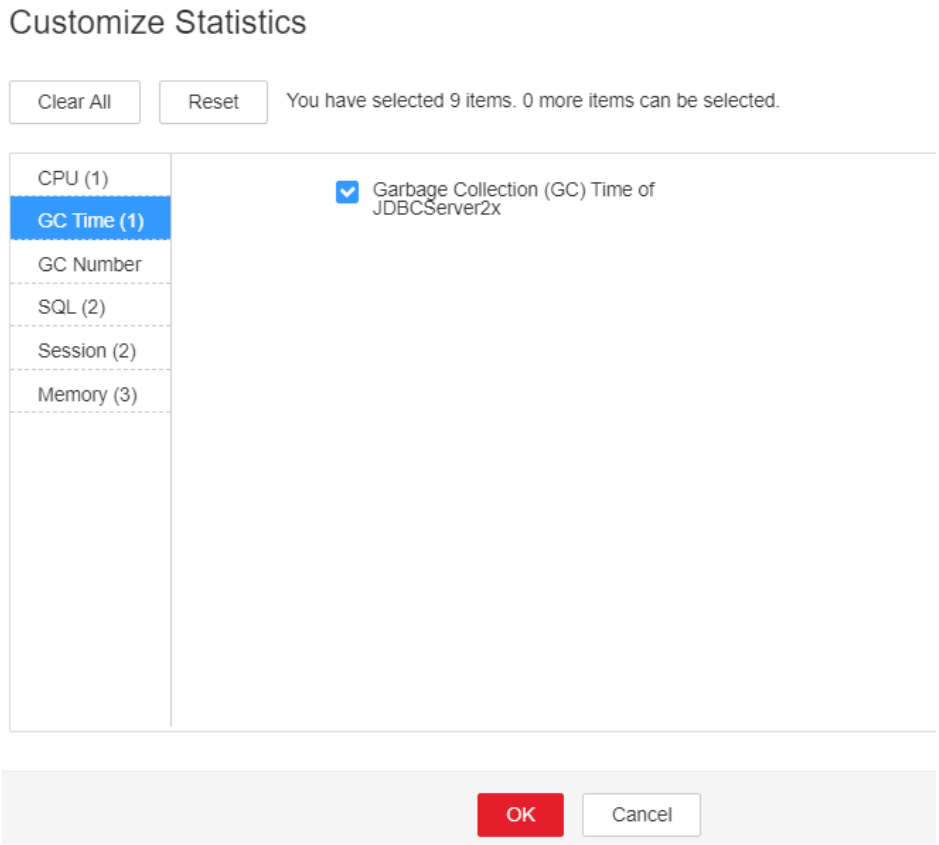
Comprobar el tiempo de GC.

Paso 1 En el portal del Administrador FusionInsight, seleccione **O&M > Alarm > Alarms** y seleccione la alarma cuyo **ID** es **43013**. Compruebe el **RoleName** en **Location** y confirme la dirección IP de **HostName**.

Paso 2 En el portal del FusionInsight Manager, elija **Cluster >** *Name of the desired cluster* **> Services** > **Spark2x** > **Instance** y haga clic en el JDBCServer2x para el que se genera la alarma para ir a la página **Dashboard**. Haga clic en el menú desplegable en el área Chart y elija **Customize** > **GC Time** > **Garbage Collection (GC) Time of JDBCServer2x** en el cuadro de lista desplegable en la esquina superior derecha y haga clic en **OK** para comprobar si el tiempo de GC es más largo que el umbral (valor predeterminado: 12 segundos).

- En caso afirmativo, vaya a **Paso 3**.
- Si no, vaya a **Paso 6**.

Figura 9-96 Tiempo de Recogida de basura (GC) de JDBCServer2x



Paso 3 En el portal del FusionInsight Manager, elija **Cluster** > *Name of the desired cluster* > **Services** > **Spark2x** > **Configurations**, y haga clic en **All Configurations**. Elija **JDBCServer2x** > **Default**. El valor predeterminado de **SPARK_DRIVER_MEMORY** es 4 GB. Puede cambiar el valor de acuerdo con las siguientes reglas: Si esta alarma se genera ocasionalmente, aumente el valor en 0.5 veces. Si la alarma se informa con frecuencia, aumente el valor en 1 vez. En el caso de un gran volumen de servicio y una alta simultaneidad de servicio, se recomienda agregar instancias.

Paso 4 Reinicie todas las instancias de JDBCServer2x.

Paso 5 Después de 10 minutos, compruebe si la alarma está borrada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 6**.

Recopilar información de fallas.

Paso 6 En la interfaz del FusionInsight Manager de los clústeres activos y en espera, seleccione **O&M** > **Log** > **Download**.

Paso 7 Seleccione **Spark2x** en el clúster requerido en el **Service**.

Paso 8 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 9 Póngase en contacto con el y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Información relacionada

Ninguna

9.228 ALM-43017 El número de Full GC del proceso JDBCServer2x supera el umbral

Descripción

El sistema comprueba el número de veces de recolección de basura completa (GC) del proceso JDBCServer2x cada 60 segundos. Esta alarma se genera cuando el número de Full GC detectado supera el umbral (excede 12 durante tres comprobaciones consecutivas.) Puede cambiar el umbral seleccionando **O&M > Alarm** > **Thresholds** > *Name of the desired cluster* > **Spark2x** > **GC number** > **Full GC Number of JDBCServer2x**. Esta alarma se borra cuando el número de GC completo del proceso JDBCServer2x es menor o igual que el umbral.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
43017	Importante	Sí

Parámetros

Nombre	Descripción
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger Condition	Especifica el umbral para activar la alarma.

Impacto en el sistema

El rendimiento del proceso JDBCServer2x se ve afectado, o incluso el proceso JDBCServer2x no está disponible.

Causas posibles

El uso de memoria heap del proceso JDBCServer2x es excesivamente grande, o la memoria heap se asigna de forma inadecuada. Como resultado, se produce con frecuencia Full CG.

Procedimiento

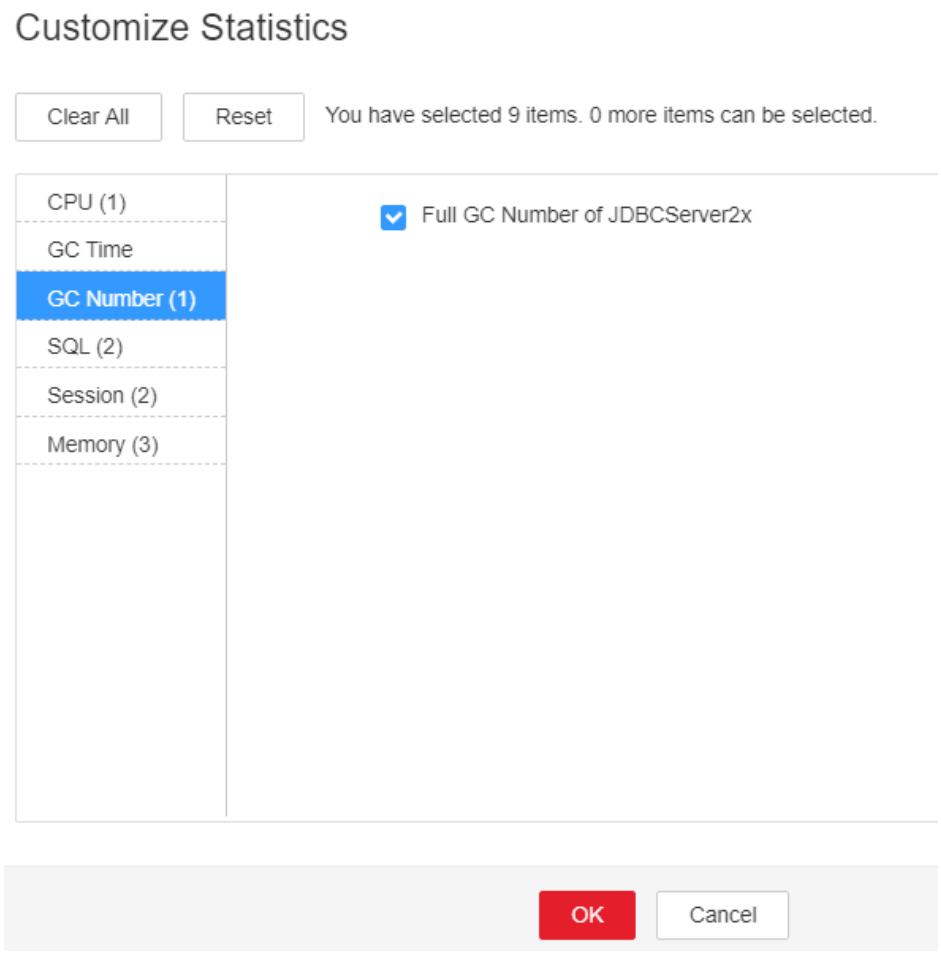
Comprobar el número de Full GCs.

Paso 1 Inicie sesión en FusionInsight Manager, seleccione **O&M** > **Alarm > Alarms**, seleccione esta alarma y compruebe el **RoleName** en **Location** y confirme la dirección IP de **HostName**.

Paso 2 Elija **Cluster** > *Name of the desired cluster* > **Services** > **Spark2x** > **Instance**. En la página mostrada, haga clic en el JDBCServer2x para el que se reporta la alarma. En la página **Dashboard** que se muestra, haga clic en el menú desplegable en el área Chart y elija **Customize** > **GC Number** > **Full GC Number of JDBCServer2x** en la esquina superior derecha y haga clic en **OK**. Compruebe si el número de Full GC del proceso JDBCServer2x es mayor que el umbral(valor predeterminado: 12).

- Si lo es, vaya a **Paso 3**.
- Si no es así, vaya a **Paso 6**.

Figura 9-97 Número de Full GC de JDBCServer2x



Paso 3 Seleccione **Cluster** > *Name of the desired cluster* > **Services** > **Spark2x** > **Configurations** > **All Configurations**. En la página mostrada, elija **JDBCServer2x** >**Tuning**. El valor

predeterminado de **SPARK_DRIVER_MEMORY** es de 4GB. Puede cambiar el valor de acuerdo con las siguientes reglas: Si esta alarma se genera ocasionalmente, aumente el valor en 0.5 veces. Si la alarma se informa con frecuencia, aumente el valor en 1 vez. En el caso de un gran volumen de servicio y alta simultaneidad, agregue instancias.

Paso 4 Reinicie todas las instancias de JDBCServer2x.

Paso 5 Después de 10 minutos, compruebe si la alarma está borrada.

- Si lo es, no se requiere ninguna otra acción.
- Si no es así, vaya a **Paso 6**.

Recopilar información de fallas.

Paso 6 Inicie sesión en el Administrador de FusionInsight y elija **O&M** > **Log** > **Download**.

Paso 7 Seleccione **Spark2x** en el clúster requerido en la lista desplegable **Service**.

Paso 8 Haga clic en  en la esquina superior derecha. En el cuadro de diálogo que se muestra, establezca **Start Date** y **End Date** en 10 minutos antes y después del tiempo de generación de alarmas respectivamente y haga clic en **OK**. A continuación, haga clic en **Download**.

Paso 9 Póngase en contacto con el y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borrará automáticamente después de que se corrija la falla.

Información relacionada

Ninguna

9.229 ALM-43018 Número de Full GC de proceso de JobHistory2x supera el umbral

Descripción

El sistema comprueba el número de veces de recolección de basura completa (GC) del proceso JobHistory2x cada 60 segundos. Esta alarma se genera cuando el número de GC completo detectado supera el umbral (excede 12 durante tres comprobaciones consecutivas.) Puede cambiar el umbral seleccionando **O&M** > **Alarm > Thresholds** > *Name of the desired cluster* > **Spark2x** > **GC number** > **Full GC Number of JobHistory2x**. Esta alarma se borra cuando el número de GC completo del proceso JobHistory2x es menor o igual que el umbral.

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
43018	Importante	Sí

Parámetros

Nombre	Descripción
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger Condition	Especifica el umbral para activar la alarma.

Impacto en el sistema

El rendimiento del proceso de JobHistory2x se ve afectado, o incluso el proceso de JobHistory2x no está disponible.

Causas posibles

El uso de memoria heap del proceso JobHistory2x es excesivamente grande, o la memoria heap se asigna de forma inadecuada. Como resultado, se produce con frecuencia Full CG.

Procedimiento

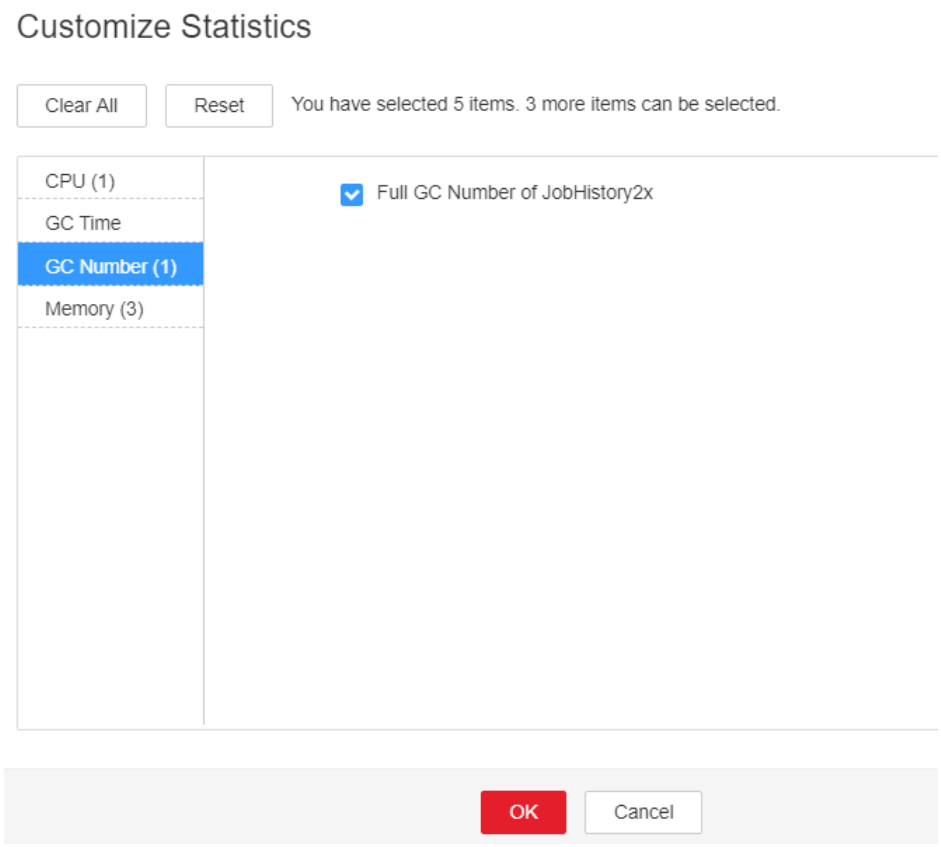
Comprobar el número de Full GCs.

Paso 1 Inicie sesión en FusionInsight Manager, seleccione **O&M** > **Alarm > Alarms**, seleccione esta alarma y compruebe el **RoleName** en **Location** y confirme la dirección IP de **HostName**.

Paso 2 Elija **Cluster** > *Name of the desired cluster* > **Services** > **Spark2x** > **Instance**. En la página mostrada, haga clic en JobHistory2x para la que se ha informado la alarma. En la página **Dashboard** que se muestra, haga clic en el menú desplegable en el área Gráfico y elija **Customize** > **GC Number** > **Full GC Number of JobHistory2x** en la esquina superior derecha y haga clic en **OK**. Compruebe si el número de GC completos del proceso JobHistory2x es mayor que el umbral (valor predeterminado: 12).

- Si lo es, vaya a **Paso 3**.
- Si no es así, vaya a **Paso 6**.

Figura 9-98 Número de Full GC de JobHistory2x



Paso 3 Seleccione **Cluster** > *Name of the desired cluster* > **Services** > **Spark2x** > **Configurations** > **All Configurations**. En la página mostrada, elija **JobHistory2x** > **Default.** El valor predeterminado de **SPARK_DAEMON_MEMORY** es 4GB. Puede cambiar el valor de acuerdo con las siguientes reglas: Si esta alarma se genera ocasionalmente, aumente el valor en 0.5 veces. Si la alarma se informa con frecuencia, aumente el valor en 1 vez.

Paso 4 Reinicie todas las instancias de JobHistory2x.

Paso 5 Después de 10 minutos, compruebe si la alarma está borrada.

- Si lo es, no se requiere ninguna otra acción.
- Si no es así, vaya a **Paso 6**.

Recopilar información de fallas.

Paso 6 Inicie sesión en el Administrador de FusionInsight y elija **O&M** > **Log** > **Download**.

Paso 7 Seleccione **Spark2x** en el clúster requerido en el **Service**.

Paso 8 Haga clic en en la esquina superior derecha. En el cuadro de diálogo que se muestra, establezca **Start Date** y **End Date** en 10 minutos antes y después del tiempo de generación de alarmas respectivamente y haga clic en **OK**. A continuación, haga clic en **Download**.

Paso 9 Póngase en contacto con el y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borrará automáticamente después de que se corrija la falla.

Información relacionada

Ninguna

9.230 ALM-43019 El uso de memoria heap del proceso de IndexServer2x supera el umbral

Descripción

El sistema comprueba el estado del proceso IndexServer2x cada 30 segundos. La alarma se genera cuando el uso de memoria heap de un proceso de IndexServer2x excede el umbral (95% de la memoria máxima).

Atributo

ID de alarma	Severidad	Borrar automáticamente
43019	Importante	Sí

Parámetros

Parámetro	Descripción
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger Condition	Especifica el umbral para activar la alarma.

Impacto en el sistema

Si la memoria heap de procesos de IndexServer2x disponible es insuficiente, se produce un desbordamiento de memoria y el servicio se interrumpe.

Causas posibles

La memoria heap del proceso IndexServer2x se utiliza en exceso o la memoria heap se asigna de forma inadecuada.

Procedimiento

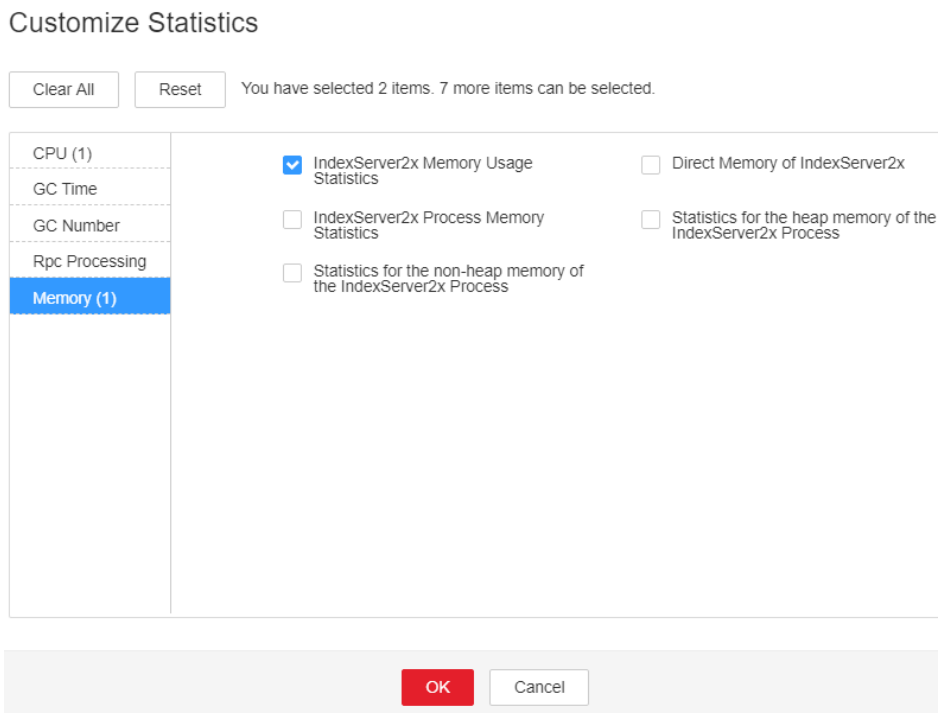
Comprobar el uso de la memoria heap.

Paso 1 En FusionInsight Manager, elija **O&M** >**Alarm > Alarms**. En la lista de alarmas mostrada, elija la alarma para la que el ID es **43019**, compruebe el **RoleName** en **Location** y confirme la dirección IP de **HostName**.

Paso 2 En FusionInsight Manager, seleccione **Cluster** > *Name of the desired cluster* > **Services** > **Spark2x** > **Instance**. Haga clic en IndexServer2x que informó la alarma para ir a la página **Dashboard**. Haga clic en la lista desplegable situada en la esquina superior derecha del área del gráfico y elija **Customize** > **Memory** > **IndexServer2x Memory Usage Statistics** > **OK**. Compruebe si la memoria heap utilizada por el proceso IndexServer2x alcanza el umbral máximo de memoria heap (95% de forma predeterminada).

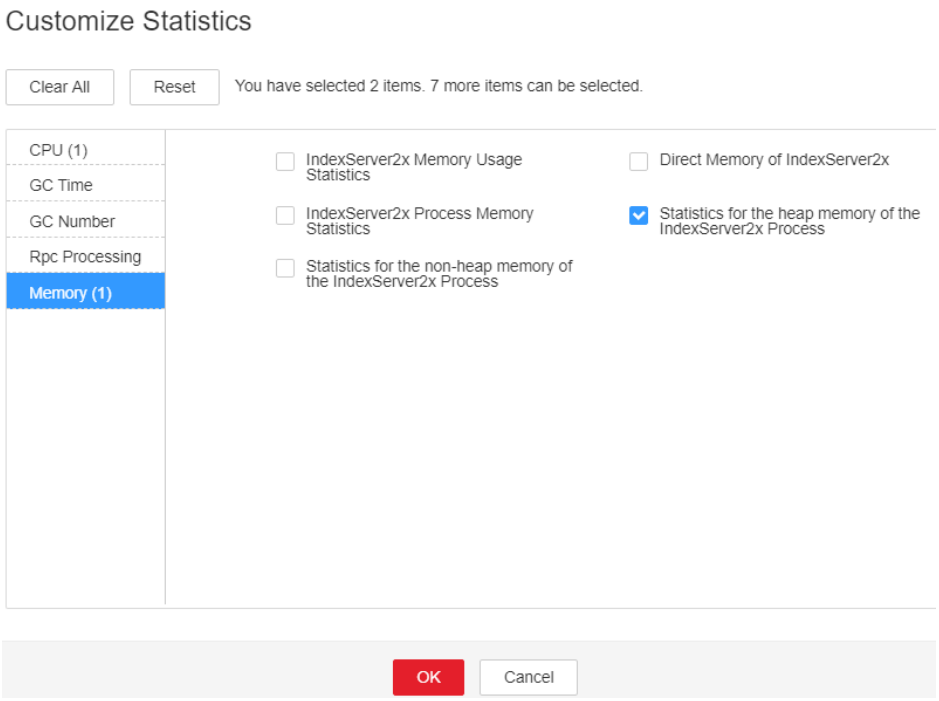
- Si se alcanza el umbral, vaya a **Paso 3**.
- Si no se alcanza el umbral, vaya a **Paso 7**.

Figura 9-99 Estadísticas de uso de memoria de IndexServer2x



Paso 3 En FusionInsight Manager, seleccione **Cluster** > *Name of the desired cluster* > **Services** > **Spark2x** > **Instance**. Haga clic en IndexServer2x que informó la alarma para ir a la página **Dashboard**. Haga clic en la lista desplegable situada en la esquina superior derecha del área del gráfico y elija **Customize** > **Memory** > **Statistics for the heap memory of the IndexServer2x Process** > **OK**. En función del tiempo de generación de alarma, compruebe los valores de la memoria heap utilizada del proceso de IndexServer2x en el período correspondiente y obtenga el valor máximo.

Figura 9-100 Estadísticas para la memoria heap del proceso IndexServer2x



Paso 4 En FusionInsight Manager, seleccione **Cluster** > *Name of the desired cluster* > **Services** > **Spark2x** > **Configurations** > **All Configuration** > **IndexServer2x**> **Tuning**. El valor predeterminado del parámetro **SPARK_DRIVER_MEMORY** es 4 GB. Puede cambiar el valor en función de la relación entre la memoria heap máxima utilizada por el proceso de IndexServer2x y el umbral especificado por **IndexServer2x Heap Memory Usage Statistics (IndexServer2x)** en el período de alarma. Si la alarma persiste después de cambiar el valor del parámetro, aumente el valor en 0.5 veces. Si la alarma se genera con frecuencia, duplique la velocidad.

NOTA

En FusionInsight Manager, puede elegir **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster* > **Spark2x** > **Memory** > **IndexServer2x Heap Memory Usage Statistics (IndexServer2x)** para ver el umbral.

Paso 5 Reinicie todas las instancias de IndexServer2x.

Paso 6 Después de 10 minutos, compruebe si la alarma está borrada.

- Si la alarma se ha borrado, no se requiere ninguna acción adicional.
- Si la alarma no está desactivada, vaya a **Paso 7**.

Recopilar información de fallas.

Paso 7 En FusionInsight Manager, elija **O&M** > **Log** > **Download**.

Paso 8 Expanda la lista desplegable **Service** y seleccione **Spark2x** para el clúster de destino.

Paso 9 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas respectivamente. A continuación, haga clic en **Download**.

Paso 10 Póngase en contacto con el y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Referencia

Ninguna

9.231 ALM-43020 El uso de memoria no heap del proceso IndexServer2x supera el umbral

Descripción

El sistema comprueba el estado del proceso IndexServer2x cada 30 segundos. La alarma se genera cuando el uso de memoria no heap del proceso IndexServer2x excede el umbral (95% de la memoria máxima).

Atributo

ID de alarma	Severidad	Borrar automáticamente
43020	Importante	Sí

Parámetros

Parámetro	Descripción
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger Condition	Especifica el umbral para activar la alarma.

Impacto en el sistema

Si la memoria no heap del proceso IndexServer2x disponible es insuficiente, se produce un desbordamiento de memoria y el servicio se interrumpe.

Causas posibles

La memoria no heap del proceso IndexServer2x se utiliza en exceso o la memoria no heap se asigna de forma inadecuada.

Procedimiento

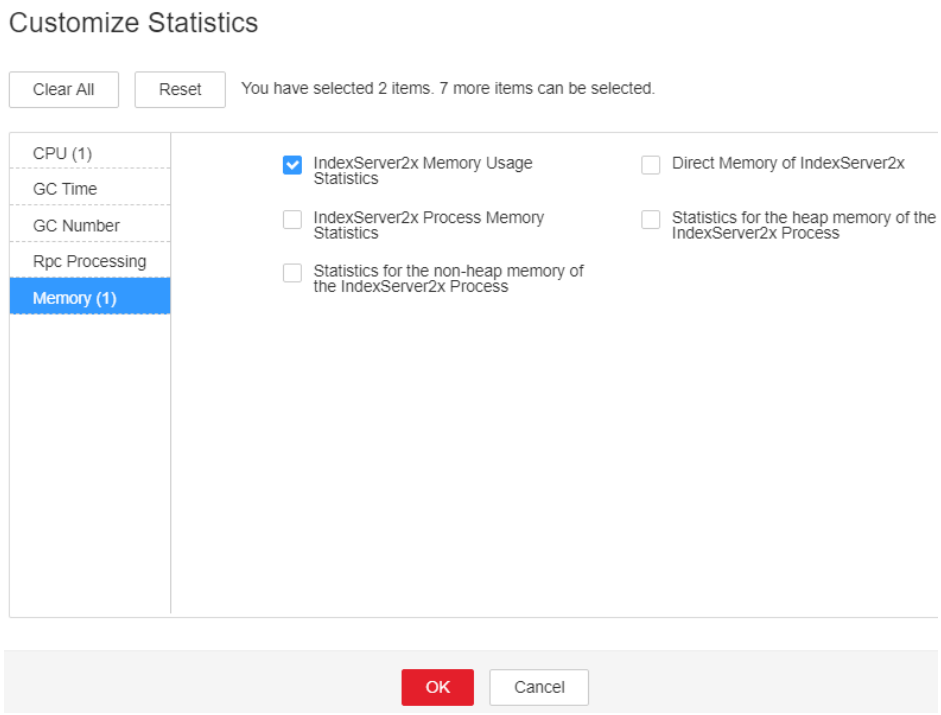
Verificar el uso de memoria no heap.

Paso 1 En FusionInsight Manager, elija **O&M** >**Alarm > Alarms**. En la lista de alarmas mostrada, elija la alarma para la que el ID es **43020**, compruebe el **RoleName** en **Location** y confirme la dirección IP de **HostName**.

Paso 2 En FusionInsight Manager, seleccione **Cluster** > *Name of the desired cluster* > **Services** > **Spark2x** > **Instance**. Haga clic en IndexServer2x que informó la alarma para ir a la página **Dashboard**. Haga clic en la lista desplegable situada en la esquina superior derecha del área del gráfico y elija **Customize** > **Memory > IndexServer2x Memory Usage Statistics** > **OK**. Compruebe si la memoria no heap utilizada por el proceso IndexServer2x alcanza el umbral máximo de memoria no heap (95% de forma predeterminada).

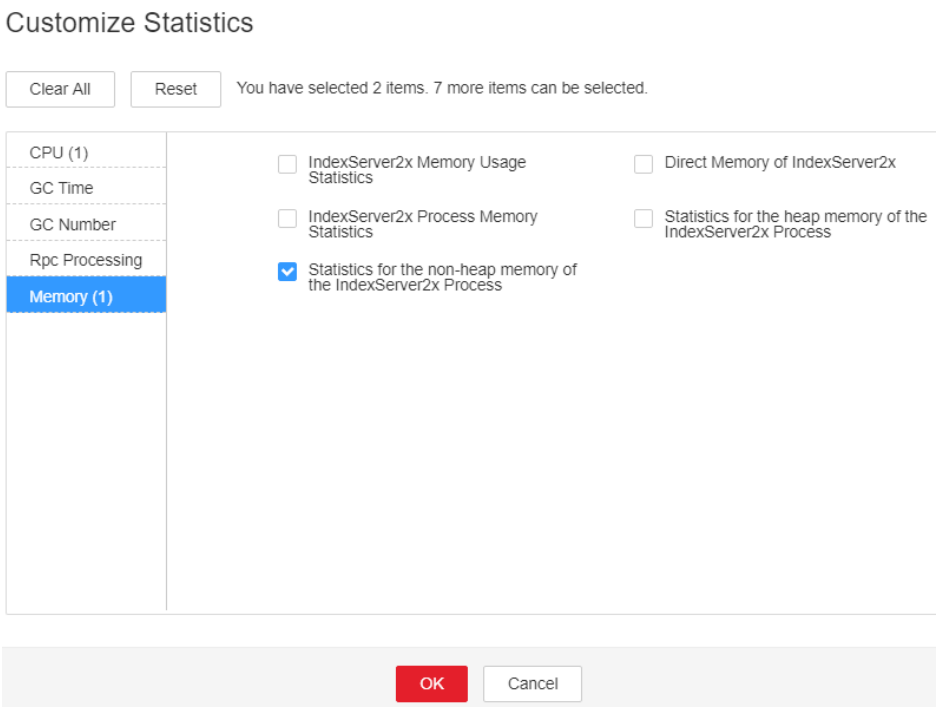
- Si se alcanza el umbral, vaya a **Paso 3**.
- Si no se alcanza el umbral, vaya a **Paso 7**.

Figura 9-101 Estadísticas de uso de memoria de IndexServer2x



Paso 3 En FusionInsight Manager, seleccione **Cluster** > *Name of the desired cluster* > **Services** > **Spark2x** > **Instance**. Haga clic en IndexServer2x que informó la alarma para ir a la página **Dashboard**. Haga clic en la lista desplegable situada en la esquina superior derecha del área del gráfico y elija **Customize** > **Memory** > **Statistics for the non-heap memory of the IndexServer2x Process** > **OK**. En función del tiempo de generación de alarmas, compruebe los valores de la memoria no heap utilizada del proceso IndexServer2x en el período correspondiente y obtenga el valor máximo.

Figura 9-102 Estadísticas para la memoria no heap del proceso IndexServer2x



Paso 4 En FusionInsight Manager, seleccione **Cluster** > *Name of the desired cluster* > **Services** > **Spark2x** > **Configurations** > **All Configurations** > **IndexServer2x**> **Tuning**. Puede cambiar el valor de **XX:MaxMetaspaceSize** en el parámetro **spark.driver.extraJavaOptions** en función de la relación entre la memoria no heap máxima utilizada por el proceso IndexServer2x y el umbral especificado por **IndexServer2x Non-Heap Memory Usage Statistics (IndexServer2x)** en el período de alarma.

NOTA

En FusionInsight Manager, puede elegir **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster* > **Spark2x** > **Memory** > **IndexServer2x Non-Heap Memory Usage Statistics (IndexServer2x)** para ver el umbral.

Paso 5 Reinicie todas las instancias de IndexServer2x.

Paso 6 Después de 10 minutos, compruebe si la alarma está borrada.

- Si la alarma se ha borrado, no se requiere ninguna acción adicional.
- Si la alarma no está borrada, vaya a **Paso 7**.

Recopilar información de fallas.

Paso 7 En FusionInsight Manager, elija **O&M** > **Log** > **Download**.

Paso 8 Expanda la lista desplegable **Service** y seleccione **Spark2x** para el clúster de destino.

Paso 9 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas respectivamente. A continuación, haga clic en **Download**.

Paso 10 Póngase en contacto con el y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Referencia

Ninguna

9.232 ALM-43021 El uso de memoria directa del proceso IndexServer2x supera el umbral

Descripción

El sistema comprueba el estado del proceso IndexServer2x cada 30 segundos. La alarma se genera cuando el uso directo de memoria heap de un proceso IndexServer2x excede el umbral (95% de la memoria máxima).

Atributo

ID de alarma	Severidad	Borrar automáticamente
43021	Importante	Sí

Parámetros

Parámetro	Descripción
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger Condition	Especifica el umbral para activar la alarma.

Impacto en el sistema

Si la memoria directa del proceso IndexServer2x disponible es insuficiente, se produce un desbordamiento de memoria y el servicio se interrumpe.

Causas posibles

La memoria heap directa del proceso IndexServer2x se utiliza en exceso o la memoria heap directa se asigna de forma inadecuada.

Procedimiento

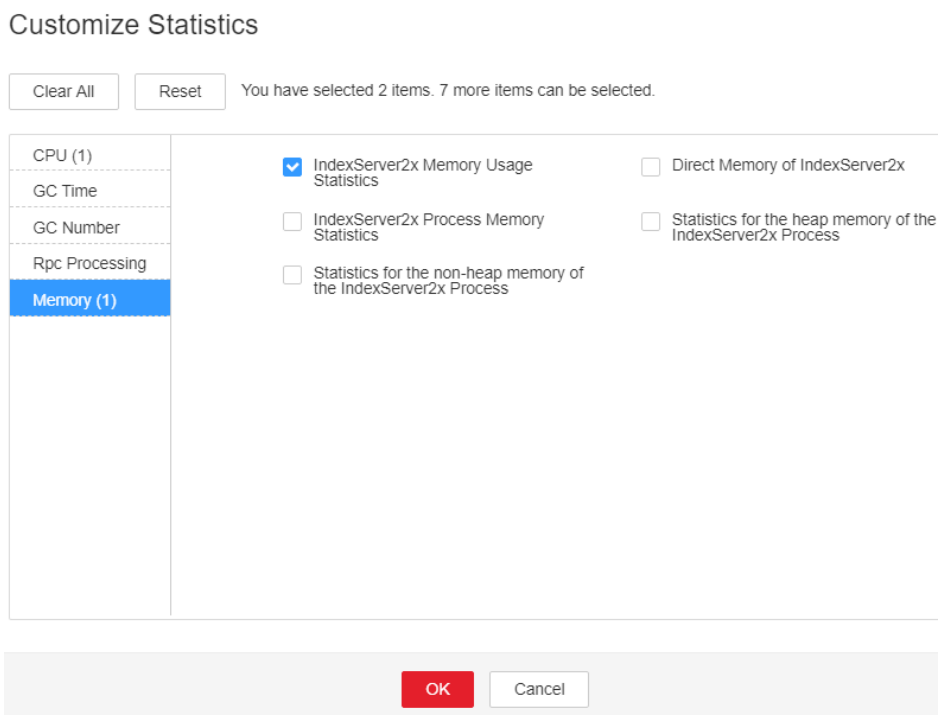
Comprobar el uso de memoria heap directa.

Paso 1 En FusionInsight Manager, elija **O&M** >**Alarm > Alarms**. En la lista de alarmas mostrada, elija la alarma para la que el ID es **43021**, compruebe el **RoleName** en **Location** y confirme la dirección IP de **HostName**.

Paso 2 En FusionInsight Manager, seleccione **Cluster** > *Name of the desired cluster* > **Services** > **Spark2x** > **Instance**. Haga clic en IndexServer2x que informó la alarma para ir a la página **Dashboard**. Haga clic en la lista desplegable situada en la esquina superior derecha del área del gráfico y elija **Customize** > **Memory** > **IndexServer2x Memory Usage Statistics** > **OK**. Compruebe si la memoria directa utilizada por el proceso IndexServer2x alcanza el umbral máximo de memoria directa.

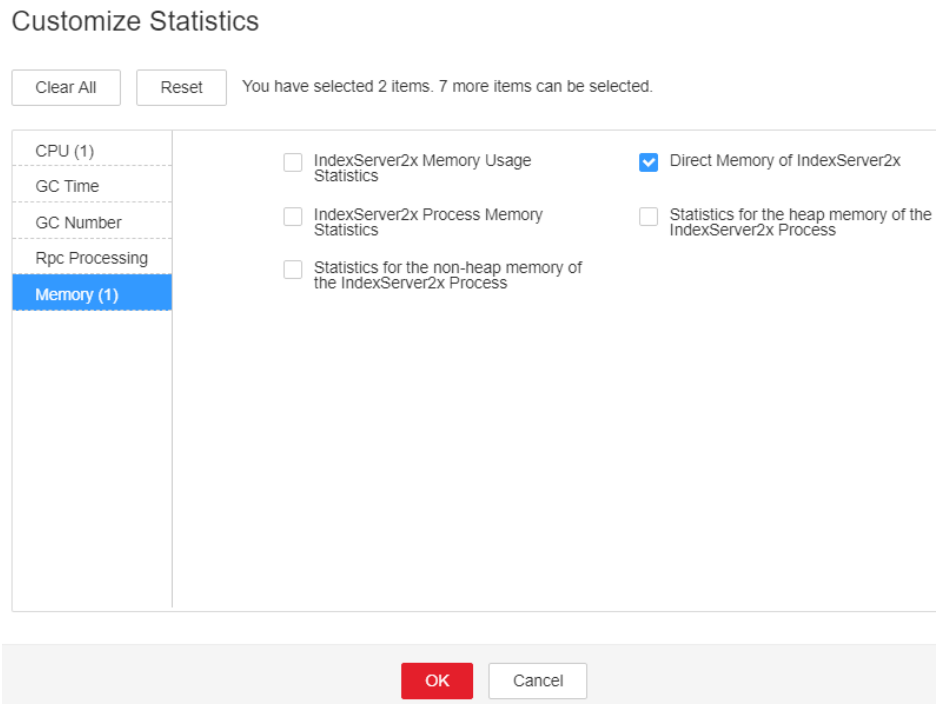
- Si se alcanza el umbral, vaya a **Paso 3**.
- Si no se alcanza el umbral, vaya a **Paso 7**.

Figura 9-103 Estadísticas de uso de memoria de IndexServer2x



Paso 3 En FusionInsight Manager, seleccione **Cluster** > *Name of the desired cluster* > **Services** > **Spark2x** > **Instance**. Haga clic en IndexServer2x que informó la alarma para ir a la página **Dashboard**. Haga clic en la lista desplegable situada en la esquina superior derecha del área del gráfico y elija **Customize** > **Memory** > **Direct Memory of IndexServer2x** > **OK**. En función del tiempo de generación de alarma, compruebe los valores de la memoria directa utilizada del proceso IndexServer2x en el período correspondiente y obtenga el valor máximo.

Figura 9-104 Memoria directa de IndexServer2x



Paso 4 En FusionInsight Manager, seleccione **Cluster** > *Name of the desired cluster* > **Services** > **Spark2x** > **Configurations** > **All Configurations** > **IndexServer2x**> **Tuning**. Puede cambiar el valor de **XX:MaxDirectMemorySize** (el valor predeterminado es 512 MB) en el parámetro **spark.driver.extraJavaOptions** en función de la relación entre la memoria directa máxima utilizada por el proceso IndexServer2x y el umbral especificado por **IndexServer2x Direct Memory Usage Statistics (IndexServer2x)** en el período de alarma. Si la alarma persiste después de cambiar el valor del parámetro, aumente el valor en 0.5 veces. Si la alarma se genera con frecuencia, duplique la velocidad.

NOTA

En el Administrador de FusionInsight, puede elegir **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster* > **Spark2x** > **Memory** > **IndexServer2x Direct Memory Usage Statistics (IndexServer2x)** para ver el umbral.

Paso 5 Reinicie todas las instancias de IndexServer2x.

Paso 6 Después de 10 minutos, compruebe si la alarma está borrada.

- Si la alarma se ha borrado, no se requiere ninguna acción adicional.
- Si la alarma no está borrada, vaya a **Paso 7**.

Recopilar información de fallas.

Paso 7 En FusionInsight Manager, elija **O&M** > **Log** > **Download**.

Paso 8 Expanda la lista desplegable **Service** y seleccione **Spark2x** para el clúster de destino.

Paso 9 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas respectivamente. A continuación, haga clic en **Download**.

Paso 10 Póngase en contacto con el y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Referencia

Ninguna

9.233 ALM-43022 El tiempo de GC de proceso de IndexServer2x supera el umbral

Descripción

El sistema comprueba la hora de GC del proceso IndexServer2x cada 60 segundos. Esta alarma se genera cuando el tiempo GC detectado excede el umbral (12 segundos) durante tres veces consecutivas. Para cambiar el umbral, elija **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster* > **Spark2x** > **GC Time** > **Total GC time in milliseconds (IndexServer2x)**. Esta alarma se borra cuando el tiempo de GC de IndexServer2x es menor o igual que el umbral.

Atributo

ID de alarma	Severidad	Borrar automáticamente
43022	Importante	Sí

Parámetros

Parámetro	Descripción
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger Condition	Especifica el umbral para activar la alarma.

Impacto en el sistema

Si el tiempo de GC excede el umbral, IndexServer2x puede ejecutarse con bajo rendimiento o incluso no estar disponible.

Causas posibles

La memoria heap del proceso IndexServer2x se utiliza en exceso o la memoria heap se asigna de forma inadecuada. Como resultado, la GC ocurre con frecuencia.

Procedimiento

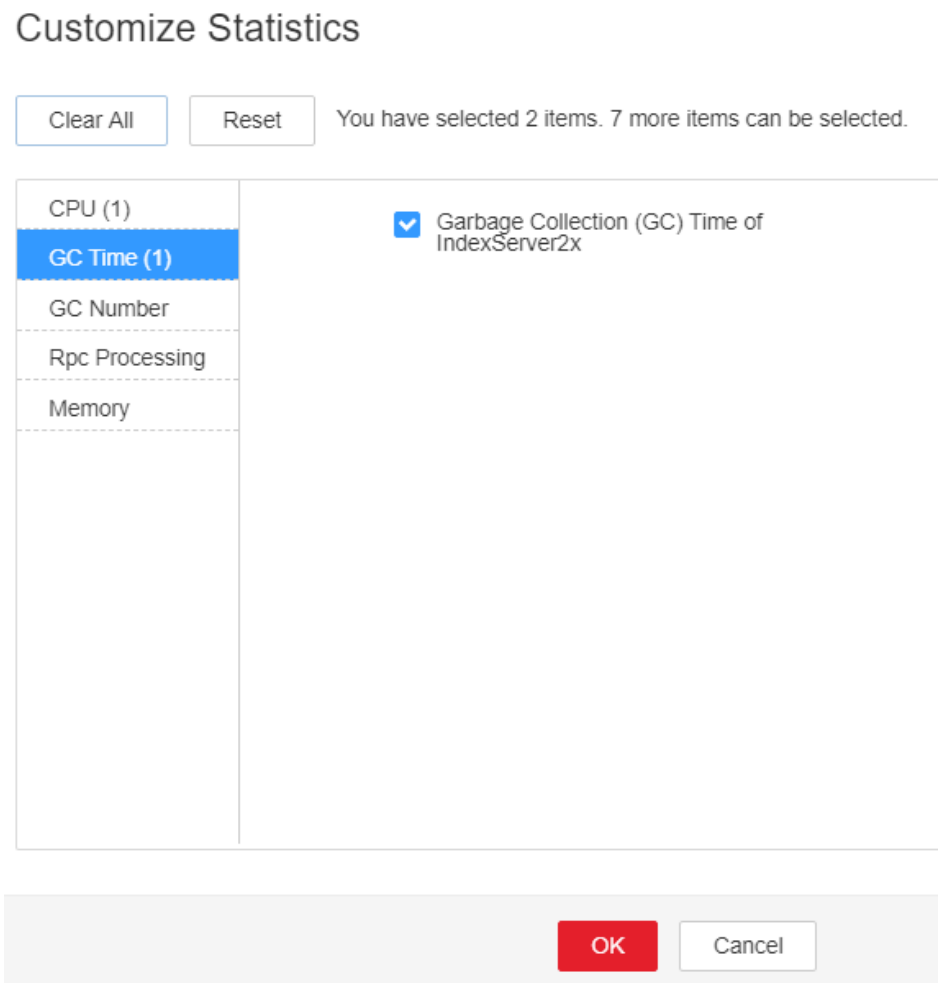
Comprobar el tiempo de GC.

Paso 1 En FusionInsight Manager, elija **O&M** >**Alarm > Alarms**. En la lista de alarmas mostrada, elija la alarma con ID **43022**, compruebe el **RoleName** en **Location** y confirme la dirección IP de **HostName**.

Paso 2 En FusionInsight Manager, elija **Cluster** > *Name of the desired cluster* > **Services** > **Spark2x** > **Instance** y haga clic en IndexServer2x para el que se genera la alarma para ir a la página **Dashboard**. Haga clic en el menú desplegable en el área Chart y elija **Customize** > **GC Time** > **Garbage Collection (GC) Time of IndexServer2x** en el cuadro de lista desplegable en la esquina superior derecha y haga clic en **OK** para comprobar si el tiempo de GC es más largo que el umbral (valor predeterminado: 12 segundos).

- Si se alcanza el umbral, vaya a **Paso 3**.
- Si no se alcanza el umbral, vaya a **Paso 6**.

Figura 9-105 Tiempo de recolección de basura (GC) de IndexServer2x



Paso 3 En FusionInsight Manager, elija **Cluster** > *Name of the desired cluster* > **Services** > **Spark2x** > **Configurations** > **All Configurations** > **IndexServer2x** > **Default**. El valor predeterminado del **SPARK_DRIVER_MEMORY** es 4 GB. Puede cambiar el valor de acuerdo con las siguientes reglas: Aumente el valor del parámetro **SPARK_DRIVER_MEMORY** 1.5 veces a su valor predeterminado. Si esta alarma todavía se genera ocasionalmente después del ajuste, aumente el valor en 0.5 veces. Duplique el valor si la alarma se informa con frecuencia.

Paso 4 Reinicie todas las instancias de IndexServer2x.

Paso 5 Después de 10 minutos, compruebe si la alarma está borrada.

- Si la alarma se ha borrado, no se requiere ninguna acción adicional.
- Si la alarma no está desactivada, vaya a **Paso 6**.

Recopilar información de fallas.

Paso 6 En FusionInsight Manager, elija **O&M** > **Log** > **Download**.

Paso 7 Expanda la lista desplegable **Service** y seleccione **Spark2x** para el clúster de destino.

Paso 8 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas respectivamente. A continuación, haga clic en **Download**.

Paso 9 Póngase en contacto con el y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Referencia

Ninguna

9.234 ALM-43023 El número de Full GC del proceso IndexServer2x supera el umbral

Descripción

El sistema comprueba el número de Full GC del proceso IndexServer2x cada 60 segundos. Esta alarma se genera cuando el número de Full GC detectado excede el umbral (12) durante tres veces consecutivas. Puede cambiar el umbral seleccionando **O&M** > **Alarm** > **Thresholds** > *Name of the desired cluster* > **Spark2x** > **GC Number** > **Full GC Number of IndexServer2x**. Esta alarma se borra cuando el número de Full GC del proceso IndexServer2x es menor o igual que el umbral. Esta alarma se borra cuando el número de Full GC del proceso IndexServer2x es menor o igual que el umbral.

Atributo

ID de alarma	Severidad	Borrar automáticamente
43023	Importante	Sí

Parámetros

Parámetro	Descripción
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger Condition	Especifica el umbral para activar la alarma.

Impacto en el sistema

Si el número de GC excede el umbral, IndexServer2x puede ejecutarse con bajo rendimiento o incluso no está disponible.

Causas posibles

La memoria heap del proceso IndexServer2x se utiliza en exceso o la memoria heap se asigna de forma inadecuada. Como resultado, se produce con frecuencia Full CG.

Procedimiento

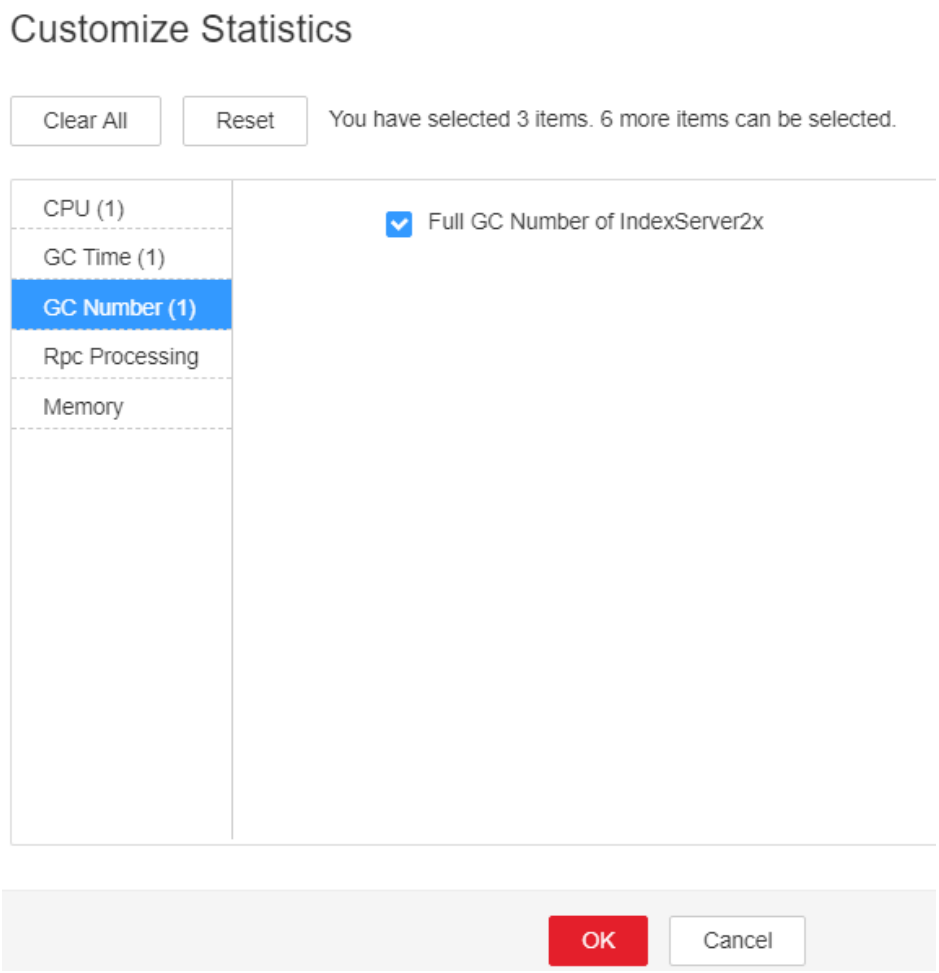
Comprobar el número de Full GCs.

Paso 1 En FusionInsight Manager, elija **O&M** >**Alarm > Alarms**. En la lista de alarmas mostrada, elija la alarma con el ID **43023**, compruebe el **RoleName** en **Location** y confirme la dirección IP de **HostName**.

Paso 2 En FusionInsight Manager, elija **Cluster** > *Name of the desired cluster* > **Services** > **Spark2x** > **Instance** y haga clic en IndexServer2x para el que se genera la alarma para ir a la página **Dashboard**. Haga clic en el menú desplegable en el área del gráfico y elija **Customize** > **GC Number > Full GC Number of IndexServer2x** en el cuadro de lista desplegable en la esquina superior derecha y haga clic en **OK** para comprobar si el número de GC es mayor que el umbral (valor predeterminado: 12).

- Si se alcanza el umbral, vaya a **Paso 3**.
- Si no se alcanza el umbral, vaya a **Paso 6**.

Figura 9-106 Número de Full GC de IndexServer2x



Paso 3 En FusionInsight Manager, elija **Cluster** > *Name of the desired cluster* > **Services** > **Spark2x** > **Configurations** > **All Configurations** > **IndexServer2x** > **Tuning**. El valor predeterminado del **SPARK_DRIVER_MEMORY** es 4 GB. Puede cambiar el valor de acuerdo con las siguientes reglas: Si esta alarma se genera ocasionalmente, aumente el valor en 0.5 veces. Duplique el valor si la alarma se informa con frecuencia. En el caso de un gran volumen de servicio y una alta simultaneidad de servicio, se recomienda agregar instancias.

Paso 4 Reinicie todas las instancias de IndexServer2x.

Paso 5 Después de 10 minutos, compruebe si la alarma está borrada.

- Si la alarma se ha borrado, no se requiere ninguna acción adicional.
- Si la alarma no está borrada, vaya a **Paso 6**.

Recopilar información de fallas.

Paso 6 En FusionInsight Manager, elija **O&M** > **Log** > **Download**.

Paso 7 Expanda la lista desplegable **Service** y seleccione **Spark2x** para el clúster de destino.

Paso 8 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas respectivamente. A continuación, haga clic en **Download**.

Paso 9 Póngase en contacto con el y envíe los registros de fallas recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Referencia

Ninguna

9.235 ALM-44000 Servicio Presto no disponible

Descripción

El sistema comprueba el estado del servicio Presto cada 60 segundos. Esta alarma se genera cuando el sistema detecta que Presto no está disponible.

Esta alarma se borra cuando el servicio Presto se recupera.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
44000	Crítica	Sí

Parámetros

Nombre	Significado
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

Presto no puede ejecutar consultas SQL.

Causas posibles

- El proceso de Coordinator o worker de Presto es defectuoso.
- Se interrumpe la comunicación de red entre las instancias del Presto coordinator y del worker.

Procedimiento

Paso 1 Comprobar el estado de los procesos de coordinator y worker.

1. Inicie sesión en FusionInsight Manager y elija **Cluster** > **Services** > **Presto**. En la página que se muestra, haga clic en la pestaña **Instance**. En la lista de instancias de Presto, compruebe si el estado de todas las instancias de coordinator o de worker es **Unknown**.
   - En caso afirmativo, vaya a **2**.
   - Si no, vaya a **1**.
2. En la parte superior de la lista de instancias de Presto, elija **More** > **Restart Service** para reiniciar los procesos de coordinator y worker.
3. En la lista de alarmas, compruebe si ALM-44000 Servicio Presto no disponible está desactivado.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **1** en **Paso 2**.

Paso 2 Recopile información de fallas.

1. En FusionInsight Manager, elija **System** >**Export Log**.
2. Seleccione **Presto** para **Service**.
3. Haga clic en  en la esquina superior derecha.

   Establezca **Start Time** y **End Time** para la recopilación de registros a 10 minutos antes y después del tiempo de generación de alarma, respectivamente. A continuación, haga clic en **OK**.
4. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

9.236 ALM-44004 Las tareas en cola del grupo de recursos de Presto Coordinator superan el umbral

Descripción

Esta alarma se genera cuando el sistema detecta que el número de tareas de cola en un grupo de recursos excede el umbral. El sistema consulta el número de tareas de cola en un grupo de recursos a través de la interfaz JMX. Puede elegir **Components** > **Presto** > **Service Configuration** (cambiar **Basic** a **All**) > **Presto** > **resource-groups** para configurar un grupo de recursos. Puede elegir **Components** > **Presto** > **Service Configuration** (cambiar **Basic** a **All**) > **Coordinator** > **Customize** > **resourceGroupAlarm** para configurar el umbral de cada grupo de recursos.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
44004	Grave	Sí

Parámetros

Nombre	Significado
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

Si el número de tareas de cola en un grupo de recursos excede el umbral, un gran número de tareas puede estar en el estado de cola. El tiempo de tarea de Presto supera el valor esperado. Cuando el número de tareas de cola en un grupo de recursos excede el número máximo (**maxQueued**) de tareas de cola en el grupo de recursos, no se pueden ejecutar nuevas tareas.

Causas posibles

La configuración del grupo de recursos es incorrecta o se envían demasiadas tareas en el grupo de recursos.

Procedimiento

Paso 1 Seleccione **Components** > **Presto** > **Service Configuration** (cambiar **Basic** a **All**) > **Presto** > **resource-groups** para ajustar la configuración del grupo de recursos.

Paso 2 Puede elegir **Components** > **Presto** > **Service Configuration** (cambiar **Basic** a **All**) > **Coordinator** > **Customize** > **resourceGroupAlarm** para modificar el umbral de cada grupo de recursos.

Paso 3 Recopilar información de fallas.

1. Inicie sesión en el nodo del clúster según el nombre del host en la información de error y consulte el número de tareas de cola según **Resource Group** en la información adicional del cliente de Presto.
2. Inicie sesión en el nodo del clúster basándose en el nombre del host en la información de errores, vea el archivo **/var/log/Bigdata/nodeagent/monitorlog/monitor.log** y busque información del grupo de recursos para ver la información de recopilación de supervisión del grupo de recursos.
3. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Información relacionada

Ninguna

9.237 ALM-44005 El tiempo de GC de proceso Presto Coordinator excede el umbral

Descripción

El sistema recoge el tiempo de GC del proceso de Presto Coordinator cada 30 segundos. Esta alarma se genera cuando el tiempo de GC excede el umbral (excede 5 segundos durante tres veces consecutivas). Puede cambiar el umbral seleccionando **System** > **Configure Alarm Threshold** > **Service** > **Presto** > **Coordinator** > **Presto Process Garbage Collection Time** > **Garbage Collection Time of the Coordinator Process** en MRS Manager. Esta alarma se borra cuando el tiempo de proceso de GC del Coordinator es menor o igual que el umbral.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
44005	Grave	Sí

Parámetro

Parámetro	Descripción
ServiceName	Servicio para el que se genera la alarma.
RoleName	Rol para el que se genera la alarma.
HostName	Host para el que se genera la alarma.

Impacto en el sistema

Si el tiempo de GC del proceso del Coordinator es demasiado largo, el proceso del Coordinator se verá afectado y el proceso del Coordinator incluso no estará disponible.

Causas posibles

La memoria heap del proceso del Coordinator se utiliza en exceso o se asigna de manera inadecuada, lo que provoca la ocurrencia frecuente del proceso de GC.

Procedimiento

Paso 1 Compruebe el tiempo de GC.

1. Vaya a la página de detalles del clúster y elija **Alarms**.

NOTA

Para MRS 1.8.10 o anterior, inicie sesión en MRS Manager y elija **Alarms**.

2. Seleccione la alarma cuyo **Alarm ID** sea **44005** y luego compruebe el nombre del rol de **Location** y confirme la dirección IP de la instancia.
3. Seleccione **Components** > **Presto** > **Instances** > **Coordinator** (dirección IP del negocio de la instancia para la que se genera la alarma) > **Customize** > **Presto Garbage Collection Time**. Haga clic en **OK** para ver la hora de GC.
4. Compruebe si el tiempo de GC del proceso de Coordinator es superior a 5 segundos.
   - En caso afirmativo, vaya a **Paso 1.5**.
   - Si no, vaya a **Paso 2**.
5. Seleccione **Components** > **Presto** > **Service Configuration**, y cambie **Basic** a **All**. Elija **Presto** > **Coordinator**. Aumente el valor de **-Xmx** en el parámetro **JAVA_OPTS** según los requisitos del sitio.
6. Verifique si la alarma se ha borrado.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 2**.

Paso 2 Recopile información de fallas.

1. En MRS Manager, seleccione **System** > **Export Log**.
2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Referencia

Ninguna

9.238 ALM-44006 El tiempo de GC de proceso Presto Worker supera el umbral

Descripción

El sistema recoge el tiempo de GC del proceso de Presto Worker cada 30 segundos. Esta alarma se genera cuando el tiempo de GC excede el umbral (excede 5 segundos durante tres veces consecutivas). Puede cambiar el umbral seleccionando **System** > **Configure Alarm Threshold** > **Service** > **Presto** > **Worker** > **Presto Garbage Collection Time** > **Garbage Collection Time of the Worker Process** en MRS Manager. Esta alarma se borra cuando el tiempo de GC del proceso del trabajador es más corto que o igual al umbral.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
44006	Grave	Sí

Parámetro

Parámetro	Descripción
ServiceName	Servicio para el que se genera la alarma.
RoleName	Rol para el que se genera la alarma.
HostName	Host para el que se genera la alarma.

Impacto en el sistema

Si el tiempo de GC del proceso de Worker es demasiado largo, el rendimiento de ejecución del proceso de Worker se verá afectado y el proceso de Worker incluso no estará disponible.

Causas posibles

La memoria de pila del proceso de Worker se usa en exceso o se asigna de forma inadecuada, lo que provoca la ocurrencia frecuente del proceso de GC.

Procedimiento

Paso 1 Compruebe el tiempo de GC.

1. Vaya a la página de detalles del clúster y elija **Alarms**.

   NOTA

   Para MRS 1.8.10 o anterior, inicie sesión en MRS Manager y elija **Alarms**.

2. Seleccione la alarma cuyo **Alarm ID** sea **44006**. A continuación, compruebe el nombre del rol de **Location** y confirme la dirección IP de la instancia.
3. Elija **Components** > **Presto** > **Instances** > **Worker** (dirección IP del negocio de la instancia para la que se genera la alarma) > **Customize** > **Presto Garbage Collection Time**. Haga clic en **OK** para ver la hora de GC.
4. Compruebe si el tiempo de GC del proceso de Worker es superior a 5 segundos.
   - En caso afirmativo, vaya a **Paso 1.5**.
   - Si no, vaya a **Paso 2**.
5. Elija **Components** > **Presto** > **Service Configuration**, y cambie **Basic** a **All**, y elija **Presto** > **Worker** Aumente el valor de **-Xmx** (memoria heap máxima) en el parámetro **JAVA_OPTS** en función de los requisitos del sitio.
6. Verifique si la alarma se ha borrado.
   - En caso afirmativo, no es necesario hacer nada más.
   - Si no, vaya a **Paso 2**.

Paso 2 Recopile información de fallas.

1. En MRS Manager, seleccione **System** > **Export Log**.
2. Póngase en contacto con el personal de O&M y envíe los registros recopilados.

----Fin

Referencia

Ninguna

9.239 ALM-45000 Servicio HetuEngine no disponible

Descripción

El sistema comprueba el estado del servicio cada 300 segundos. Esta alarma se genera cuando el servicio no está disponible.

Esta alarma se borra cuando se recupera el servicio .

Atributo

ID de alarma	Gravedad de la alarma	Borrar automáticamente
45000	Crítica	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

Las tareas de no se pueden ejecutar.

Causas posibles

- El servicio KrbServer es anormal.
- El servicio ZooKeeper es anormal.
- El servicio HDFS es anormal.
- El servicio Yarn es anormal.
- El servicio DBService es anormal.
- El servicio Hive es anormal.

- No hay instancias de HSBroker en .

Procedimiento

Comprobar el estado de servicio KrbServer.

Paso 1 En FusionInsight Manager, seleccione **O&M** > **Alarm** > **Alarm**.

Paso 2 En la lista de alarmas, compruebe si se genera la alarma "ALM-25500 Servicio KrbServer no disponible".

- En caso afirmativo, vaya a **Paso 3**.
- Si no, vaya a **Paso 5**.

Paso 3 Borre "ALM-25500 Servicio KrbServer no disponible" de acuerdo con la ayuda de alarma.

Paso 4 En la lista de alarmas, compruebe si la alarma "ALM-45000 Servicio no disponible" está desactivada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 5**.

Verificar el estado del servicio de ZooKeeper.

Paso 5 En la lista de alarmas, compruebe si se genera la alarma "ALM-12007 Falla de proceso".

- En caso afirmativo, vaya a **Paso 6**.
- Si no, vaya a **Paso 9**.

Paso 6 En la lista de alarmas, haga clic en ⌄ en la fila que contiene la alarma "Falla de proceso". Compruebe si el nombre del servicio para el que se genera la alarma es ZooKeeper en **Location Information**.

- En caso afirmativo, vaya a **Paso 7**.
- Si no, vaya a **Paso 9**.

Paso 7 Borre "ALM-12007 Falla de proceso" de acuerdo con la ayuda de alarma.

Paso 8 En la lista de alarmas, compruebe si la alarma "ALM-45000 Servicio no disponible" está desactivada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 9**.

Comprobar el estado de servicio HDFS.

Paso 9 En la lista de alarmas, compruebe si se genera la alarma "ALM-14000 Servicio HDFS no disponible."

- En caso afirmativo, vaya a **Paso 10**.
- Si no, vaya a **Paso 12**.

Paso 10 Borre "ALM-14000 Servicio HDFS no disponible" de acuerdo con la ayuda de alarma.

Paso 11 En la lista de alarmas, compruebe si la alarma "ALM-45000 Servicio no disponible" está desactivada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 12**.

Comprobar el estado de servicio YARN.

Paso 12 En la lista de alarmas, compruebe si se genera la alarma "ALM-18000 Servicio YARN no disponible".

- En caso afirmativo, vaya a **Paso 13**.
- Si no, vaya a **Paso 15**.

Paso 13 Borre "ALM-18000 Servicio YARN no disponible" de acuerdo con la ayuda de alarma.

Paso 14 En la lista de alarmas, compruebe si la alarma "ALM-45000 Servicio no disponible" está desactivada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 15**.

Comprobar el estado del servicio DBService.

Paso 15 En la lista de alarmas, compruebe si se genera la alarma "ALM-27001 Servicio DBService no disponible".

- En caso afirmativo, vaya a **Paso 16**.
- Si no, vaya a **20**.

Paso 16 Borre "ALM-27001 Servicio DBService no disponible" de acuerdo con la ayuda de alarma.

Paso 17 En la lista de alarmas, compruebe si la alarma "ALM-45000 Servicio no disponible" está desactivada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **20**.

Comprobar el estado de servicio Hive.

Paso 18 En la lista de alarmas, compruebe si se genera la alarma "ALM-16004 Servicio Hive no disponible".

- En caso afirmativo, vaya a **Paso 19**.
- Si no, vaya a **20**.

Paso 19 Borre "ALM-16004 Servicio Hive no disponible" de acuerdo con la ayuda de alarma.

Paso 20 En la lista de alarmas, compruebe si la alarma "ALM-45000 Servicio no disponible" está desactivada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **20**.

Comprobar si no hay instancias de HSBroker en .

Paso 21 En FusionInsight Manager, elija **Cluster** > *Name of the desired cluster* > **Services** > . En la página que se muestra, haga clic en la pestaña **Instance**.

Paso 22 Compruebe si no hay instancias de HSBroker.

- Si es así, haga clic en **Add Instance** para agregar uno.
- Si no, vaya a **23**.

Paso 23 En la lista de alarmas, compruebe si la alarma "ALM-45000 Servicio no disponible" está desactivada.

- De ser así, no se requiere ninguna acción adicional.

- Si no, vaya a **23**.

Comprobar la conexión de red entre y ZooKeeper, HDFS, YARN, DBService y Hive.

Paso 24 En FusionInsight Manager, elija **Cluster** > *Name of the desired cluster* > **Services** > . En la página que se muestra, haga clic en la pestaña **Instance**.

Paso 25 Haga clic en el nombre de host en la fila **HSBroker** y registre la dirección IP de gestión en el área **Basic Information**.

Paso 26 Inicie sesión en el host donde reside HSBroker como usuario **omm** usando la dirección IP obtenida en **Paso 25**.

Paso 27 Ejecute el comando **ping** para comprobar si la conexión de red entre el host donde reside HSBroker y los hosts donde residen ZooKeeper y HDFS, Yarn, DBService y Hive está en el estado normal.

- En caso afirmativo, vaya a **Paso 30**.
- Si no, vaya a **Paso 28**.

Paso 28 Póngase en contacto con el administrador de red para restaurar la red.

Paso 29 En la lista de alarmas, compruebe si la alarma "ALM-45000 Servicio no disponible" está desactivada.

- De ser así, no se requiere ninguna acción adicional.
- Si no, vaya a **Paso 30**.

Recopilar información de fallas.

Paso 30 En FusionInsight Manager, elija **O&M** > **Log** > **Download**.

Paso 31 Expanda la lista desplegable **Service**. En el cuadro de diálogo **Services** que se muestra, seleccione en el nombre del clúster de destino y haga clic en **OK**.

Paso 32 Expanda la lista desplegable **Hosts**. En el cuadro de diálogo **Select Host** que se muestra, seleccione los hosts a los que pertenece el rol y haga clic en **OK**.

Paso 33 Haga clic en  en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 30 minutos antes y después del tiempo de generación de alarmas respectivamente. A continuación, haga clic en **Download**.

Paso 34 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar la falla, el sistema borra automáticamente esta alarma.

Referencia

Ninguna

9.240 ALM-45001 Instancias de cómputo de HetuEngine defectuoso

Esta alarma solo se aplica a MRS 3.2.0 o posterior.

Descripción

El sistema comprueba el estado de la instancia de cómputo de cada 60 segundos. Esta alarma se genera cuando una instancia de cómputo de es defectuosa.

Esta alarma se borra cuando se restauran todas las instancias de cómputo de defectuosas.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
45001	Grave	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

Las tareas de no se pueden ejecutar.

Causas posibles

- El servicio HDFS es anormal.
- El servicio Yarn es anormal.
- Los recursos de cola de Yarn son insuficientes.
- El proceso de las instancias de cómputo es defectuoso.

Procedimiento

Comprobar el estado de servicio HDFS.

Paso 1 En la lista de alarmas, compruebe si se genera la alarma "ALM-14000 Servicio HDFS no disponible."

- En caso afirmativo, vaya a **Paso 2**.
- Si no, vaya a **Paso 4**.

Paso 2 Borre "ALM-14000 Servicio HDFS no disponible" de acuerdo con la ayuda de alarma.

Paso 3 En la lista de alarmas, compruebe si la alarma "ALM-45001 Instancias de cómputo de defectuosas" está desactivada.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 4**.

Comprobar el estado de servicio YARN.

Paso 4 En la lista de alarmas, compruebe si se genera la alarma "ALM-18000 Servicio YARN no disponible".

- En caso afirmativo, vaya a **Paso 5**.
- Si no, vaya a **Paso 7**.

Paso 5 Borre "ALM-18000 Servicio YARN no disponible" de acuerdo con la ayuda de alarma.

Paso 6 En la lista de alarmas, compruebe si la alarma "ALM-45001 Instancias de cómputo de defectuosas" está desactivada.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 7**.

Comprobar el estado de recurso de cola de YARN.

Paso 7 En la lista de alarmas, compruebe si se genera la alarma "ALM-18022 Recursos de cola de YARN insuficientes".

- En caso afirmativo, vaya a **8**.
- Si no, vaya a **Paso 10**.

Paso 8 Borre "ALM-18022 Recursos de cola de YARN insuficientes" de acuerdo con la ayuda de alarma.

Paso 9 En la lista de alarmas, compruebe si la alarma "ALM-45001 Instancias de cómputo de defectuosas" está desactivada.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 10**.

Comprobar el estado de instancia de cómputo de .

Paso 10 Inicie sesión en FusionInsight Manager como administrador que puede acceder a la interfaz de usuario web de y elija **Cluster** > **Services >** .

Paso 11 En el área **Basic Information** de la página de pestaña **Dashboard**, haga clic en el vínculo situado junto a **HSConsole WebUI** para acceder a la página HSConsole.

Paso 12 En la página de instancia de cómputo, compruebe si alguna instancia de cómputo está en estado **FAULT**.

- En caso afirmativo, vaya a **Paso 13**.
- Si no, vaya a **Paso 14**.

Paso 13 En la columna **Operation** de la instancia de cálculo de destino, haga clic en **Start** y espere hasta que se inicie la instancia.

Paso 14 En la lista de alarmas, compruebe si la alarma "ALM-45001 Instancias de cómputo de defectuosas" está desactivada.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 15**.

Recopilar información de fallas.

Paso 15 En FusionInsight Manager, elija **O&M** > **Log** > **Download**.

Paso 16 Expanda la lista desplegable **Service**. En el cuadro de diálogo **Services** que se muestra, seleccione en el nombre del clúster de destino y haga clic en **OK**.

Paso 17 Expanda la lista desplegable **Hosts**. En el cuadro de diálogo **Select Host** que se muestra, seleccione los hosts a los que pertenece el rol y haga clic en **OK**.

Paso 18 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 30 minutos antes y después del tiempo de generación de alarmas respectivamente. A continuación, haga clic en **Download**.

Paso 19 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

Información relacionada

Ninguna

9.241 ALM-45175 El tiempo promedio para invocar a las API de metadatos de OBS es mayor que el umbral

Descripción

El sistema comprueba si la duración promedio para invocar a las API de metadatos de OBS es mayor que el umbral cada 30 segundos. Esta alarma se genera cuando el número de veces consecutivas que el tiempo promedio excede el umbral especificado es mayor que el número de veces de suavizado.

Esta alarma se borra automáticamente cuando la duración promedio para invocar a las API de metadatos de OBS es menor que el umbral.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
45175	Menor	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger Condition	Especifica el umbral para activar la alarma.

Impacto en el sistema

Si el tiempo promedio para invocar a las API de metadatos de OBS excede el umbral, los servicios de computación de big data de capa superior pueden verse afectados. Para ser más específicos, el tiempo de ejecución de algunas tareas informáticas excederá el umbral.

Causas posibles

La congelación de tramas se produce en el servidor OBS o la red entre el cliente OBS y el servidor OBS es inestable.

Procedimiento

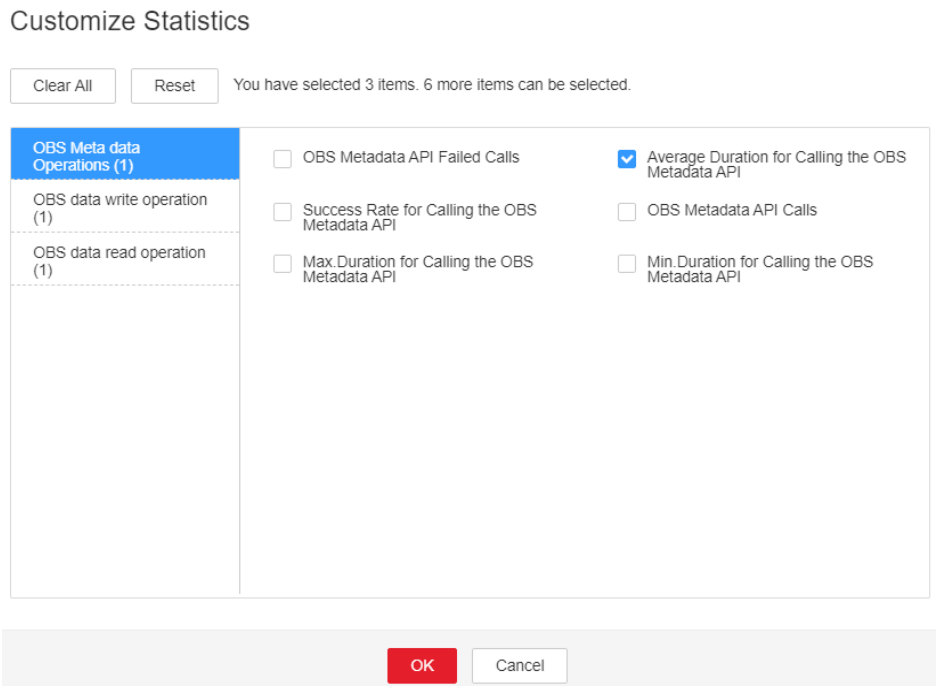
Comprobar el uso de memoria heap.

Paso 1 En la página de inicio **FusionInsight Manager**, elija **O&M** > **Alarm** > **Alarms** > **Average Time for Calling the OBS Metadata API Exceeds the Threshold**, vea el nombre de rol en **Location**, y compruebe la dirección IP de instancia.

Paso 2 Elija **Cluster** > *Name of the desired cluster* > **Services** > **meta** > **Instance** > **meta** (dirección IP de la instancia para la que se genera la alarma). Haga clic en la lista desplegable situada en la esquina superior derecha del área del gráfico y elija **Customize**. En el cuadro de diálogo que se muestra, seleccione **Average time of OBS interface calls** en **OBS Meta data Operations** y haga clic en **OK**. Comprueba si el tiempo promedio de las invocaciones a la API de metadatos de OBS excede el umbral.

- En caso afirmativo, vaya a **Paso 3**.
- Si no, vaya a **Paso 5**.

Figura 9-107 Duración promedio para invocar a la API de metaData de OBS



Paso 3 Elija **Cluster** > *Name of the desired cluster* > **O&M** > **Alarm** > **Thresholds** > **meta** > **Average Time for Calling the OBS Metadata API**. Aumente el umbral o los tiempos de suavizado según sea necesario.

Paso 4 Verifique si la alarma se ha borrado.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 5**.

Recopilar información de fallas.

Paso 5 En FusionInsight Manager, seleccione **O&M**. En el panel de navegación de la izquierda, elija **Log** > **Download**.

Paso 6 En el área **Services**, seleccione **NodeAgent**, **NodeMetricAgent**, **OmmServer** y **OmmAgent** en OMS.

Paso 7 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 30 minutos antes y después del tiempo de generación de alarmas respectivamente. A continuación, haga clic en **Download**.

Paso 8 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

Información relacionada

Ninguna

9.242 ALM-45176 La tasa de éxito de las invocaciones a las API de metadatos de OBS es inferior al umbral

Descripción

El sistema comprueba si la tasa de éxito al invocar a las API de metadatos de OBS es inferior al umbral cada 30 segundos. Esta alarma se genera cuando la tasa de éxito es inferior al umbral.

Esta alarma se borra automáticamente cuando la tasa de éxito de invocaciones a las API para escribir datos OBS es mayor que el umbral.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
45176	Menor	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger Condition	Especifica el umbral para activar la alarma.

Impacto en el sistema

Si la tasa de éxito de invocar a las API de metadatos de OBS es menor que el umbral, los servicios de computación de big data de capa superior pueden verse afectados. Para ser más específicos, es posible que algunas tareas informáticas no se ejecuten.

Causas posibles

Se produce una excepción de ejecución o un tiempo de espera severo en el servidor OBS.

Procedimiento

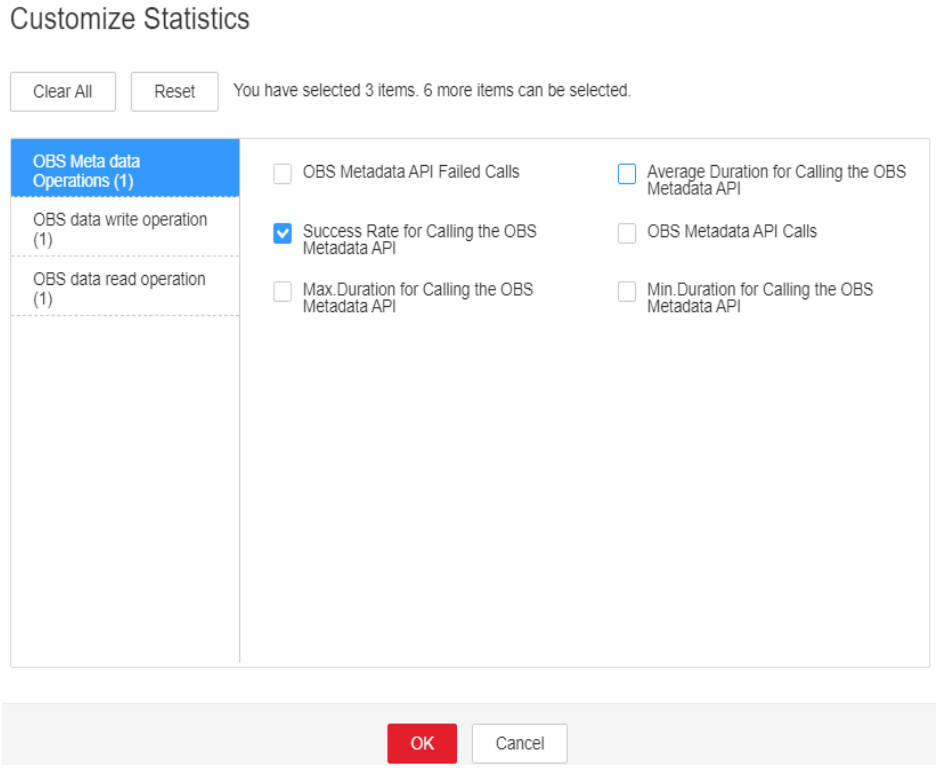
Comprobar el uso de memoria heap.

Paso 1 En la página de inicio **FusionInsight Manager**, elija **O&M** > **Alarm** > **Alarms** > **Success Rate for Calling the OBS Metadata API Is Lower Than the Threshold**, vea el nombre de rol en **Location**, y compruebe la dirección IP de instancia.

Paso 2 Elija **Cluster** > *Name of the desired cluster* > **Services** > **meta** > **Instance** > **meta** (dirección IP de la instancia para la que se genera la alarma). Haga clic en la lista desplegable situada en la esquina superior derecha del área del gráfico y elija **Customize**. En el cuadro de diálogo que se muestra, seleccione **Success percent of OBS interface calls** en **OBS Meta data Operations** y haga clic en **OK**. Comprueba si el tiempo promedio de las invocaciones a la API de metadatos de OBS excede el umbral.

- En caso afirmativo, vaya a **Paso 3**.
- Si no, vaya a **Paso 5**.

Figura 9-108 Tasa de éxito para invocar a la API de OBS



Paso 3 Elija **Cluster** > *Name of the desired cluster* > **O&M** > **Alarm** > **Thresholds** > **meta** > **Success Rate for Calling the OBS Metadata API**. Aumente el umbral o los tiempos de suavizado según sea necesario.

Paso 4 Verifique si la alarma se ha borrado.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 5**.

Recopilar información de fallas.

Paso 5 En FusionInsight Manager, seleccione **O&M**. En el panel de navegación de la izquierda, elija **Log** > **Download**.

Paso 6 En el área **Services**, seleccione **NodeAgent**, **NodeMetricAgent**, **OmmServer** y **OmmAgent** en OMS.

Paso 7 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 30 minutos antes y después del tiempo de generación de alarmas respectivamente. A continuación, haga clic en **Download**.

Paso 8 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

Información relacionada

Ninguna

9.243 ALM-45177 La tasa de éxito de las invocaciones a las API de lectura de datos de OBS es inferior al umbral

Descripción

El sistema comprueba si la tasa de éxito al invocar a las API para leer datos OBS es inferior al umbral cada 30 segundos. Esta alarma se genera cuando la tasa de éxito es inferior al umbral.

Esta alarma se borra automáticamente cuando la tasa de éxito al invocar a las API para leer datos OBS es mayor que el umbral.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
45177	Menor	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.

Nombre	Significado
HostName	Especifica el host para el que se genera la alarma.
Trigger Condition	Especifica el umbral para activar la alarma.

Impacto en el sistema

Si la tasa de éxito de invocar a las API de OBS para leer datos es menor que el umbral, los servicios de computación de big data de capa superior pueden verse afectados. Para ser más específicos, es posible que algunas tareas informáticas no se ejecuten.

Causas posibles

Se produce una excepción de ejecución o un tiempo de espera severo en el servidor OBS.

Procedimiento

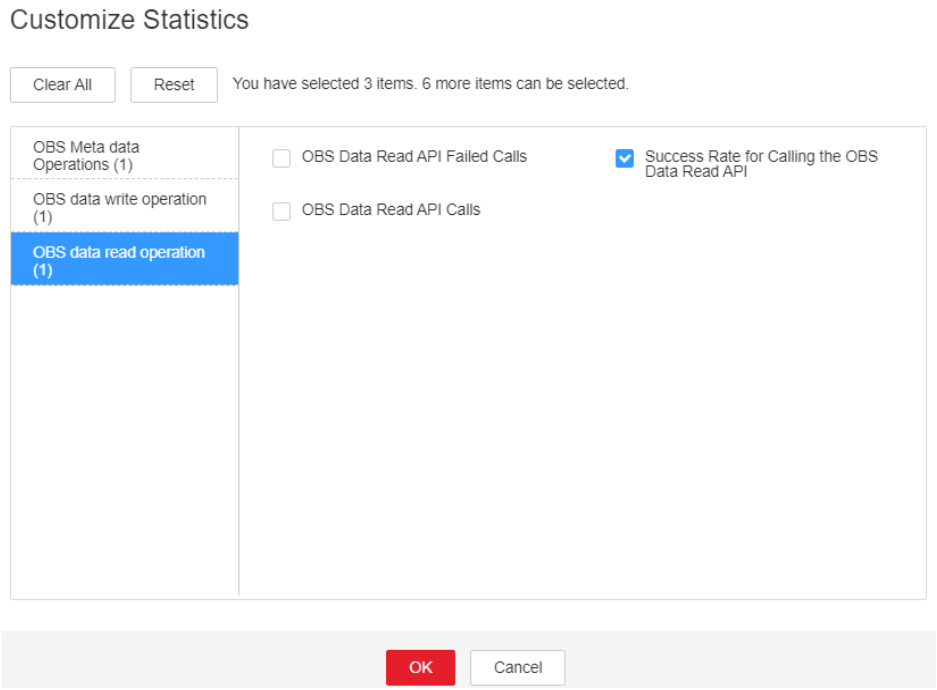
Comprobar el uso de memoria heap.

Paso 1 En la página de inicio **FusionInsight Manager**, Elija **O&M** > **Alarm** > **Alarms** > **Success Rate for Calling the OBS Data Read API Is Lower Than the Threshold**, vea el nombre de rol en **Location**, y compruebe la dirección IP de instancia.

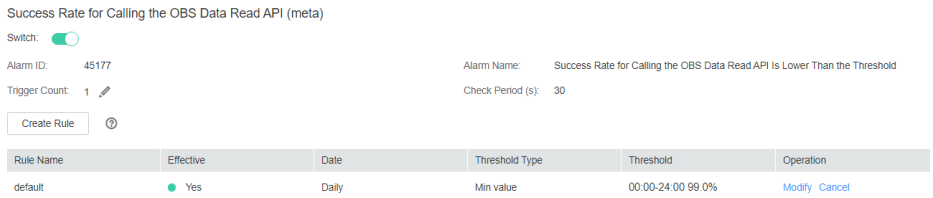
Paso 2 Elija **Cluster** > *Name of the desired cluster* > **Services** > **meta** > **Instance** > **meta** (dirección IP de la instancia para la que se genera la alarma). Haga clic en la lista desplegable situada en la esquina superior derecha del área del gráfico y elija **Customize**. En el cuadro de diálogo que se muestra, seleccione **Success percent of OBS data read operation interface calls** en **OBS data read operation** y haga clic en **OK**. Comprueba si el tiempo promedio de las invocaciones a la API de metadatos de OBS excede el umbral.

- En caso afirmativo, vaya a **Paso 3**.
- Si no, vaya a **Paso 5**.

Figura 9-109 Tasa de éxito para invocar a la API de lectura de datos de OBS



Paso 3 Elija **Cluster** > *Name of the desired cluster* > **O&M** > **Alarm** > **Thresholds** > **meta** > **Success Rate for Calling the OBS Data Read API**. Aumente el umbral o los tiempos de suavizado según sea necesario.



Paso 4 Verifique si la alarma se ha borrado.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 5**.

Recopilar información de fallas.

Paso 5 En FusionInsight Manager, seleccione **O&M**. En el panel de navegación de la izquierda, elija **Log** > **Download**.

Paso 6 En el área **Services**, seleccione **NodeAgent**, **NodeMetricAgent**, **OmmServer** y **OmmAgent** en OMS.

Paso 7 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 30 minutos antes y después del tiempo de generación de alarmas respectivamente. A continuación, haga clic en **Download**.

Paso 8 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

Información relacionada

Ninguna

9.244 ALM-45178 La tasa de éxito de las invocaciones a las API de escritura de datos de OBS es menor que el umbral

Descripción

El sistema comprueba si la tasa de éxito al invocar a las API para escribir datos OBS es menor que el umbral cada 30 segundos. Esta alarma se genera cuando la tasa de éxito es inferior al umbral.

Esta alarma se borra automáticamente cuando la tasa de éxito de invocaciones a las API para escribir datos OBS es mayor que el umbral.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
45178	Menor	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger Condition	Especifica el umbral para activar la alarma.

Impacto en el sistema

Si la tasa de éxito de invocar a las API de OBS para escribir datos es menor que el umbral, los servicios de computación de big data de capa superior pueden verse afectados. Para ser más específicos, es posible que algunas tareas informáticas no se ejecuten.

Causas posibles

Se produce una excepción de ejecución o un tiempo de espera severo en el servidor OBS.

Procedimiento

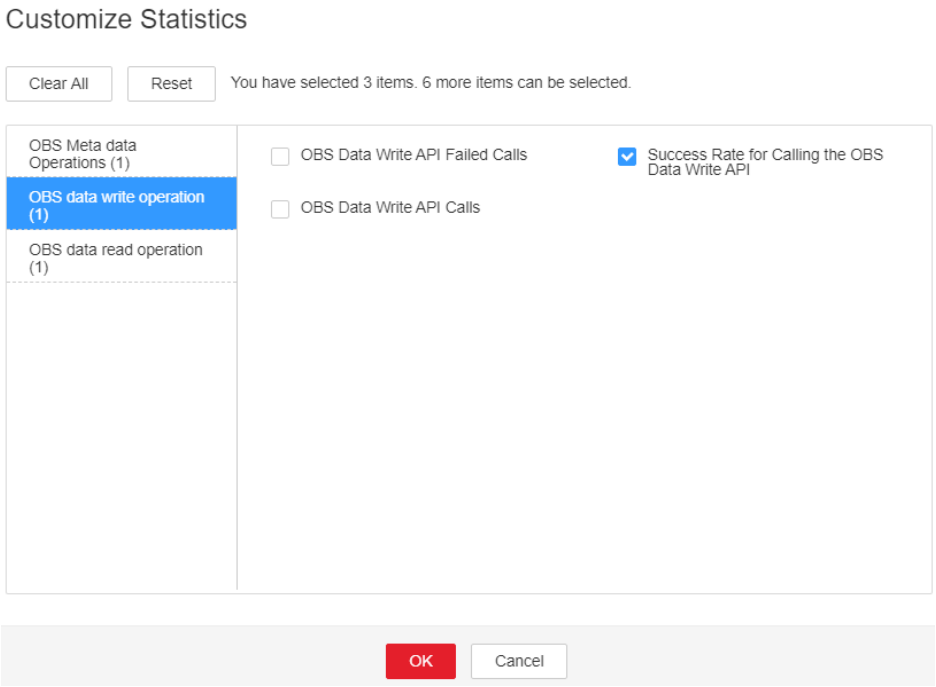
Comprobar el uso de memoria heap.

Paso 1 En la página de inicio **FusionInsight Manager**, elija **O&M** > **Alarm** > **Alarms** > **Success Rate for Calling the OBS Data Write API Is Lower Than the Threshold**, vea el nombre de rol en **Location**, y compruebe la dirección IP de instancia.

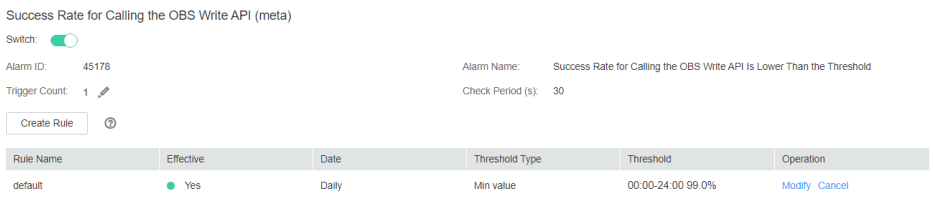
Paso 2 Elija **Cluster** > *Name of the desired cluster* > **Services** > **meta** > **Instance** > **meta** (dirección IP de la instancia para la que se genera la alarma). Haga clic en la lista desplegable situada en la esquina superior derecha del área del gráfico y elija **Customize**. En el cuadro de diálogo que se muestra, seleccione **Success percent of OBS data write operation interface calls** en **OBS data write operation** y haga clic en **OK**. Comprueba si el tiempo promedio de las invocaciones a la API de metadatos de OBS excede el umbral.

- En caso afirmativo, vaya a **Paso 3**.
- Si no, vaya a **Paso 5**.

Figura 9-110 Tasa de éxito para invocar a la API de escritura de datos de OBS



Paso 3 Elija **Cluster** > *Name of the desired cluster* > **O&M** > **Alarm** > **Thresholds** > **meta** > **Success Rate for Calling the OBS Data Write API**. Aumente el umbral o los tiempos de suavizado según sea necesario.



Paso 4 Verifique si la alarma se ha borrado.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 5**.

Recopilar información de fallas.

Paso 5 En FusionInsight Manager, seleccione **O&M**. En el panel de navegación de la izquierda, elija **Log** > **Download**.

Paso 6 En el área **Services**, seleccione **NodeAgent**, **NodeMetricAgent**, **OmmServer** y **OmmAgent** en OMS.

Paso 7 Haga clic en  en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 30 minutos antes y después del tiempo de generación de alarmas respectivamente. A continuación, haga clic en **Download**.

Paso 8 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

Información relacionada

Ninguna

9.245 ALM-45179 Número de invocaciones a la API de OBS readFully supera el umbral

Descripción

El sistema comprueba si el número de invocaciones a la API de OBS readFully fallidas excede el umbral cada 30 segundos. Esta alarma se genera cuando el número de invocaciones a la API fallidas excede el umbral.

Esta alarma se borra automáticamente cuando el número de invocaciones a la API de OBS readFully fallidas es menor que el umbral.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
45179	Menor	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger Condition	Especifica el umbral para activar la alarma.

Impacto en el sistema

Ciertas tareas de computación de big data de capa superior no se ejecutarán.

Causas posibles

Se produce una excepción de ejecución o un tiempo de espera severo en el servidor OBS.

Procedimiento

Paso 1 Inicie sesión en FusionInsight Manager y elija **O&M** > **Alarm** > **Thresholds**. En la página **Thresholds**, elija **meta** > **Number of failed calls to the OBS readFully interface**. En el panel derecho, establezca **Threshold** o **Trigger Count** en un valor mayor según sea necesario.

Paso 2 Verifique si la alarma se ha borrado.

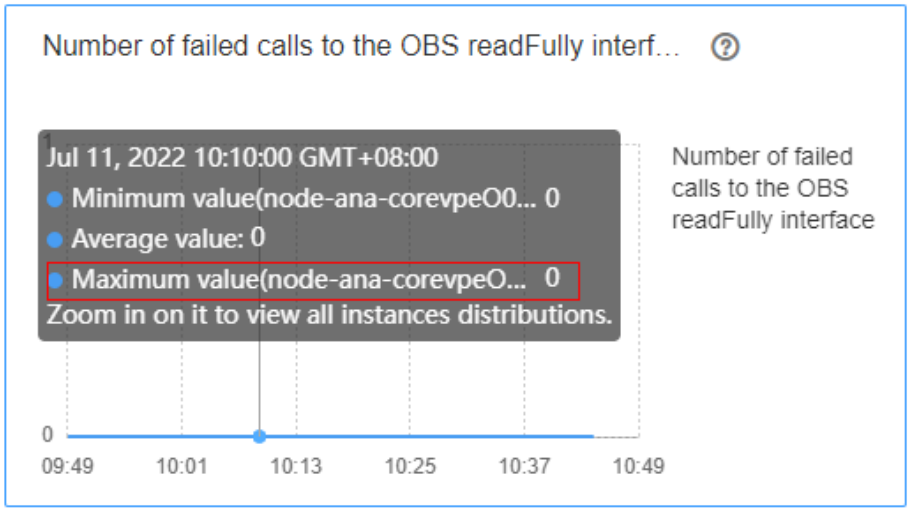
- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 3**.

Paso 3 Póngase en contacto con el de OBS para comprobar si el servicio OBS es normal.

- En caso afirmativo, vaya a **Paso 4**.
- Si no, póngase en contacto con de OBS para restaurar el servicio de OBS.

Recopilar información de fallas.

Paso 4 En FusionInsight Manager, elija **Cluster** > **Services** > **meta**. En la página que se muestra, haga clic en la pestaña **Chart**. En esta página de fichas, seleccione **OBS data read operation** en el área **Chart Category**. En el gráfico **Number of failed calls to the OBS readFully interface-All Instances**, vea el nombre de host de la instancia que tiene el número máximo de invocaciones a la API de OBS readFully fallidas. Por ejemplo, el nombre de host es **node-ana-corevpeO003**.



Paso 5 Elija **O&M** > **Log** > **Download** y seleccione **meta** y **meta** para **Service**.

Paso 6 Seleccione el host obtenido en **Paso 4** para **Hosts**.

Paso 7 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 30 minutos antes y después del tiempo de generación de alarmas respectivamente. A continuación, haga clic en **Download**.

Paso 8 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

Información relacionada

Ninguna

9.246 ALM-45180 Número de invocaciones a la API de OBS read fallidas supera el umbral

Descripción

El sistema comprueba si el número de invocaciones a la API de OBS read fallidas excede el umbral cada 30 segundos. Esta alarma se genera cuando el número de invocaciones a la API fallidas excede el umbral.

Esta alarma se borra automáticamente cuando el número de invocaciones a la API de OBS read fallidas es menor que el umbral.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
45180	Menor	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger Condition	Especifica el umbral para activar la alarma.

Impacto en el sistema

Ciertas tareas de computación de big data de capa superior no se ejecutarán.

Causas posibles

Se produce una excepción de ejecución o un tiempo de espera severo en el servidor OBS.

Procedimiento

Paso 1 Inicie sesión en FusionInsight Manager y elija **O&M** > **Alarm** > **Thresholds**. En la página **Thresholds**, elija **meta** > **Number of failed calls to the OBS read interface**. En el panel derecho, establezca **Threshold** o **Trigger Count** en un valor mayor según sea necesario.

Paso 2 Verifique si la alarma se ha borrado.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 3**.

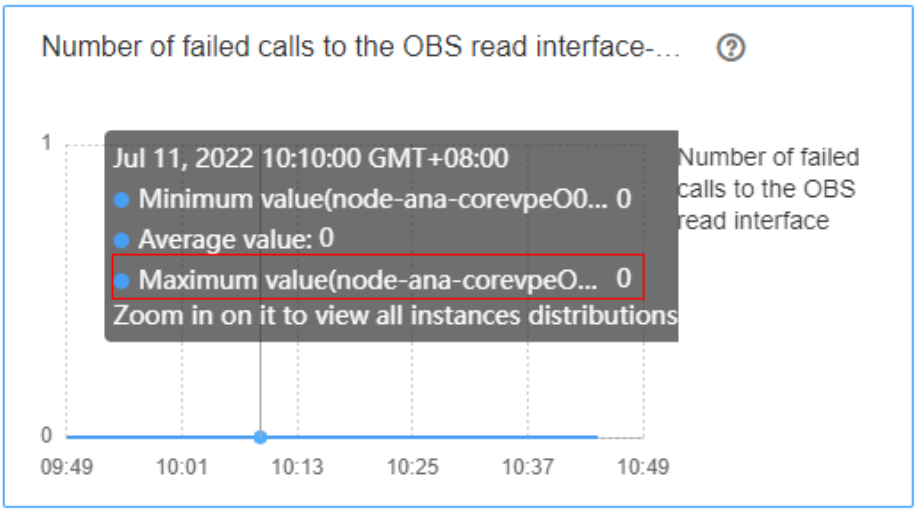
Paso 3 Póngase en contacto con el de OBS para comprobar si el servicio OBS es normal.

- En caso afirmativo, vaya a **Paso 4**.
- Si no, póngase en contacto con de OBS para restaurar el servicio de OBS.

Recopilar información de fallas.

Paso 4 En FusionInsight Manager, elija **Cluster** > **Services** > **meta**. En la página que se muestra, haga clic en la pestaña **Chart**. En esta página de fichas, seleccione **OBS data read operation** en el área **Chart Category**. En el gráfico **Número de invocaciones fallidas a la interfaz de**

read de OBS-Todas las instancias, vea el nombre de host de la instancia que tiene el número máximo de llamadas a la API de lectura de OBS fallidas. Por ejemplo, el nombre de host es **node-ana-corevpeO003**.



Paso 5 Elija **O&M** > **Log** > **Download** y seleccione **meta** y **meta** para **Service**.

Paso 6 Seleccione el host obtenido en **Paso 4** para **Hosts**.

Paso 7 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 30 minutos antes y después del tiempo de generación de alarmas respectivamente. A continuación, haga clic en **Download**.

Paso 8 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

Información relacionada

Ninguna

9.247 ALM-45181 El número de invocaciones a la API de OBS write fallidas supera el umbral

Descripción

El sistema comprueba si el número de invocaciones a la API de OBS write fallidas excede el umbral cada 30 segundos. Esta alarma se genera cuando el número de invocaciones a la API fallidas excede el umbral.

Esta alarma se borra automáticamente cuando el número de invocaciones a la API de OBS write fallidas es menor que el umbral.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
45181	Menor	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger Condition	Especifica el umbral para activar la alarma.

Impacto en el sistema

Ciertas tareas de computación de big data de capa superior no se ejecutarán.

Causas posibles

Se produce una excepción de ejecución o un tiempo de espera severo en el servidor OBS.

Procedimiento

Paso 1 Inicie sesión en FusionInsight Manager y elija **O&M** > **Alarm** > **Thresholds**. En la página **Thresholds**, elija **meta** > **Number of failed calls to the OBS write interface**. En el panel derecho, establezca **Threshold** o **Trigger Count** en un valor mayor según sea necesario.

Paso 2 Verifique si la alarma se ha borrado.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 3**.

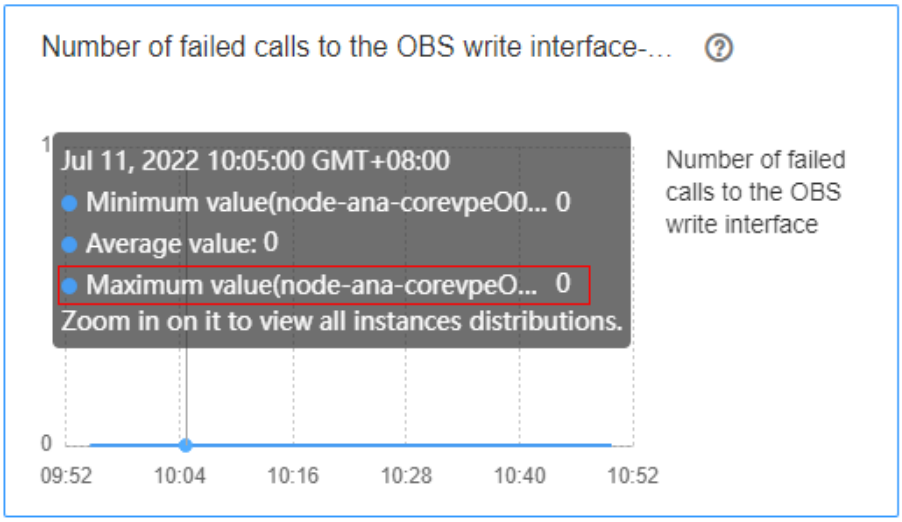
Paso 3 Póngase en contacto con el de OBS para comprobar si el servicio OBS es normal.

- En caso afirmativo, vaya a **Paso 4**.
- Si no, póngase en contacto con de OBS para restaurar el servicio de OBS.

Recopilar información de fallas.

Paso 4 En FusionInsight Manager, elija **Cluster** > **Services** > **meta**. En la página que se muestra, haga clic en la pestaña **Chart**. En esta página de pestaña, seleccione **OBS data write operation** en el área **Chart Category**. En el gráfico **Number of failed calls to the OBS**

write interface-All Instances, vea el nombre de host de la instancia que tiene el número máximo de invocaciones a la API de OBS write fallidas. Por ejemplo, el nombre de host es **node-ana-corevpeO003**.



Paso 5 Elija **O&M** > **Log** > **Download** y seleccione **meta** y **meta** para **Service**.

Paso 6 Seleccione el host obtenido en **Paso 4** para **Hosts**.

Paso 7 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 30 minutos antes y después del tiempo de generación de alarmas respectivamente. A continuación, haga clic en **Download**.

Paso 8 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

Información relacionada

Ninguna

9.248 ALM-45182 El número de operaciones de OBS limitadas supera el umbral

Descripción

El sistema comprueba si el número de operaciones de OBS limitadas excede el umbral cada 30 segundos. Esta alarma se genera cuando el número de operaciones de OBS limitadas excede el umbral.

Esta alarma se borra automáticamente cuando el número de operaciones de OBS limitadas es menor que el umbral.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
45182	Menor	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger Condition	Especifica el umbral para activar la alarma.

Impacto en el sistema

Ciertas tareas de computación de big data de capa superior no se ejecutarán.

Causas posibles

La frecuencia de solicitud de API de OBS es demasiado alta.

Procedimiento

Paso 1 Inicie sesión en FusionInsight Manager y elija **O&M** > **Alarm** > **Thresholds**. En la página **Thresholds**, elija **meta** > **Number of Throttled OBS Operations**. En el panel derecho, establezca **Threshold** o **Trigger Count** en un valor mayor según sea necesario.

Paso 2 Verifique si la alarma se ha borrado.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 3**.

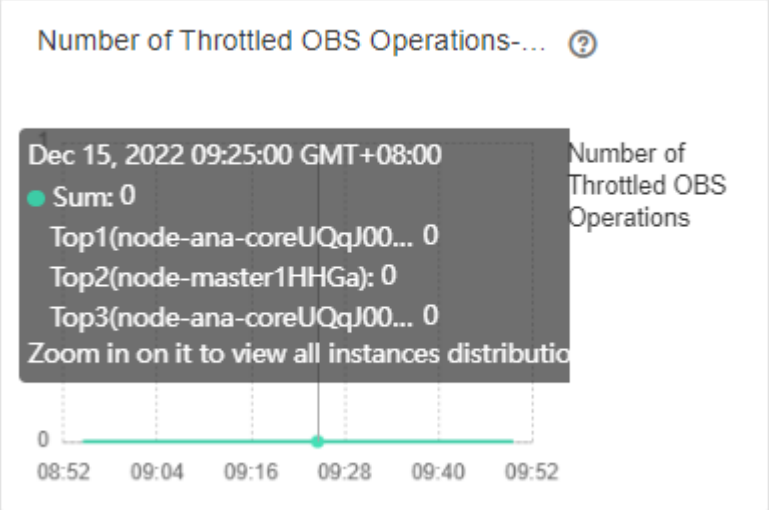
Paso 3 Póngase en contacto con el de OBS para comprobar si el servicio OBS es normal.

- En caso afirmativo, vaya a **Paso 4**.
- Si no, póngase en contacto con de OBS para restaurar el servicio de OBS.

Recopilar información de fallas.

Paso 4 En FusionInsight Manager, elija **Cluster** > **Services** > **meta**. En la página que se muestra, haga clic en la pestaña **Chart**. En esta página de fichas, seleccione **OBS Throttled** en el área **Chart Category**. En el gráfico **Number of Throttled OBS Operations-All Instances**, vea el

nombre de host de la instancia que tiene el número máximo de invocadas a la API de OBS limitadas. Por ejemplo, el nombre de host es **node-ana-coreUQqJ0002**.



Paso 5 Elija **O&M** > **Log** > **Download** y seleccione **meta** y **meta** para **Service**.

Paso 6 Seleccione el host obtenido en **Paso 4** para **Hosts**.

Paso 7 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 30 minutos antes y después del tiempo de generación de alarmas respectivamente. A continuación, haga clic en **Download**.

Paso 8 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

Información relacionada

Ninguna

9.249 ALM-45275 Servicio Ranger no disponible

Descripción

El módulo de alarma comprueba el estado del servicio Ranger cada 180 segundos. Esta alarma se genera si el servicio Ranger es anormal.

Esta alarma se borra después de que se recupere el servicio Ranger.

Atributos

ID de alarma	Severidad de alarma	Borrado automáticamente
45275	Crítica	Sí

Parámetros

Nombre	Significado
Source	Clúster para el que se genera la alarma.
ServiceName	Servicio para el que se genera la alarma.
RoleName	Rol para el que se genera la alarma.
HostName	Host para el que se genera la alarma.

Impacto en el sistema

Cuando el servicio Ranger no está disponible, Ranger no puede funcionar correctamente y no se puede acceder a la interfaz de usuario nativa de Ranger.

Causas posibles

- El servicio DBService del que depende Ranger es anormal.
- La instancia de rol RangerAdmin es anormal.

Procedimiento

Comprobar el estado de proceso DBService.

Paso 1 En FusionInsight Manager, seleccione **O&M** > **Alarm** > **Alarms**. En la página que se muestra, compruebe si se notifica la alarma ALM-27001 Servicio DBService no disponible.

- En caso afirmativo, vaya a **Paso 2**.
- Si no, vaya a **Paso 3**.

Paso 2 Rectifique el error de servicio DBService siguiendo el procedimiento de manejo de ALM-27001 Servicio DBService no disponible. Una vez borrada la alarma DBService, compruebe si la alarma del servicio Ranger no disponible está borrada.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 3**.

Comprobar todas las instancias de RangerAdmin.

Paso 3 Inicie sesión en el nodo donde se encuentra la instancia RangerAdmin como usuario **omm** y ejecute el comando **ps -ef|grep "proc_RangerAdmin"** para comprobar si el proceso RangerAdmin existe en el nodo actual.

- En caso afirmativo, vaya a **Paso 5**.

- Si no, reinicie la instancia de RangerAdmin o el servicio Ranger defectuosos y vaya a **Paso 4**.

Paso 4 En la lista de alarmas, compruebe si la alarma "Servicio Range No Disponible" está desactivada.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 5**.

Recopilar información de fallas.

Paso 5 En FusionInsight Manager, elija **O&M** > **Log** > **Download**.

Paso 6 Expanda la lista desplegable **Service** y seleccione **Ranger** para el clúster de destino.

Paso 7 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 1 hora antes y después del tiempo de generación de alarma, respectivamente. A continuación, haga clic en **Download**.

Paso 8 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar el fallo que activa la alarma, la alarma se borra automáticamente.

Información relacionada

Ninguna

9.250 ALM-45276 Estado anormal de RangerAdmin

Descripción

El módulo de alarma comprueba el estado del servicio RangerAdmin cada 60 segundos. Esta alarma se genera si RangerAdmin no está disponible.

Esta alarma se borra automáticamente una vez que se recupera el servicio RangerAdmin.

Atributos

ID de alarma	Severidad de alarma	Borrado automáticamente
45276	Grave	Sí

Parámetros

Nombre	Significado
Source	Clúster para el que se genera la alarma.

Nombre	Significado
ServiceName	Servicio para el que se genera la alarma.
RoleName	Rol para el que se genera la alarma.
HostName	Host para el que se genera la alarma.

Impacto en el sistema

Si el estado de un RangerAdmin es anormal, el acceso a la interfaz de usuario nativa de Ranger no se ve afectado. Si hay dos instancias de RangerAdmin anormales, no se puede acceder a la interfaz de usuario nativa de Ranger y las operaciones como crear, modificar y eliminar políticas no están disponibles.

Causas posibles

El puerto RangerAdmin no se inicia.

Procedimiento

Comprobar el proceso de puerto.

Paso 1 En la lista de alarmas del FusionInsight Manager, busque la fila que contiene la alarma y haga clic en ⌄ para ver el nombre del host para el que se genera la alarma.

Paso 2 Inicie sesión en el nodo donde se encuentra la instancia RangerAdmin como usuario **omm**. Ejecute el comando **ps -ef|grep "proc_RangerAdmin" | grep -v grep | awk -F ' ' '{print $2}'** para obtener el ***pid*** del proceso RangerAdmin y ejecute el comando **netstat -anp|grep *pid* | grep LISTEN** para comprobar si el proceso RangerAdmin escucha el puerto 21401 en el modo de seguridad y el puerto 21400 en el modo estándar.

- En caso afirmativo, vaya a **Paso 4**.
- Si no, reinicie la instancia de RangerAdmin o el servicio Ranger defectuosos y vaya a **Paso 3**.

Paso 3 En la lista de alarmas, compruebe si la alarma "Estado anormal de RangerAdmin" está desactivada.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 4**.

Recopilar información de fallas.

Paso 4 En FusionInsight Manager, elija **O&M** > **Log** > **Download**.

Paso 5 Expanda la lista desplegable **Service** y seleccione **Ranger** para el clúster de destino.

Paso 6 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 1 hora antes y después del tiempo de generación de alarma, respectivamente. A continuación, haga clic en **Download**.

Paso 7 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar el fallo que activa la alarma, la alarma se borra automáticamente.

Información relacionada

Ninguna

9.251 ALM-45277 El uso de memoria heap de RangerAdmin supera el umbral

Descripción

El sistema comprueba el uso de memoria heap del servicio RangerAdmin cada 60 segundos. Esta alarma se genera cuando el sistema detecta que el uso de memoria heap de la instancia RangerAdmin excede el umbral (95% de la memoria máxima) durante 10 veces consecutivas. Esta alarma se borra cuando el uso de memoria heap es menor que el umbral.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
45277	Grave	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger Condition	Especifica el umbral para activar la alarma.

Impacto en el sistema

El desbordamiento de la memoria heap puede causar una falla en el servicio.

Causas posibles

El uso de memoria heap de la instancia RangerAdmin es alto o la memoria heap está asignada incorrectamente.

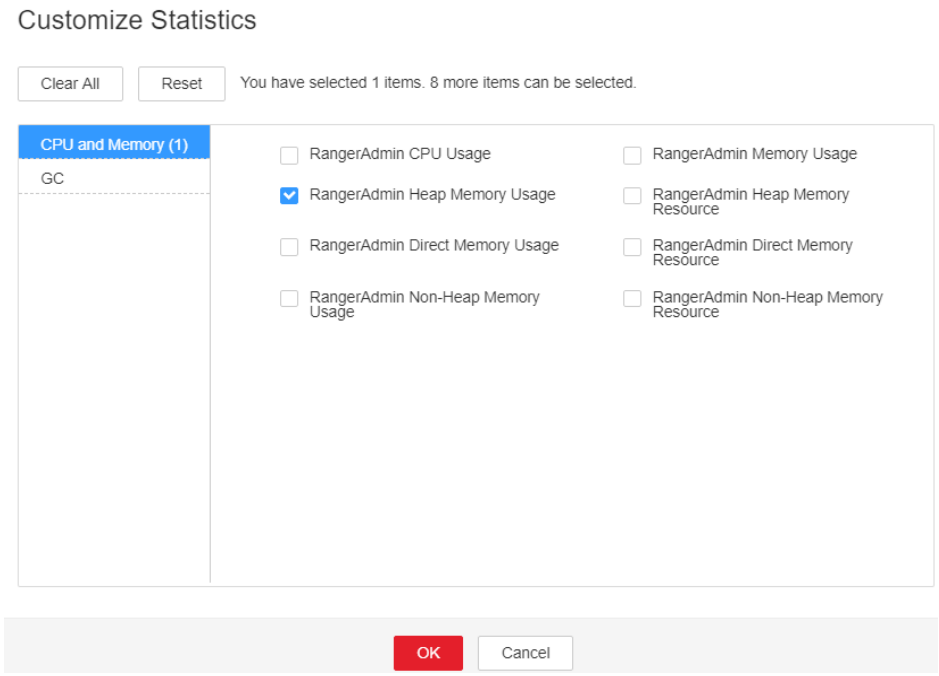
Procedimiento

Comprobar el uso de memoria heap.

Paso 1 En FusionInsight Manager, elija **O&M** > **Alarm** > **Alarms** > **ALM-45277 RangerAdmin Heap Memory Usage Exceeds the Threshold**. Compruebe la información de ubicación de la alarma y vea el nombre de host de la instancia para la que se genera la alarma.

Paso 2 En FusionInsight Manager, seleccione **Cluster** > **Services** > **Ranger** > **Instance**. Seleccione el rol correspondiente al nombre de host de la instancia para la que se genera la alarma. Haga clic en la lista desplegable situada en la esquina superior derecha del área del gráfico y elija **Customize** > **CPU and Memory** > **RangerAdmin Heap Memory Usage**. Haga clic en **OK**.

Figura 9-111 Uso de memoria heap de RangerAdmin



Paso 3 Compruebe si la memoria heap utilizada por RangerAdmin alcanza el umbral (95% de la memoria heap máxima de forma predeterminada).

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 6**.

Paso 4 En FusionInsight Manager, seleccione **Cluster** > **Services** > **Ranger** > **Instance** > **RangerAdmin** > **Instance Configuration**. Haga clic en **All Configurations** y elija **RangerAdmin** > **System**. Aumente el valor de **-Xmx** en el parámetro **GC_OPTS** según los requisitos del sitio y guarde la configuración.

NOTA

Si se genera esta alarma, la memoria heap configurada para RangerAdmin no puede cumplir con la memoria heap requerida por el proceso RangerAdmin. Se recomienda comprobar el uso de la memoria heap de RangerAdmin y cambiar el valor de **-Xmx** en **GC_OPTS** a las dos veces de la memoria heap utilizada por RangerAdmin. El valor se puede cambiar en función del escenario de servicio real. Para obtener más información, consulte **Paso 2**.

Paso 5 Reinicie los servicios o instancias afectados y compruebe si la alarma está desactivada.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 6**.

Recopilar información de fallas.

Paso 6 En FusionInsight Manager, seleccione **O&M**. En el panel de navegación de la izquierda, elija **Log** > **Download**.

Paso 7 Expanda la lista desplegable **Service** y seleccione **Ranger** para el clúster de destino.

Paso 8 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 9 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

Información relacionada

Ninguna

9.252 ALM-45278 El uso de memoria directa de RangerAdmin supera el umbral

Descripción

El sistema comprueba el uso directo de memoria del servicio RangerAdmin cada 60 segundos. Esta alarma se genera cuando el uso de memoria directa de la instancia RangerAdmin supera el umbral (80% de la memoria máxima) durante cinco veces consecutivas. Esta alarma se borra cuando el uso de memoria directa de RangerAdmin es menor o igual que el umbral.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
45278	Grave	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger Condition	Especifica el umbral para activar la alarma.

Impacto en el sistema

El desbordamiento de la memoria directa puede provocar una falla en el servicio.

Causas posibles

La memoria directa de la instancia RangerAdmin se utiliza en exceso o la memoria directa se asigna de forma inapropiada. Como resultado, el uso de memoria excede el umbral.

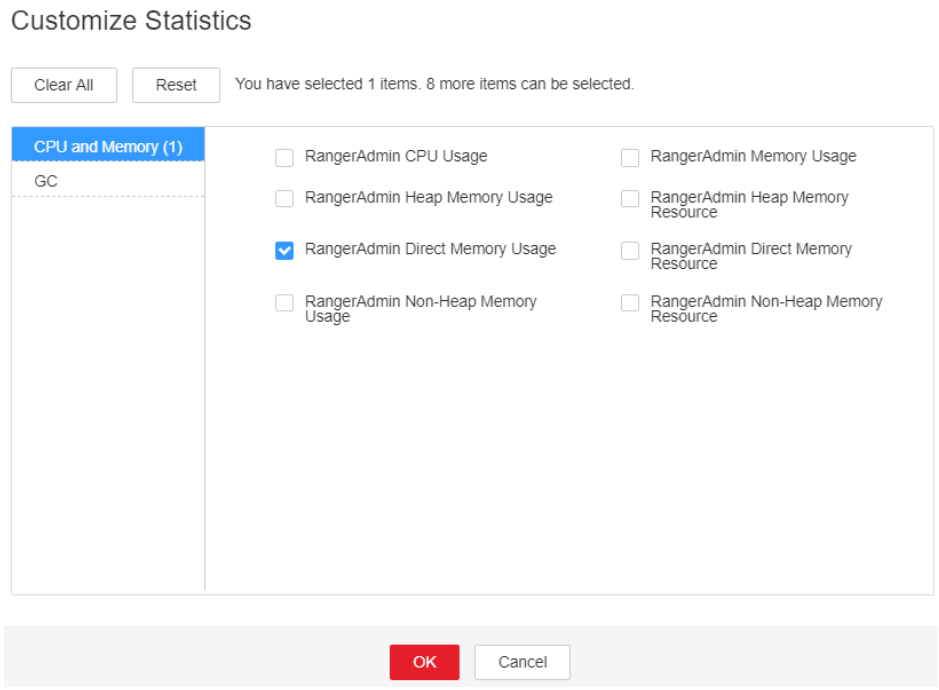
Procedimiento

Comprobar el uso de la memoria directa.

Paso 1 En FusionInsight Manager, elija **O&M** > **Alarm** > **Alarms** > **ALM-45278 RangerAdmin Direct Memory Usage Exceeds the Threshold**. Compruebe la información de ubicación de la alarma y vea el nombre de host de la instancia para la que se genera la alarma.

Paso 2 En FusionInsight Manager, seleccione **Cluster** > **Services** > **Ranger** > **Instance**. Seleccione el rol correspondiente al nombre de host de la instancia para la que se genera la alarma. Haga clic en la lista desplegable situada en la esquina superior derecha del área del gráfico y elija **Customize** > **CPU and Memory** > **RangerAdmin Direct Memory Usage**. Haga clic en **OK**.

Figura 9-112 Uso de memoria directa de RangerAdmin



Paso 3 Compruebe si la memoria directa utilizada por RangerAdmin alcanza el umbral (80% de la memoria directa máxima por defecto).

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 6**.

Paso 4 En FusionInsight Manager, seleccione **Cluster** > **Services** > **Ranger** > **Instance** > **RangerAdmin** > **Instance Configuration**. Haga clic en **All Configurations** y elija **RangerAdmin** > **System**. Aumente el valor de **-XX:MaxDirectMemorySize** en el parámetro **GC_OPTS** según los requisitos del sitio y guarde la configuración.

NOTA

Si se genera esta alarma, la memoria directa configurada para RangerAdmin no puede cumplir con la memoria directa requerida por el proceso RangerAdmin. Se recomienda comprobar el uso directo de memoria de RangerAdmin y cambiar el valor de **-XX:MaxDirectMemorySize** en **GC_OPTS** al doble de la memoria directa utilizada por RangerAdmin. Puede cambiar el valor en función del escenario de servicio real. Para obtener más información, consulte **Paso 2**.

Paso 5 Reinicie los servicios o instancias afectados y compruebe si la alarma está desactivada.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 6**.

Recopilar información de fallas.

Paso 6 En FusionInsight Manager, seleccione **O&M**. En el panel de navegación de la izquierda, elija **Log** > **Download**.

Paso 7 Expanda la lista desplegable **Service** y seleccione **Ranger** para el clúster de destino.

Paso 8 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 9 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

Información relacionada

Ninguna

9.253 ALM-45279 El uso de memoria no heap de RangerAdmin supera el umbral

Descripción

El sistema comprueba el uso de memoria no heap del servicio RangerAdmin cada 60 segundos. Esta alarma se genera cuando el uso de memoria no heap de la instancia RangerAdmin excede el umbral (80% de la memoria máxima) durante cinco veces consecutivas. Esta alarma se borra cuando el uso de memoria no heap es menor que el umbral.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
45279	Grave	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger Condition	Especifica el umbral para activar la alarma.

Impacto en el sistema

El desbordamiento de la memoria no heap puede provocar una falla en el servicio.

Causas posibles

El uso de memoria no-heap de la instancia RangerAdmin es alto o la memoria no-heap está asignada incorrectamente.

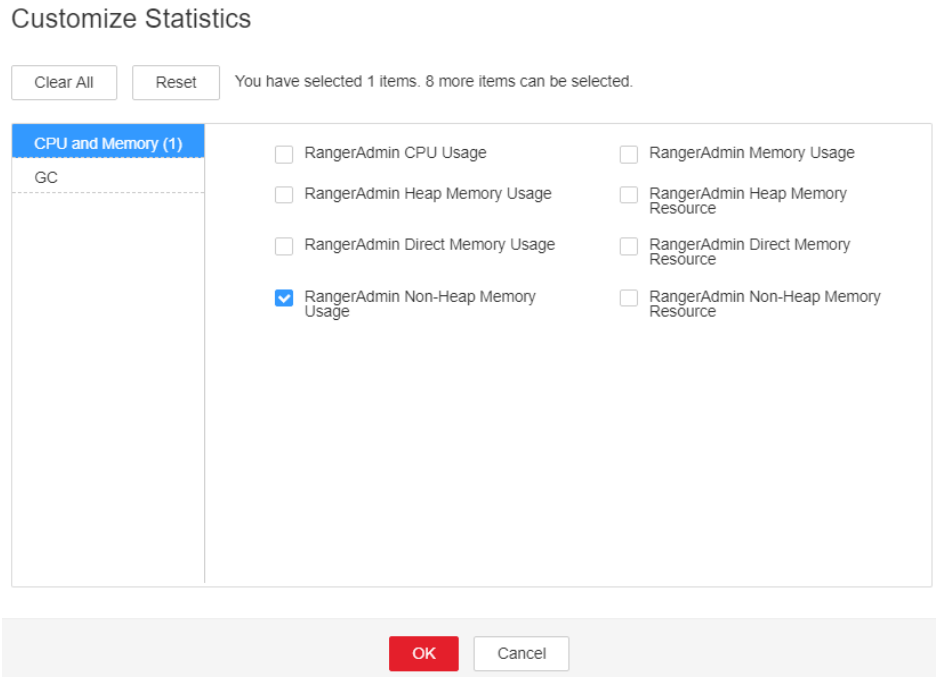
Procedimiento

Comprobar el uso de memoria no heap.

Paso 1 En FusionInsight Manager, elija **O&M** > **Alarm** > **Alarms** > **ALM-45279 RangerAdmin Non Heap Memory Usage Exceeds the Threshold**. Compruebe la información de ubicación de la alarma y vea el nombre de host de la instancia para la que se genera la alarma.

Paso 2 En FusionInsight Manager, seleccione **Cluster** > **Services** > **Ranger** > **Instance**. Seleccione el rol correspondiente al nombre de host de la instancia para la que se genera la alarma. Haga clic en la lista desplegable situada en la esquina superior derecha del área del gráfico y elija **Customize** > **CPU and Memory** > **RangerAdmin Non Heap Memory Usage**. Haga clic en **OK**.

Figura 9-113 Uso de memoria no heap de RangerAdmin



Paso 3 Compruebe si la memoria no heap utilizada por RangerAdmin alcanza el umbral (80% de la memoria máxima no heap de forma predeterminada).

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 6**.

Paso 4 En FusionInsight Manager, seleccione **Cluster** > **Services** > **Ranger** > **Instance** > **RangerAdmin** > **Instance Configuration**. Haga clic en **All Configurations** y elija **RangerAdmin** > **System**. Establezca **-XX: MaxPermSize** en el parámetro **GC_OPTS** a un valor mayor según los requisitos del sitio y guarde la configuración.

NOTA

Si se genera esta alarma, el tamaño de memoria no heap configurado para la instancia RangerAdmin no puede cumplir con la memoria no heap requerida por el proceso RangerAdmin. Se recomienda cambiar el valor de **-XX:MaxPermSize** en el **GC_OPTS** al doble del uso actual de memoria no en pila o cambiar el valor en función de los requisitos del sitio.

Paso 5 Reinicie los servicios o instancias afectados y compruebe si la alarma está desactivada.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 6**.

Recopilar información de fallas.

Paso 6 En FusionInsight Manager, seleccione **O&M**. En el panel de navegación de la izquierda, elija **Log** > **Download**.

Paso 7 Expanda la lista desplegable **Service** y seleccione **Ranger** para el clúster de destino.

Paso 8 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 9 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

Información relacionada

Ninguna

9.254 ALM-45280 La duración de GC de RangerAdmin supera el umbral

Descripción

El sistema comprueba la duración de GC del proceso RangerAdmin cada 60 segundos. Esta alarma se genera cuando la duración de GC del proceso RangerAdmin excede el umbral (12 segundos por defecto) durante cinco veces consecutivas. Esta alarma se borra cuando la duración de GC es menor que el umbral.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
45280	Grave	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger Condition	Especifica el umbral para activar la alarma.

Impacto en el sistema

El RangerAdmin responde lentamente.

Causas posibles

La memoria heap de la instancia RangerAdmin se utiliza en exceso o la memoria heap se asigna de forma inadecuada. Como resultado, los GC ocurren con frecuencia.

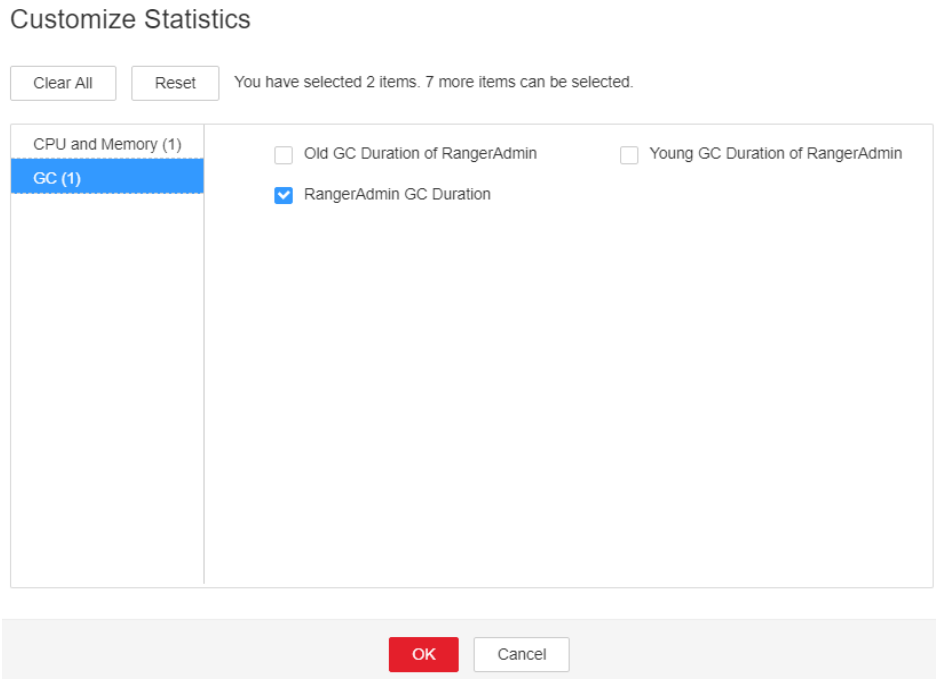
Procedimiento

Comprobar la duración del GC.

Paso 1 En FusionInsight Manager, choose **O&M** > **Alarm** > **Alarms** > **ALM-45280 RangerAdmin GC Duration Exceeds the Threshold**. Compruebe la información de ubicación de la alarma y vea el nombre de host de la instancia para la que se genera la alarma.

Paso 2 En FusionInsight Manager, seleccione **Cluster** > **Services** > **Ranger** > **Instance**. Seleccione el rol correspondiente al nombre de host de la instancia para la que se genera la alarma y haga clic en la lista desplegable en la esquina superior derecha del área del gráfico. Elija **Customize** >**GC** > **RangerAdmin GC Duration**. Haga clic en **OK**.

Figura 9-114 Duración de la recolección de basura (GC) de RangerAdmin



Paso 3 Compruebe si la duración GC del proceso RangerAdmin recopilado cada minuto supera el umbral (12 segundos por defecto).

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 6**.

Paso 4 En FusionInsight Manager, seleccione **Cluster** > **Services** > **Ranger** > **Instance** > **RangerAdmin** > **Instance Configuration**. Haga clic en **All Configurations** y elija **RangerAdmin** > **System**. Aumente el valor de **-Xmx** en el parámetro **GC_OPTS** según los requisitos del sitio y guarde la configuración.

NOTA

Si se genera esta alarma, la memoria heap configurada para RangerAdmin no puede cumplir con la memoria heap requerida por el proceso RangerAdmin. Se recomienda comprobar el uso de la memoria heap de RangerAdmin y cambiar el valor de **-Xmx** en **GC_OPTS** a las dos veces de la memoria heap utilizada por RangerAdmin. El valor se puede cambiar en función del escenario de servicio real. Para obtener más información, consulte **Paso 2**.

Paso 5 Reinicie los servicios o instancias afectados y compruebe si la alarma está desactivada.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 6**.

Recopilar información de fallas.

Paso 6 En FusionInsight Manager, seleccione **O&M**. En el panel de navegación de la izquierda, elija **Log** > **Download**.

Paso 7 Expanda la lista desplegable **Service** y seleccione **Ranger** para el clúster de destino.

Paso 8 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 9 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

Información relacionada

Ninguna

9.255 ALM-45281 El uso de memoria heap de UserSync supera el umbral

Descripción

El sistema comprueba el uso de memoria heap del servicio UserSync cada 60 segundos. Esta alarma se genera cuando el sistema detecta que el uso de memoria heap de la instancia UserSync excede el umbral (95% de la memoria máxima) durante 10 veces consecutivas. Esta alarma se borra cuando el uso de memoria heap es menor que el umbral.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
45281	Grave	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger Condition	Especifica el umbral para activar la alarma.

Impacto en el sistema

El desbordamiento de la memoria heap puede causar una falla en el servicio.

Causas posibles

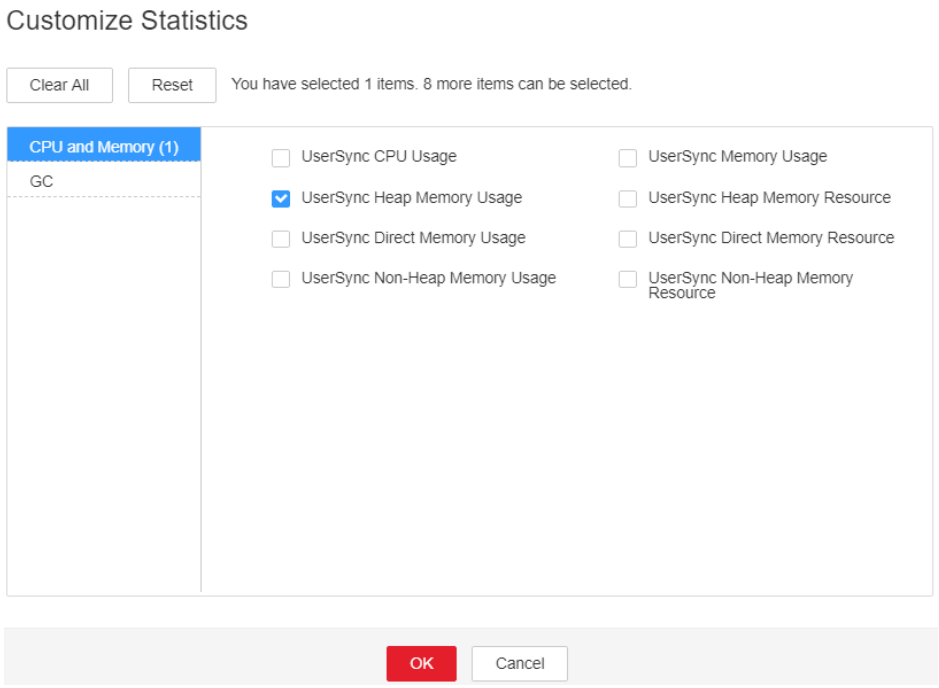
El uso de memoria heap de la instancia UserSync es alto o la memoria heap está asignada incorrectamente.

Procedimiento

Paso 1 En FusionInsight Manager, elija **O&M** > **Alarm** > **Alarms** > **ALM-45281 UserSync Heap Memory Usage Exceeds the Threshold**. Compruebe la información de ubicación de la alarma y vea el nombre de host de la instancia para la que se genera la alarma.

Paso 2 En FusionInsight Manager, seleccione **Cluster** > **Services** > **Ranger** > **Instance**. Seleccione el rol correspondiente al nombre de host de la instancia para la que se genera la alarma. Haga clic en la lista desplegable situada en la esquina superior derecha del área del gráfico y elija **Customize** > **CPU and Memory** > **UserSync Heap Memory Usage**. Haga clic en **OK**.

Figura 9-115 Uso de memoria heap de UserSync



Paso 3 Compruebe si la memoria heap utilizada por UserSync alcanza el umbral (95% de la memoria heap máxima de forma predeterminada).

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 6**.

Paso 4 En FusionInsight Manager, elija **Cluster** > **Services** > **Ranger** > **Instance** > **UserSync** > **Instance Configuration**. Haga clic en **All Configurations** y elija **UserSync** > **System**. Aumente el valor de **-Xmx** en el parámetro **GC_OPTS** según los requisitos del sitio y guarde la configuración.

NOTA

Si se genera esta alarma, la memoria heap configurada para UserSync no puede cumplir con la memoria heap requerida por el proceso UserSync. Se recomienda cambiar el valor **-Xmx** de **GC_OPTS** a dos veces el de la memoria heap utilizada por UserSync. Puede cambiar el valor en función del escenario de servicio real. Para obtener más información acerca de cómo comprobar el uso de la memoria heap de UserSync, consulte **Paso 2**.

Paso 5 Reinicie los servicios o instancias afectados y compruebe si la alarma está desactivada.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 6**.

Recopilar información de fallas.

Paso 6 En FusionInsight Manager, seleccione **O&M**. En el panel de navegación de la izquierda, elija **Log** > **Download**.

Paso 7 Expanda la lista desplegable **Service** y seleccione **Ranger** para el clúster de destino.

Paso 8 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 9 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

Información relacionada

Ninguna

9.256 ALM-45282 El uso de memoria directa de UserSync supera el umbral

Descripción

El sistema comprueba el uso de memoria directa del servicio UserSync cada 60 segundos. Esta alarma se genera cuando el uso de memoria directa de la instancia UserSync supera el umbral (80% de la memoria máxima) durante cinco veces consecutivas. Esta alarma se borra cuando el uso de memoria directa UserSync es menor o igual que el umbral.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
45282	Grave	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger Condition	Especifica el umbral para activar la alarma.

Impacto en el sistema

El desbordamiento de la memoria directa puede provocar una falla en el servicio.

Causas posibles

La memoria directa de la instancia UserSync se utiliza en exceso o la memoria directa se asigna de forma inapropiada. Como resultado, el uso de memoria excede el umbral.

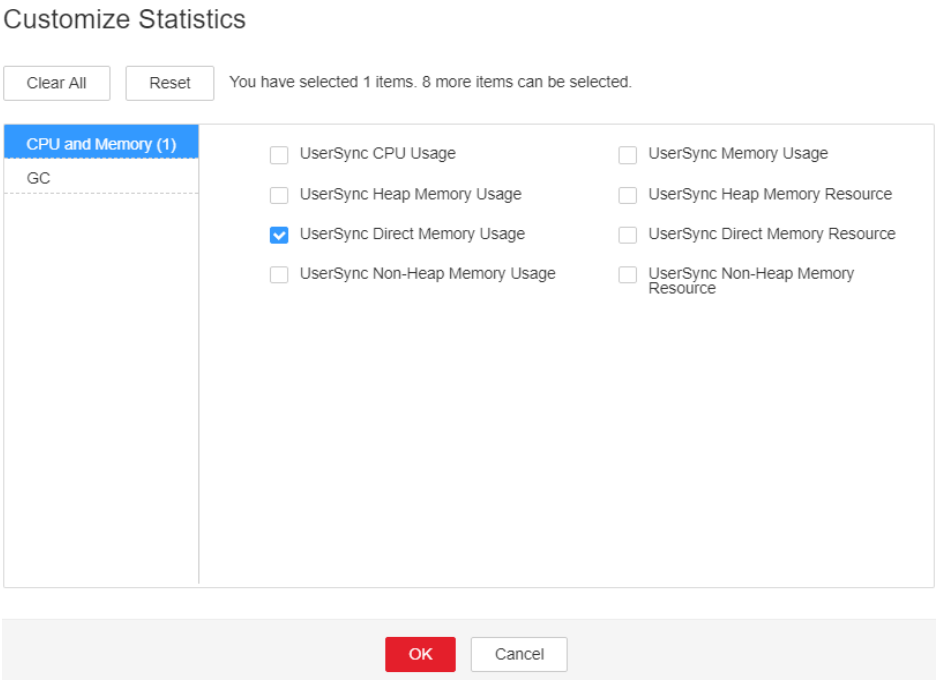
Procedimiento

Comprobar el uso de la memoria directa.

Paso 1 En FusionInsight Manager, elija **O&M** > **Alarm** > **Alarms** > **ALM-45282 UserSync Direct Memory Usage Exceeds the Threshold**. Compruebe la información de ubicación de la alarma. Compruebe el nombre del host de instancia para el que se genera la alarma.

Paso 2 En FusionInsight Manager, seleccione **Cluster** > **Services** > **Ranger** > **Instance**. Seleccione el rol correspondiente al nombre de host de la instancia para la que se genera la alarma. Haga clic en la lista desplegable situada en la esquina superior derecha del área del gráfico y elija **Customize** > **CPU and Memory** > **UserSync Direct Memory Usage**. Haga clic en **OK**.

Figura 9-116 Uso de memoria directa de UserSync



Paso 3 Compruebe si la memoria directa utilizada por el UserSync alcanza el umbral (80% de la memoria directa máxima por defecto).

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 6**.

Paso 4 En FusionInsight Manager, elija **Cluster** > **Services** > **Ranger** > **Instance** > **UserSync** > **Instance Configuration**. Haga clic en **All Configurations** y elija **UserSync** > **System**. Aumente el valor de **-XX:MaxDirectMemorySize** en el parámetro **GC_OPTS** según los requisitos del sitio y guarde la configuración.

NOTA

Si se genera esta alarma, la memoria directa configurada para UserSync no puede cumplir con la memoria directa requerida por el proceso UserSync. Se recomienda comprobar el uso directo de memoria de UserSync y cambiar el valor de **-XX:MaxDirectMemorySize** en **GC_OPTS** al doble de la memoria directa utilizada por UserSync. Puede cambiar el valor en función del escenario de servicio real. Para obtener más información, consulte **Paso 2**.

Paso 5 Reinicie los servicios o instancias afectados y compruebe si la alarma está desactivada.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 6**.

Recopilar información de fallas.

Paso 6 En FusionInsight Manager, seleccione **O&M**. En el panel de navegación de la izquierda, elija **Log** > **Download**.

Paso 7 Expanda la lista desplegable **Service** y seleccione **Ranger** para el clúster de destino.

Paso 8 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 9 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

Información relacionada

Ninguna

9.257 ALM-45283 El uso de memoria no heap de UserSync supera el umbral

Descripción

El sistema comprueba el uso de memoria no heap del servicio UserSync cada 60 segundos. Esta alarma se genera cuando el uso de memoria no heap de la instancia UserSync excede el umbral (80% de la memoria máxima) durante cinco veces consecutivas. Esta alarma se borra cuando el uso de memoria no heap es menor que el umbral.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
45283	Grave	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger Condition	Especifica el umbral para activar la alarma.

Impacto en el sistema

El desbordamiento de la memoria no heap puede provocar una falla en el servicio.

Causas posibles

La memoria no heap del proceso UserSync se utiliza en exceso o la memoria no heap se asigna de forma inadecuada.

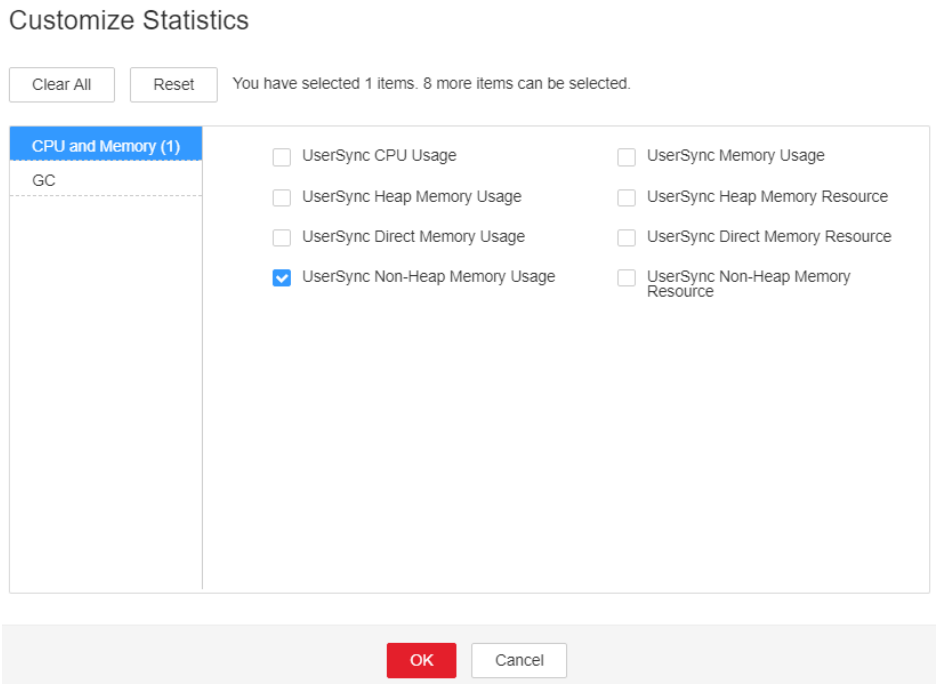
Procedimiento

Comprobar el uso de memoria no heap.

Paso 1 En FusionInsight Manager, elija **O&M** > **Alarm** > **Alarms** > **ALM-45283 UserSync Non Heap Memory Usage Exceeds the Threshold**. Compruebe la información de ubicación de la alarma y vea el nombre de host de la instancia para la que se genera la alarma.

Paso 2 En FusionInsight Manager, seleccione **Cluster** > **Services** > **Ranger** > **Instance**. Seleccione el rol correspondiente al nombre de host de la instancia para la que se genera la alarma. Haga clic en la lista desplegable situada en la esquina superior derecha del área del gráfico y elija **Customize** > **CPU and Memory** > **UserSync Non Heap Memory Usage**. Haga clic en **OK**.

Figura 9-117 Uso de memoria no heap de UserSync



Paso 3 Compruebe si la memoria no heap utilizada por UserSync alcanza el umbral (80% de la memoria máxima no heap de forma predeterminada).

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 6**.

Paso 4 En FusionInsight Manager, elija **Cluster** > **Services** > **Ranger** > **Instance** > **UserSync** > **Instance Configuration**. Haga clic en **All Configurations** y elija **UserSync** > **System**. Establezca **-XX: MaxPermSize** en el parámetro **GC_OPTS** a un valor mayor según los requisitos del sitio y haga clic en **Save** para guardar la configuración.

NOTA

Si se genera esta alarma, el tamaño de memoria no heap configurado para la instancia UserSync no puede cumplir con la memoria no heap requerida por el proceso UserSync. Se recomienda cambiar el valor **-XX:MaxPermSize** de **GC_OPTS** al doble del tamaño de memoria actual que no es de montón o cambiar el valor en función de los requisitos del sitio.

Paso 5 Reinicie los servicios o instancias afectados y compruebe si la alarma está desactivada.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 6**.

Recopilar información de fallas.

Paso 6 En FusionInsight Manager, seleccione **O&M**. En el panel de navegación de la izquierda, elija **Log** > **Download**.

Paso 7 Expanda la lista desplegable **Service** y seleccione **Ranger** para el clúster de destino.

Paso 8 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 9 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

Información relacionada

Ninguna

9.258 ALM-45284 El tiempo de recolección de basura (GC) de UserSync supera el umbral

Descripción

El sistema comprueba la duración de GC del proceso UserSync cada 60 segundos. Esta alarma se genera cuando la duración de GC del proceso UserSync excede el umbral (12 segundos por defecto) durante cinco veces consecutivas. Esta alarma se borra cuando la duración de GC es menor que el umbral.

Atributos

ID de alarma	Severidad de alarma	Borrado automáticamente
45284	Grave	Sí

Parámetros

Nombre	Significado
Source	Clúster para el que se genera la alarma.
ServiceName	Servicio para el que se genera la alarma.
RoleName	Rol para el que se genera la alarma.
HostName	Host para el que se genera la alarma.
Trigger Condition	Umbral para activar la alarma.

Impacto en el sistema

UserSync responde lentamente.

Causas posibles

La memoria heap de la instancia UserSync se utiliza en exceso o la memoria heap se asigna de forma inadecuada. Como resultado, los GC ocurren con frecuencia.

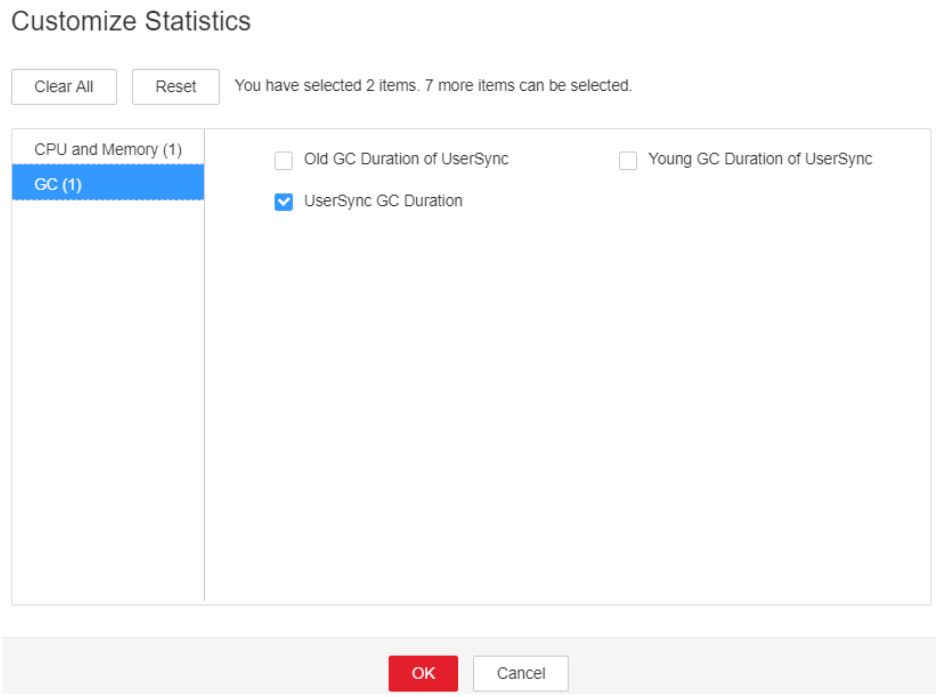
Procedimiento

Comprobar el tiempo de GC.

Paso 1 En FusionInsight Manager, elija **O&M** > **Alarm** > **Alarms** > **ALM-45284 UserSync Garbage Collection (GC) Time Exceeds the Threshold**. Compruebe la información de ubicación de la alarma y vea el nombre de host de la instancia para la que se genera la alarma.

Paso 2 En FusionInsight Manager, seleccione **Cluster** > **Services** > **Ranger** > **Instance**. Seleccione el rol correspondiente al nombre de host de la instancia para la que se genera la alarma y haga clic en la lista desplegable en la esquina superior derecha del área del gráfico. Elija **Customize** > **GC** > **UserSync GC Duration**. Haga clic en **OK**.

Figura 9-118 Duración de GC de UserSync



Paso 3 Compruebe si la duración de GC del proceso UserSync recopilado cada minuto supera el umbral (12 segundos por defecto).

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 6**.

Paso 4 En FusionInsight Manager, elija **Cluster** > **Services** > **Ranger** > **Instance** > **UserSync** > **Instance Configuration**. Haga clic en **All Configurations** y elija **UserSync** > **System**. Aumente el valor de **-Xmx** en el parámetro **GC_OPTS** según los requisitos del sitio y guarde la configuración.

NOTA

Si se genera esta alarma, la memoria heap configurada para UserSync no puede cumplir con la memoria heap requerida por el proceso UserSync. Se recomienda cambiar el valor de **GC_OPTS** por el doble de la memoria heap utilizada por UserSync. Puede cambiar el valor en función del escenario de servicio real. Para obtener más información acerca de cómo comprobar el uso de la memoria heap de UserSync, consulte **Paso 2**.

Paso 5 Reinicie los servicios o instancias afectados y compruebe si la alarma está desactivada.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 6**.

Recopilar información de fallas.

Paso 6 En FusionInsight Manager, elija **O&M** > **Log** > **Download**.

Paso 7 Expanda la lista desplegable **Service** y seleccione **Ranger** para el clúster de destino.

Paso 8 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 9 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Después de rectificar el fallo que activa la alarma, la alarma se borra automáticamente.

Información relacionada

Ninguna

9.259 ALM-45285 El uso de memoria heap de TagSync supera el umbral

Descripción

El sistema comprueba el uso de memoria heap del servicio TagSync cada 60 segundos. Esta alarma se genera cuando el uso de memoria heap de la instancia TagSync excede el umbral (95% de la memoria máxima) durante 10 veces consecutivas. Esta alarma se borra cuando el uso de memoria heap es menor que el umbral.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
45285	Grave	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger Condition	Especifica el umbral para activar la alarma.

Impacto en el sistema

El desbordamiento de la memoria heap puede causar una falla en el servicio.

Causas posibles

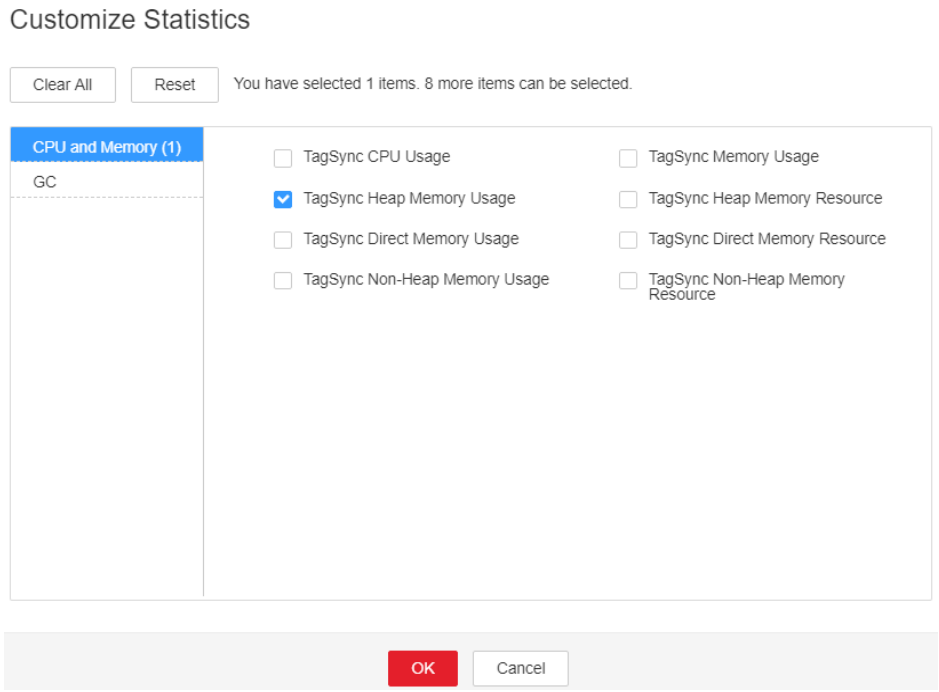
El uso de memoria heap de la instancia TagSync es alto o la memoria heap está asignada incorrectamente.

Procedimiento

Paso 1 En FusionInsight Manager, elija **O&M** > **Alarm** > **Alarms** > **ALM-45285 TagSync Heap Memory Usage Exceeds the Threshold**. Compruebe la información de ubicación de la alarma y vea el nombre de host de la instancia para la que se genera la alarma.

Paso 2 En FusionInsight Manager, seleccione **Cluster** > **Services** > **Ranger** > **Instance**. Seleccione el rol correspondiente al nombre de host de la instancia para la que se genera la alarma. Haga clic en la lista desplegable situada en la esquina superior derecha del área del gráfico y elija **Customize** > **CPU and Memory** > **TagSync Heap Memory Usage**. Haga clic en **OK**.

Figura 9-119 Uso de memoria heap de TagSync



Paso 3 Compruebe si la memoria heap utilizada por TagSync alcanza el umbral (95% de la memoria heap máxima de forma predeterminada).

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 6**.

Paso 4 En FusionInsight Manager, elija **Cluster** > **Services** > **Ranger** > **Instance** > **TagSync** > **Instance Configuration**. Haga clic en **All Configurations** y seleccione **TagSync** > **System**. Aumente el valor de **-Xmx** en el parámetro **GC_OPTS** según los requisitos del sitio y guarde la configuración.

NOTA

Si se genera esta alarma, la memoria heap configurada para TagSync no puede cumplir con la memoria heap requerida por el proceso TagSync. Se recomienda cambiar el valor **-Xmx** de **GC_OPTS** a dos veces el de la memoria heap utilizada por TagSync. Puede cambiar el valor en función del escenario de servicio real. Para obtener más información acerca de cómo comprobar el uso de la memoria del montón TagSync, consulte **Paso 2**.

Paso 5 Reinicie los servicios o instancias afectados y compruebe si la alarma está desactivada.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 6**.

Recopilar información de fallas.

Paso 6 En FusionInsight Manager, seleccione **O&M**. En el panel de navegación de la izquierda, elija **Log** > **Download**.

Paso 7 Expanda la lista desplegable **Service** y seleccione **Ranger** para el clúster de destino.

Paso 8 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 9 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

Información relacionada

Ninguna

9.260 ALM-45286 El uso de memoria directa de TagSync supera el umbral

Descripción

El sistema comprueba el uso de memoria directa del servicio TagSync cada 60 segundos. Esta alarma se genera cuando el uso de memoria directa de la instancia TagSync supera el umbral (80% de la memoria máxima) durante cinco veces consecutivas. Esta alarma se borra cuando el uso de memoria directa TagSync es menor o igual que el umbral.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
45286	Grave	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger Condition	Especifica el umbral para activar la alarma.

Impacto en el sistema

El desbordamiento de la memoria directa puede provocar una falla en el servicio.

Causas posibles

La memoria directa de la instancia TagSync se utiliza en exceso o la memoria directa se asigna de forma inapropiada. Como resultado, el uso de memoria excede el umbral.

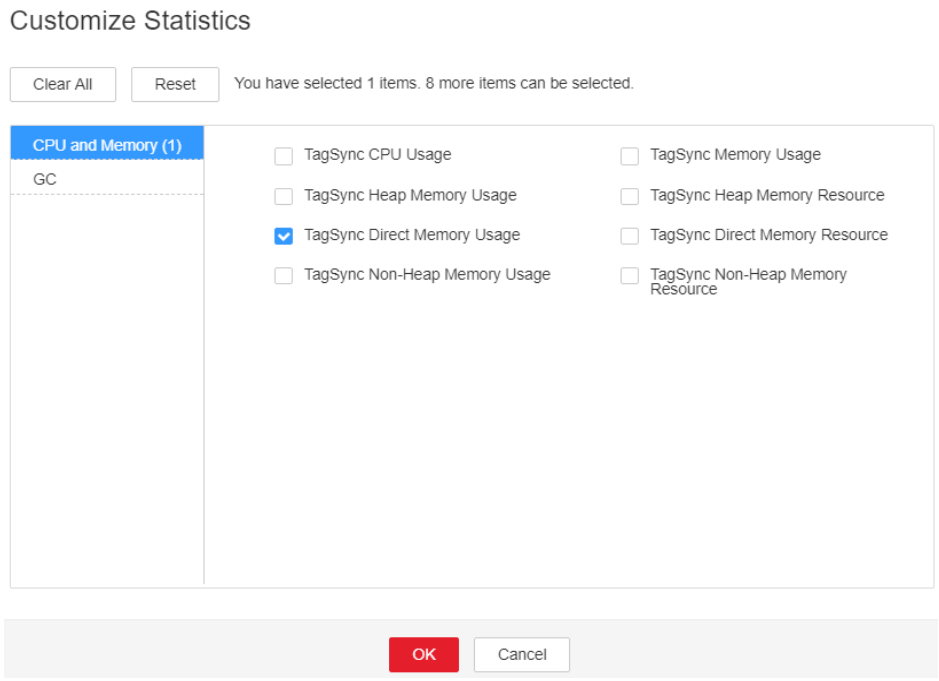
Procedimiento

Comprobar el uso de la memoria directa.

Paso 1 En FusionInsight Manager, elija **O&M** > **Alarm** > **Alarms** > **ALM-45286 TagSync Direct Memory Usage Exceeds the Threshold**. Compruebe la información de ubicación de la alarma y vea el nombre de host de la instancia para la que se genera la alarma.

Paso 2 En FusionInsight Manager, seleccione **Cluster** > **Services** > **Ranger** > **Instance**. Seleccione el rol correspondiente al nombre de host de la instancia para la que se genera la alarma. Haga clic en la lista desplegable situada en la esquina superior derecha del área del gráfico y elija **Customize** > **CPU and Memory** > **TagSync Direct Memory Usage**. Haga clic en **OK**.

Figura 9-120 Uso de memoria directa de TagSync



Paso 3 Compruebe si la memoria directa utilizada por el TagSync alcanza el umbral (80% de la memoria directa máxima por defecto).

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 6**.

Paso 4 En FusionInsight Manager, elija **Cluster** > **Services** > **Ranger** > **Instance** > **TagSync** > **Instance Configuration**. Haga clic en **All Configurations** y seleccione **TagSync** > **System**. Aumente el valor de **-XX:MaxDirectMemorySize** en el parámetro **GC_OPTS** según los requisitos del sitio y guarde la configuración.

NOTA

Si se genera esta alarma, la memoria directa configurada para TagSync no puede cumplir con la memoria directa requerida por el proceso TagSync. Se recomienda comprobar el uso de memoria directa de TagSync y cambiar el valor de **-XX:MaxDirectMemorySize** en **GC_OPTS** al doble de la memoria directa utilizada por TagSync. Puede cambiar el valor en función del escenario de servicio real. Para obtener más información, consulte **Paso 2**.

Paso 5 Reinicie los servicios o instancias afectados y compruebe si la alarma está desactivada.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 6**.

Recopilar información de fallas.

Paso 6 En FusionInsight Manager, seleccione **O&M**. En el panel de navegación de la izquierda, elija **Log** > **Download**.

Paso 7 Expanda la lista desplegable **Service** y seleccione **Ranger** para el clúster de destino.

Paso 8 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 9 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

Información relacionada

Ninguna

9.261 ALM-45287 El uso de memoria no heap de TagSync supera el umbral

Descripción

El sistema comprueba el uso de memoria no heap del servicio TagSync cada 60 segundos. Esta alarma se genera cuando el uso de memoria no heap de la instancia TagSync excede el umbral (80% de la memoria máxima) durante cinco veces consecutivas. Esta alarma se borra cuando el uso de memoria no heap es menor que el umbral.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
45287	Grave	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger Condition	Especifica el umbral para activar la alarma.

Impacto en el sistema

El desbordamiento de la memoria no heap puede provocar una falla en el servicio.

Causas posibles

La memoria no heap del proceso TagSync se utiliza en exceso o la memoria no heap se asigna de forma inadecuada.

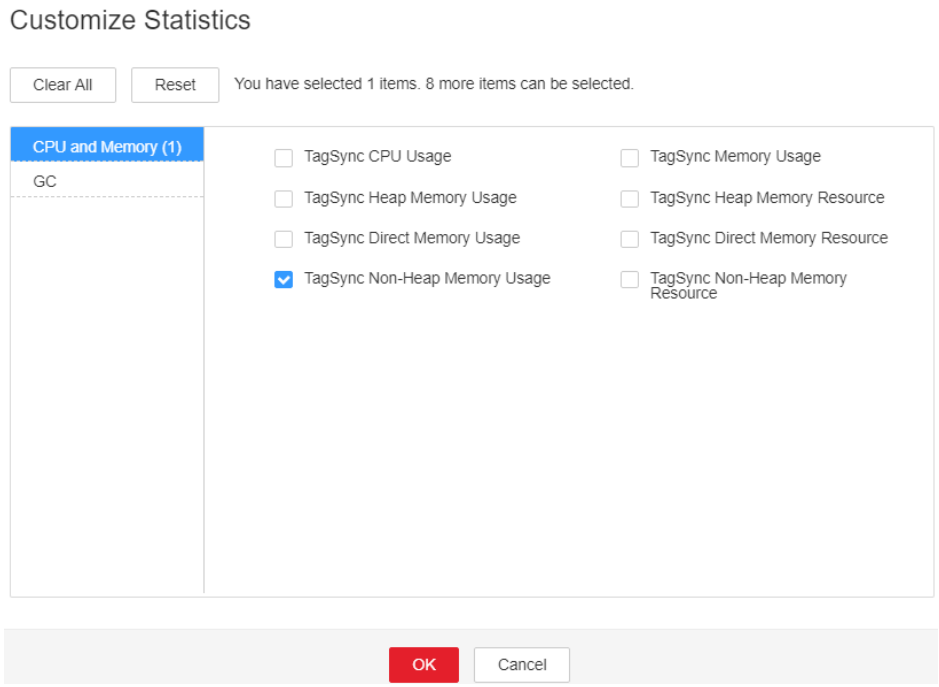
Procedimiento

Comprobar el uso de memoria no heap.

Paso 1 En FusionInsight Manager, elija **O&M** > **Alarm** > **Alarms** > **ALM-45287 TagSync Non Heap Memory Usage Exceeds the Threshold**. Compruebe la información de ubicación de la alarma y vea el nombre de host de la instancia para la que se genera la alarma.

Paso 2 En FusionInsight Manager, seleccione **Cluster** > **Services** > **Ranger** > **Instance**. Seleccione el rol correspondiente al nombre de host de la instancia para la que se genera la alarma. Haga clic en la lista desplegable situada en la esquina superior derecha del área del gráfico y elija **Customize** > **CPU and Memory** > **TagSync Non Heap Memory Usage**. Haga clic en **OK**.

Figura 9-121 Uso de memoria no heap de TagSync



Paso 3 Compruebe si la memoria no heap utilizada por TagSync alcanza el umbral (80% de la memoria máxima no heap de forma predeterminada).

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 6**.

Paso 4 En FusionInsight Manager, elija **Cluster** > **Services** > **Ranger** > **Instance** > **TagSync** > **Instance Configuration**. Haga clic en **All Configurations** y seleccione **TagSync** > **System**. Establezca **-XX: MaxPermSize** en el parámetro **GC_OPTS** a un valor mayor según los requisitos del sitio y guarde la configuración.

NOTA

Si se genera esta alarma, el tamaño de memoria no heap configurado para la instancia TagSync no puede cumplir con la memoria no heap requerida por el proceso TagSync. Se recomienda cambiar el valor **-XX:MaxPermSize** de **GC_OPTS** al doble del tamaño de memoria actual que no es de montón o cambiar el valor en función de los requisitos del sitio.

Paso 5 Reinicie los servicios o instancias afectados y compruebe si la alarma está desactivada.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 6**.

Recopilar información de fallas.

Paso 6 En FusionInsight Manager, seleccione **O&M**. En el panel de navegación de la izquierda, elija **Log** > **Download**.

Paso 7 Expanda la lista desplegable **Service** y seleccione **Ranger** para el clúster de destino.

Paso 8 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 9 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

Información relacionada

Ninguna

9.262 ALM-45288 El tiempo de recolección de basura (GC) de TagSync supera el umbral

Descripción

El sistema comprueba la duración de GC del proceso TagSync cada 60 segundos. Esta alarma se genera cuando la duración de GC del proceso TagSync excede el umbral (12 segundos por defecto) durante cinco veces consecutivas. Esta alarma se borra cuando la duración de GC es menor que el umbral.

Atributos

ID de alarma	Severidad de alarma	Borrar automáticamente
45288	Grave	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger Condition	Especifica el umbral para activar la alarma.

Impacto en el sistema

TagSync responde lentamente.

Causas posibles

La memoria heap de la instancia TagSync se utiliza en exceso o la memoria heap se asigna de forma inadecuada. Como resultado, los GC ocurren con frecuencia.

Procedimiento

Comprobar la duración del GC.

Paso 1 En FusionInsight Manager, elija **O&M** > **Alarm** > **Alarms** > **ALM-45288 TagSync Garbage Collection (GC) Time Exceeds the Threshold**. Compruebe la información de ubicación de la alarma y vea el nombre de host de la instancia para la que se genera la alarma.

Paso 2 En FusionInsight Manager, seleccione **Cluster** > **Services** > **Ranger** > **Instance**. Seleccione el rol correspondiente al nombre de host de la instancia para la que se genera la alarma y haga clic en la lista desplegable en la esquina superior derecha del área del gráfico. Elija **Customize** >**GC** > **TagSync GC Duration**. Haga clic en **OK**.

Figura 9-122 Duración de GC de TagSync

Paso 3 Compruebe si la duración de GC del proceso TagSync recopilado cada minuto supera el umbral (12 segundos por defecto).

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 6**.

Paso 4 En FusionInsight Manager, elija **Cluster** > **Services** > **Ranger** > **Instance** > **TagSync** > **Instance Configuration**. Haga clic en **All Configurations** y seleccione **TagSync** > **System**. Aumente el valor de **-Xmx** en el parámetro **GC_OPTS** según los requisitos del sitio y guarde la configuración.

NOTA

Si se genera esta alarma, la memoria heap configurada para TagSync no puede cumplir con la memoria heap requerida por el proceso TagSync. Se recomienda cambiar el valor **-Xmx** de **GC_OPTS** a dos veces el de la memoria heap utilizada por TagSync. Puede cambiar el valor en función del escenario de servicio real. Para obtener más información acerca de cómo comprobar el uso de la memoria del montón TagSync, consulte **Paso 2**.

Paso 5 Reinicie los servicios o instancias afectados y compruebe si la alarma está desactivada.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 6**.

Recopilar información de fallas.

Paso 6 En FusionInsight Manager, seleccione **O&M**. En el panel de navegación de la izquierda, elija **Log** > **Download**.

Paso 7 Expanda la lista desplegable **Service** y seleccione **Ranger** para el clúster de destino.

Paso 8 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 9 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

Información relacionada

Ninguna

9.263 ALM-45425 Servicio ClickHouse no disponible

Descripción

El módulo de alarma comprueba el estado de la instancia ClickHouse cada 60 segundos. Esta alarma se genera cuando el módulo de alarma detecta que todas las instancias de ClickHouse son anormales.

Esta alarma se borra cuando el sistema detecta que se restaura cualquier instancia de ClickHouse y se borra la alarma.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
45425	Crítica	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster o sistema para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

El servicio ClickHouse es anormal. No puede usar FusionInsight Manager para realizar operaciones de clúster en el servicio ClickHouse. La función de servicio ClickHouse no está disponible.

Causas posibles

La información de configuración del archivo **metrika.xml** del directorio de configuración de componentes del nodo de instancia ClickHouse defectuoso no es coherente con la de la instancia ClickHouse correspondiente en ZooKeeper.

Procedimiento

Compruebe si la configuración en metrika.xml de la instancia ClickHouse es correcta.

Paso 1 Inicie sesión en FusionInsight Manager, elija **Cluster** > **Services** > **ClickHouse** > **Instance** y localice la instancia anormal de ClickHouse en función de la información de alarma.

- En caso afirmativo, vaya a **Paso 2**.
- Si no, vaya a **Paso 9**.

Paso 2 Inicie sesión en el host donde el servicio ClickHouse es anormal y haga ping a la dirección IP de otro nodo de instancia de ClickHouse normal para comprobar si la conexión de red es normal.

- En caso afirmativo, vaya a **Paso 3**.
- Si no, póngase en contacto con el administrador de red para reparar la red.

Paso 3 Elija **Cluster** > **Services** > **ClickHouse** > **Instance**, haga clic en el nombre de instancia anormal en la columna **Role**, haga clic en **Configurations**, busque **macros.id** en el cuadro de búsqueda y busque el valor de **macros.id** de la instancia actual.

Paso 4 Inicie sesión en el host donde se encuentra el cliente ZooKeeper e inicie sesión en el cliente ZooKeeper.

Cambie al directorio de instalación del cliente.

Ejemplo: **cd /opt/client**

Ejecute el siguiente comando para configurar las variables de entorno:

source bigdata_env

Ejecute el siguiente comando para autenticar al usuario (omita este paso en el modo común):

kinit *Component service user*

Ejecute el siguiente comando para iniciar sesión en la herramienta de cliente:

zkCli.sh -server *service IP address of the node where the ZooKeeper role instance locates*:*client port*

Paso 5 Ejecute el siguiente comando para comprobar si se puede obtener la información de topología de clúster ClickHouse.

get /clickhouse/config/*value of* ***macros.id*** *in* **Paso 3**/**metrika.xml**

- En caso afirmativo, vaya a **Paso 6**.
- Si no, vaya a **Paso 9**.

Paso 6 Inicie sesión en el host donde la instancia ClickHouse es anormal y vaya al directorio de configuración de la instancia ClickHouse.

cd ${BIGDATA_HOME}/**FusionInsight_ClickHouse_***Version*/x_x_**ClickHouseServer/etc**

cat metrika.xml

Paso 7 Compruebe si la información de topología de clúster de ZooKeeper obtenida en **Paso 5** es la misma que en el archivo **metrika.xml** del directorio de configuración de componentes en **Paso 6**.

- En caso afirmativo, compruebe si la alarma está desactivada. Si la alarma persiste, vaya a **Paso 9**.
- Si no, vaya a **Paso 8**.

Paso 8 En FusionInsight Manager, elija **Cluster** > **Services** > **ClickHouse**, haga clic en **More**, y seleccione **Synchronize Configuration**. A continuación, compruebe si el estado del servicio es normal y si la alarma se borra 5 minutos después.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 9**.

Recopilar información de fallas.

Paso 9 En FusionInsight Manager, seleccione **O&M**. En el panel de navegación de la izquierda, elija **Log** > **Download**.

Paso 10 Expanda la lista desplegable **Service** y seleccione **ClickHouse** para el clúster de destino.

Paso 11 Elija el host correspondiente de la lista de hosts.

Paso 12 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 1 hora antes y después del tiempo de generación de alarma, respectivamente. A continuación, haga clic en **Download**.

Paso 13 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

Información relacionada

Ninguna

9.264 ALM-45426 El uso de la cuota de cantidad del servicio ClickHouse en ZooKeeper supera el umbral

Descripción

El módulo de alarma comprueba el uso de cuota del servicio ClickHouse en el ZooKeeper cada 60 segundos. Esta alarma se genera cuando el módulo de alarma detecta que el uso excede el umbral (90%).

Esta alarma se borra cuando el sistema detecta que el uso es menor que el umbral y la alarma se borra.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
45426	Mayor (predeterminado)	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster o sistema para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

Una vez que la cuota de cantidad de ZooKeeper del servicio ClickHouse supera el umbral, no puede realizar operaciones de clúster en el servicio ClickHouse en FusionInsight Manager. Como resultado, no se puede utilizar el servicio ClickHouse.

Causas posibles

- Cuando se crean, insertan o eliminan datos de tabla, el ClickHouse crea znodes en nodos de ZooKeeper. A medida que aumenta el volumen de servicio, el número de znodes puede exceder el umbral configurado.
- No se ha establecido ningún límite de cuota para el directorio de metadatos **/clickhouse** de ClickHouse en ZooKeeper.

Procedimiento

Comprobar el número de znodes creados por ClickHouse en ZooKeeper.

Paso 1 Inicie sesión en el host donde se encuentra el cliente ZooKeeper e inicie sesión en el cliente ZooKeeper.

Cambie al directorio de instalación del cliente.

Ejemplo: **cd /opt/client**

Ejecute el siguiente comando para configurar las variables de entorno:

source bigdata_env

Ejecute el siguiente comando para autenticar al usuario (omita este paso en el modo común):

kinit *Component service user*

Ejecute el siguiente comando para iniciar sesión en la herramienta de cliente:

zkCli.sh -server *service IP address of the node where the ZooKeeper role instance locates*:*client port*

Paso 2 Ejecute el siguiente comando para comprobar la cuota utilizada por el ClickHouse en el ZooKeeper y comprobar si la información de cuota está correctamente establecida:

listquota /clickhouse

```
absolute path is /zookeeper/quota/clickhouse
Quota for path /clickhouse does not exist.
```

Si la información anterior indica que la configuración de la cuota es incorrecta, vaya a **Paso 3**.

Si no, vaya a **Paso 5**.

Paso 3 Inicie sesión en FusionInsight Manager y elija **Cluster** > **Services** > **ZooKeeper**. En la página mostrada, haga clic en **Configurations** y haga clic en **All Configurations**. En esta página de subpestaña, busque **quotas.auto.check.enable** para comprobar si su valor es de **true**.

Si el valor no es **true**, cambie el valor a **true** y haga clic en **Save**.

Paso 4 En FusionInsight Manager, elija **Cluster** > **Services** > **ClickHouse**, haga clic en **More**, y seleccione **Synchronize Configuration**. Una vez que la sincronización se haya realizado correctamente, vaya a **Paso 1**.

Paso 5 Ejecute el siguiente comando y compruebe si la relación entre el valor de **count** de **Output stat** y el valor de **count** de **Output quota** en la salida del comando es mayor que **0.9**:

listquota /clickhouse

```
absolute path is /zookeeper/quota/clickhouse
Output quota for /clickhouse count=200000,bytes=1000000000
Output stat for /clickhouse count=2667,bytes=60063
```

En la información anterior, el valor **count** de **Output stat** es de **2667** y el valor **count** de **Output quota** es de **200000**.

- En caso afirmativo, vaya a **Paso 6**.
- En caso negativo, compruebe si la alarma se borra 5 minutos después. Si la alarma persiste, vaya a **Paso 8**.

Paso 6 En FusionInsight Manager, elija **Cluster** > **Services** > **ClickHouse** > **Configurations** > **All Configurations**, busque el parámetro **clickhouse.zookeeper.quota.node.count**, y cambie el valor de este parámetro al doble del valor de **count** de **Output stat** en **Paso 5**.

Paso 7 Reinicie la instancia ClickHouse para la que se genera la alarma y compruebe si la alarma se borra 5 minutos después.

- En caso afirmativo, no es necesario hacer nada más.
- En caso negativo, vuelva a realizar **Paso 6** y compruebe si la alarma se borra 5 minutos más tarde. Si la alarma persiste, vaya a **Paso 8**.

Recopilar información de fallas.

Paso 8 En FusionInsight Manager, seleccione **O&M**. En el panel de navegación de la izquierda, elija **Log** > **Download**.

Paso 9 Expanda la lista desplegable **Service** y seleccione **ClickHouse** para el clúster de destino.

Paso 10 Elija el host correspondiente de la lista de hosts.

Paso 11 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 1 hora antes y después del tiempo de generación de alarma, respectivamente. A continuación, haga clic en **Download**.

Paso 12 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

Información relacionada

Ninguna

9.265 ALM-45427 El uso de la cuota de capacidad del servicio ClickHouse en ZooKeeper supera el umbral

Descripción

El módulo de alarma comprueba el uso de cuota del servicio ClickHouse en el ZooKeeper cada 60 segundos. Esta alarma se genera cuando el módulo de alarma detecta que el uso excede el umbral (90%).

Esta alarma se borra cuando el sistema detecta que el uso es menor que el umbral y la alarma se borra.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
45427	Mayor (predeterminado)	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

Una vez que la cuota de cantidad de ZooKeeper del servicio ClickHouse supera el umbral, no puede realizar operaciones de clúster en el servicio ClickHouse en FusionInsight Manager. Como resultado, no se puede utilizar el servicio ClickHouse.

Causas posibles

- Cuando se crean, insertan o eliminan datos de tabla, el ClickHouse crea znodes en nodos de ZooKeeper. A medida que aumenta el volumen de servicio, la capacidad de los znodes puede exceder el umbral configurado.
- No se ha establecido ningún límite de cuota para el directorio de metadatos **/clickhouse** de ClickHouse en ZooKeeper.

Procedimiento

Comprobar la capacidad znode de la ClickHouse en el ZooKeeper.

Paso 1 Inicie sesión en el host donde se encuentra el cliente ZooKeeper e inicie sesión en el cliente ZooKeeper.

Cambie al directorio de instalación del cliente.

Ejemplo: **cd /opt/client**

Ejecute el siguiente comando para configurar las variables de entorno:

source bigdata_env

Ejecute el siguiente comando para autenticar al usuario (omita este paso en el modo común):

kinit *Component service user*

Ejecute el siguiente comando para iniciar sesión en la herramienta de cliente:

zkCli.sh -server *service IP address of the node where the ZooKeeper role instance locates*:*client port*

Paso 2 Ejecute el siguiente comando para comprobar la cuota utilizada por el ClickHouse en el ZooKeeper y comprobar si la información de cuota está correctamente establecida:

listquota /clickhouse

```
absolute path is /zookeeper/quota/clickhouse
Quota for path /clickhouse does not exist.
```

- Si la información anterior indica que la configuración de la cuota es incorrecta, vaya a **Paso 3**.
- Si no es así, vaya a **Paso 5**.

Paso 3 Inicie sesión en FusionInsight Manager y elija **Cluster** > **Services** > **ZooKeeper**. En la página mostrada, haga clic en **Configurations** y haga clic en **All Configurations**. En esta página de subpestaña, busque **quotas.auto.check.enable** para comprobar si su valor es de **true**.

Si el valor no es **true**, cambie el valor a **true** y haga clic en **Save**.

Paso 4 En FusionInsight Manager, elija **Cluster** > **Services** > **ClickHouse**, haga clic en **More**, y seleccione **Synchronize Configuration**. Una vez que la sincronización se haya realizado correctamente, vaya a **Paso 1**.

Paso 5 Ejecute el siguiente comando y compruebe si la relación entre el valor de **bytes** de **Output stat** y el valor de **bytes** de **Output quota** en la salida del comando es mayor que **0.9**:

listquota /clickhouse

```
absolute path is /zookeeper/quota/clickhouse
Output quota for /clickhouse count=200000,bytes=1000000000
Output stat for /clickhouse count=2667,bytes=60063
```

En la información anterior, el valor **bytes** de **Output stat** es de **60063** y el valor **bytes** de **Output quota** es de **1000000000**.

- En caso afirmativo, vaya a **Paso 6**.
- En caso negativo, compruebe si la alarma se borra 5 minutos después. Si la alarma persiste, vaya a **Paso 8**.

Paso 6 En FusionInsight Manager, elija **Cluster** > **Services** > **ClickHouse** > **Configurations** > **All Configurations**, busque el parámetro **clickhouse.zookeeper.quota.size**, y cambie el valor de este parámetro al doble del valor de **bytes** de **Output stat** en **Paso 5**.

Paso 7 Reinicie la instancia ClickHouse para la que se genera la alarma y compruebe si la alarma se borra 5 minutos después.

- En caso afirmativo, no es necesario hacer nada más.
- En caso negativo, vuelva a realizar **Paso 6** y compruebe si la alarma se borra 5 minutos más tarde. Si la alarma persiste, vaya a **Paso 8**.

Recopilar información de fallas.

Paso 8 En FusionInsight Manager, seleccione **O&M**. En el panel de navegación de la izquierda, elija **Log** > **Download**.

Paso 9 Expanda la lista desplegable **Service** y seleccione **ClickHouse** para el clúster de destino.

Paso 10 Elija el host correspondiente de la lista de hosts.

Paso 11 Haga clic en  en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 1 hora antes y después del tiempo de generación de alarma, respectivamente. A continuación, haga clic en **Download**.

Paso 12 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

Información relacionada

Ninguna

9.266 ALM-45428 Excepción de E/S de disco de ClickHouse

Descripción

Esta alarma se genera cuando el módulo de alarma detecta errores EIO o EROFS durante la lectura y escritura de ClickHouse cada 60 segundos.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
45428	Mayor (predeterminado)	No

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

- ClickHouse no puede leer y escribir datos. Las operaciones INSERT, SELECT y CREATE en las tablas locales pueden ser anormales. Las tablas distribuidas no se ven afectadas.
- Los servicios se ven afectados y las E/S fallan.

Causas posibles

El disco está envejecido o tiene sectores defectuosos.

Procedimiento

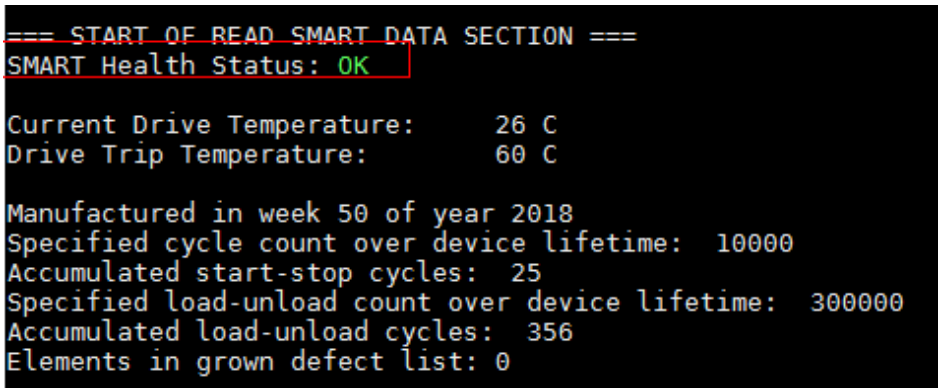
Paso 1 En FusionInsight Manager, seleccione **O&M** > **Alarm** > **Alarms** > **ALM-45428 ClickHouse Disk I/O Exception**. Compruebe el nombre del rol y la dirección IP del host donde se genera la alarma en **Location**.

Paso 2 Utilice PuTTY para iniciar sesión en el nodo para el que se genera el error como usuario **root**.

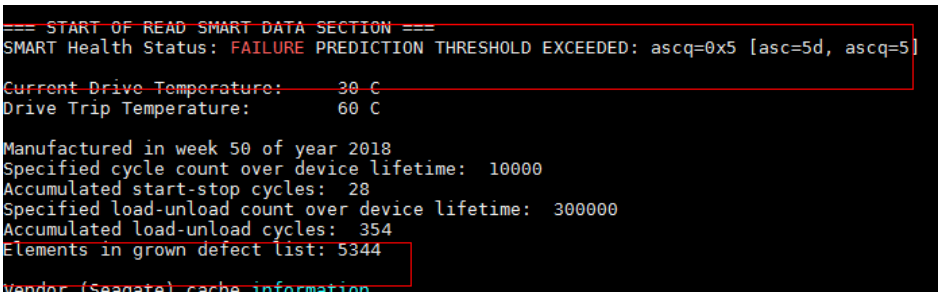
Paso 3 Ejecute el comando **df -h** para comprobar el directorio de montaje y encontrar el disco montado en el directorio defectuoso.

Paso 4 Ejecute el comando **smartctl -a /dev/sd*** para comprobar los discos.

- Si se muestra **SMART Health Status: OK**, como se muestra en la siguiente figura, el disco está en buen estado. En este caso, vaya a **Paso 6**.



- Si el número siguiente a **Elements in grown defect list** no es 0, como se muestra en la siguiente figura, el disco puede tener sectores defectuosos. Si se muestra **SMART Health Status: FAILURE**, el disco se encuentra en el estado de salud secundaria. En este caso, póngase en contacto con el personal.



Paso 5 Una vez rectificada la falla, borre manualmente la alarma en FusionInsight Manager y compruebe si la alarma vuelve a generarse durante la comprobación periódica.

- En caso afirmativo, vaya a **Paso 6**.
- En caso negativo, no se requiere ninguna otra acción.

Recopilar información de fallas.

Paso 6 En FusionInsight Manager, seleccione **O&M**. En el panel de navegación de la izquierda, elija **Log** > **Download**.

Paso 7 Expanda la lista desplegable **Service** y seleccione **ClickHouse** para el clúster de destino.

Paso 8 Elija el host correspondiente de la lista de hosts.

Paso 9 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 1 hora antes y después del tiempo de generación de alarma, respectivamente. A continuación, haga clic en **Download**.

Paso 10 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Si la alarma no tiene impacto, borre la alarma manualmente.

Información relacionada

Ninguna

9.267 ALM-45429 Error de sincronización de metadatos de tabla en el nodo ClickHouse añadido

NOTA

Esta sección solo se aplica a MRS 3.1.2 o posterior.

Descripción

Esta alarma se genera cuando la tabla local correspondiente a la tabla distribuida no se crea durante la expansión de la capacidad de ClickHouse.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
45429	Grave	No

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

No se puede consultar la tabla distribuida.

Causas posibles

Un nodo se detiene o falla durante la expansión de la capacidad.

Procedimiento

Paso 1 En FusionInsight Manager, elija **Cluster** > **Services** > **ClickHouse** > **Instance**.

Paso 2 Compruebe si una instancia está detenida, fuera de servicio o defectuosa.

- En caso afirmativo, vaya a **Paso 3**.
- Si no, vaya a **Paso 4**.

Paso 3 Inicie la instancia o rectifique el error de instancia hasta que todas las instancias se ejecuten correctamente.

Paso 4 En FusionInsight Manager, elija **O&M** > **Alarm** > **Alarms**, localice esta alarma y el host defectuoso basado en la información de ubicación.

Paso 5 Inicie sesión en el host defectuoso como usuario **omm**.

Paso 6 Ejecute los siguientes comandos para inicializar variables de entorno:

source *Cluster installation directory*/**FusionInsight_ClickHouse_*/*_*_ClickHouseServer/etc/ENV_VARS**

source *Cluster installation directory*/**FusionInsight_ClickHouse_*/*_*_ClickHouseServer/etc/clickhouse-env.sh**

export CLICKHOUSE_CONF_DIR=${CLICKHOUSE_CONF_DIR}

Paso 7 Ejecute el siguiente comando para ejecutar la herramienta de sincronización de metadatos para sincronizar metadatos desde el nodo existente al nodo defectuoso:

sh *Cluster installation directory*/**FusionInsight_ClickHouse_*/install/FusionInsight-ClickHouse-*/clickhouse/sbin/clickhouse-create-meta.sh true**

Paso 8 Ejecute el siguiente comando para ver la información del registro y comprobar si los metadatos se han sincronizado:

vim /var/log/Bigdata/clickhouse/clickhouseServer/start.log

- Si la sincronización se ha completado, vaya a **Paso 9**.
- Si la sincronización falla, vaya a **Paso 10**.

Paso 9 En FusionInsight Manager, seleccione **O&M** > **Alarm** > **Alarms**. En la columna **Alarm ID**, localice la alarma correspondiente y haga clic en **Clear** en la columna **Operation**. En el cuadro de diálogo que se muestra, haga clic en **OK** para borrar manualmente la alarma.

Recopilar información de fallas.

Paso 10 En FusionInsight Manager, seleccione **O&M**. En el panel de navegación de la izquierda, elija **Log** > **Download**.

Paso 11 Expanda la lista desplegable **Service**, seleccione **ClickHouse** para el clúster de destino y haga clic en **OK**.

Paso 12 Elija el host correspondiente de la lista de hosts.

Paso 13 Haga clic en  en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 30 minutos antes y después del tiempo de generación de alarmas respectivamente. A continuación, haga clic en **Download**.

Paso 14 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma necesita ser borrada manualmente después de que se corrija la falla.

Información relacionada

Ninguna

9.268 ALM-45430 Error de sincronización de metadatos de permisos en el nodo ClickHouse agregado

NOTA

Esta sección solo se aplica a MRS 3.1.2 o posterior.

Descripción

Esta alarma se genera cuando la información de usuario y permiso no se sincroniza durante la expansión de la capacidad de ClickHouse.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
45430	Grave	No

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

El usuario creado no tiene permisos de operación en el nodo.

Causas posibles

Un nodo se detiene o falla durante la expansión de la capacidad.

Procedimiento

Paso 1 En FusionInsight Manager, elija **Cluster** > **Services** > **ClickHouse** > **Instance**.

Paso 2 Compruebe si una instancia está detenida, fuera de servicio o defectuosa.

- En caso afirmativo, vaya a **Paso 3**.
- Si no, vaya a **Paso 4**.

Paso 3 Inicie la instancia o rectifique el error de instancia hasta que todas las instancias se ejecuten correctamente.

Paso 4 En FusionInsight Manager, elija **O&M** > **Alarm** > **Alarms**, localice esta alarma y el host defectuoso basado en la información de ubicación.

Paso 5 Inicie sesión en el host defectuoso como usuario **omm**.

Paso 6 Ejecute los siguientes comandos para inicializar variables de entorno:

source *Cluster installation directory*/**FusionInsight_ClickHouse_*/*_*_ClickHouseServer/etc/ENV_VARS**

source *Cluster installation directory*/**FusionInsight_ClickHouse_*/*_*_ClickHouseServer/etc/clickhouse-env.sh**

export CLICKHOUSE_CONF_DIR=${CLICKHOUSE_CONF_DIR}

Paso 7 Ejecute el siguiente comando para ejecutar la herramienta de sincronización de metadatos para sincronizar metadatos desde el nodo existente al nodo defectuoso:

sh *Cluster installation directory*/**FusionInsight_ClickHouse_*/install/FusionInsight-ClickHouse-*/clickhouse/sbin/clickhouse-create-meta.sh true**

Paso 8 Ejecute el siguiente comando para ver la información del registro y comprobar si los metadatos se han sincronizado:

vim /var/log/Bigdata/clickhouse/clickhouseServer/start.log

Si la sincronización se ha completado, vaya a **Paso 9**.

Si la sincronización falla, vaya a **Paso 10**.

Paso 9 En FusionInsight Manager, seleccione **O&M** > **Alarm** > **Alarms**. En la columna **Alarm ID**, localice la alarma correspondiente y haga clic en **Clear** en la columna **Operation**. En el cuadro de diálogo que se muestra, haga clic en **OK** para borrar manualmente la alarma.

Recopilar información de fallas.

Paso 10 En FusionInsight Manager, seleccione **O&M**. En el panel de navegación de la izquierda, elija **Log** > **Download**.

Paso 11 Expanda la lista desplegable **Service**, seleccione **ClickHouse** para el clúster de destino y haga clic en **OK**.

Paso 12 Elija el host correspondiente de la lista de hosts.

Paso 13 Haga clic en  en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 30 minutos antes y después del tiempo de generación de alarmas respectivamente. A continuación, haga clic en **Download**.

Paso 14 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma necesita ser borrada manualmente después de que se corrija la falla.

Información relacionada

Ninguna

9.269 ALM-45431 Distribución inadecuada de instancias ClickHouse para la asignación de topologías

Descripción

La distribución de instancias ClickHouseServer no cumple los requisitos de asignación de topología.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
45431	Crítica	No

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

Algunas instancias de ClickHouseServer no están disponibles.

Causas posibles

Durante la instalación o la ampliación de la capacidad, el número de instancias o el modo de asignación no cumple con los requisitos de topología.

Procedimiento

Paso 1 En FusionInsight Manager, seleccione **O&M**. En el panel de navegación de la izquierda, elija **Alarm** > **Alarms**, busque la fila que contiene la alarma y analice la causa basándose en **Location** e **Additional Information**.

Paso 2 Maneje la alarma basándose en la información adicional de alarma y el método de manejo en la siguiente tabla.

Información adicional	Observaciones	Método de gestión
Las instancias de *n* ClickHouseServer deben agregarse a otras zonas de disponibilidad.	Esta alarma se genera cuando se despliega un solo clúster en modo DR entre AZ. El despliegue de la instancia ClickHouseServer no cumple con los requisitos de asignación de topologías de DR entre AZ. Como resultado, algunas instancias no pueden funcionar correctamente.	1. En FusionInsight Manager, elija **Cluster** > **Services** > **ClickHouse**, y haga clic en la pestaña **Instance**, busque la fila que contiene la alarma, vea el nombre del host en **Location**, y encuentre la zona de disponibilidad para el que se genera la alarma en la columna AZ basado en el nombre del host. 2. En la página **Instance**, haga clic en **Add Instance** para agregar *n*instancias de ClickHouseServer a otras AZ excepto la AZ donde se genera la alarma.

Información adicional	Observaciones	Método de gestión
Se deben agregar instancias de *n* ClickHouseServer.	Esta alarma se genera cuando se despliega un clúster no único en el modo de despliegue predeterminado de DR entre AZ. El número de instancias ClickHouseServer en el clúster es inferior a un número par. Como resultado, algunas instancias no pueden funcionar correctamente.	1. Determine el número (*n*) de instancias de ClickHouseServer que se van a agregar en función de la información de alarma. 2. En FusionInsight Manager, elija **Cluster** > **Services** > **ClickHouse**, haga clic en la pestaña **Instance** y agregue *n* instancias de ClickHouseServer al clúster.

----Fin

Eliminación de alarmas

Esta alarma necesita ser borrada manualmente después de que se corrija la falla.

Información relacionada

Ninguna

9.270 ALM-45432 Falla el proceso de sincronización de usuario de ClickHouse

Descripción

El sistema comprueba el estado del proceso de sincronización de roles de usuario ClickHouse cada 5 minutos. Esta alarma se genera cuando el sistema detecta que el proceso de sincronización de roles de usuario ClickHouse está defectuoso o que falla la sincronización de roles de usuario.

Esta alarma se borra automáticamente cuando el proceso o función de sincronización de roles de usuario ClickHouse se vuelve normal.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
45432	Grave	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

Algunas instancias de ClickHouseServer no están disponibles.

Causas posibles

- El proceso de sincronización de roles de usuario ClickHouse no se inicia correctamente o se sale de forma anormal.
- El proceso de sincronización de roles de usuario ClickHouse no sincroniza la información de roles de usuario porque el servicio LdapServer es defectuoso.

Procedimiento

Comprobar si el proceso de sincronización de roles de usuario de ClickHouse es normal.

Paso 1 Inicie sesión en FusionInsight Manager y elija **O&M** > **Alarm** > **Alarms**. En la página que se muestra, busque **ALM-45432 El proceso de sincronización de usuarios de ClickHouse falla**.

Paso 2 Compruebe el nombre del host y la información adicional en los detalles de la alarma.

- Si la información adicional es "Process clickhouse-ugsync is not exit"., vaya a **Paso 3**.
- Si la información adicional es "Process clickhouse-ugsync sync user failed.", vaya a **Paso 6**.

Paso 3 Inicie sesión en el host defectuoso como usuario **omm** y ejecute el siguiente comando para comprobar si el proceso de sincronización de roles de usuario ClickHouse es normal:

ps -ef | grep 'clickhouse-ugsync'

Resultado anormal del proceso de sincronización:

```
[omm@server-2110081635-0001 ~]$ ps -ef | grep 'clickhouse-ugsync'
omm      20104 13146  0 15:57 pts/7    00:00:00 grep --color=auto clickhouse-ugsync
```

- En caso afirmativo, la alarma se borra automáticamente. Si la alarma se ha borrado, no se requiere ninguna acción adicional. Si la alarma persiste, vaya a **Paso 8**.
- Si no, vaya a **Paso 4**.

Paso 4 Inicie sesión en el host defectuoso como usuario **omm** y ejecute el siguiente comando para comprobar si la tarea demonio crontab está correctamente configurada:

crontab -l

Configuración normal de la tarea de daemon de contab:

```
*/5 * * * * bash /xxxxx/clickhouse_ugsync_check.sh >/dev/null 2>&1
```

- En caso afirmativo, compruebe si la alarma se apaga 5 minutos más tarde. Si la alarma se ha borrado, no se requiere ninguna acción adicional. Si la alarma persiste, vaya a **Paso 8**.
- Si no, vaya a **Paso 5**.

Paso 5 Inicie sesión en FusionInsight Manager y seleccione **Cluster** > **Services** > **ClickHouse**. En la página que se muestra, haga clic en la pestaña **Instance**. En esta página de pestaña, busque la instancia anormal de ClickHouseServer basada en la información de error y reiníciela. Espere 5 minutos y compruebe si la alarma está desactivada.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 6**.

Comprobar si el servicio LdapServer es normal.

Paso 6 Inicie sesión en FusionInsight Manager, elija **Cluster** > **Services** y compruebe si **Running Status** de LdapServer es **Normal**.

- En caso afirmativo, vaya a **Paso 8**.
- Si no, vaya a **Paso 7**.

Paso 7 Maneje la alarma no disponible del servicio LdapServer de acuerdo con ALM-25000 Servicio LdapServer no disponible.

Después de que **Running Status** de LdapServer se convierta en **Normal**, compruebe si esta alarma está borrada.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 8**.

Recopilar información de fallas.

Paso 8 En FusionInsight Manager, elija **O&M** > **Log** > **Download**.

Paso 9 Expanda la lista desplegable junto al campo **Service**. En el cuadro de diálogo **Services** que se muestra, seleccione **ClickHouseServer** para el clúster de destino.

Paso 10 Expanda la lista **Hosts**. En el cuadro de diálogo **Select Host** que se muestra, seleccione el host anormal y haga clic en **OK**.

Paso 11 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 1 hora antes y después del tiempo de generación de alarma, respectivamente. A continuación, haga clic en **Download**.

Paso 12 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

Información relacionada

Ninguna

9.271 ALM-45433 Excepción de topología de ClickHouse AZ

Descripción

Si la función de HA entre AZ está habilitada para un clúster en el que se ha desplegado ClickHouse, la topología ClickHouse permanece sin cambios. Esta alarma se genera cuando el HA entre AZ no tiene efecto si los nodos de copia de respaldo del mismo shard están en la misma AZ.

Esta alarma se borra automáticamente cuando el sistema detecta que todos los shards cumplen los requisitos de despliegue de HA entre AZ.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
45433	Crítica	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

El despliegue actual del servicio ClickHouse no admite HA entre AZ.

Causas posibles

Después de que HA entre AZ está habilitado, todos los nodos de copia de respaldo de un shard están en la misma AZ.

Procedimiento

Modificar la AZ de nodos de copia de respaldo.

Paso 1 Inicie sesión en el nodo donde está instalado el cliente como usuario de instalación del cliente. Ejecute el siguiente comando para cambiar al directorio de instalación del cliente:

cd *{Client installation path}*

Paso 2 Ejecute el siguiente comando para configurar las variables de entorno:

source bigdata_env

Paso 3 Ejecute el siguiente comando para autenticar al usuario (omita este paso en modo normal):

kinit *Component service user*

Paso 4 Ejecute el siguiente comando para iniciar sesión en la herramienta de cliente:

zkCli.sh -server*Service IP address of the node where the ZooKeeper instance resides***:***Client port*

Paso 5 Ejecute el siguiente comando para ver la topología actual:

get /clickhouse/topo

NOTA

Si el ClickHouse está instalado con varios servicios, ejecute el comando **get /ClickHouse{-n}/topo**. Por ejemplo, si el ClickHouse-1 está instalado, ejecute el comando **get /clickhouse-1/topo**.

```
[zk: 192.168.20.36:24002(CONNECTED) 0] get /clickhouse/topo

<topo>
  <mcluster>
    <shard id="14" index="1">
      <server id="15">
        <replica>1</replica>
        <az>AZ1</az>
        <host>192-168-20-205</host>
        <port>21427</port>
      </server>
      <server id="16">
        <replica>2</replica>
        <az>AZ1</az>
        <host>192-168-20-2205</host>
        <port>21427</port>
      </server>
    </shard>
  </mcluster>
</topo>
```

Paso 6 Seleccione un host del shard deseado y despliegue el host en otra zona de disponibilidad.

Paso 7 Inicie sesión en FusionInsight Manager, click **Host**, seleccione el host en el que ha desplegado en **Paso 6** and elija **More** > **Reinstall** para reinstalar el host.

Paso 8 Elija **Cluster** > **Cross-AZ HA**, haga clic en **Configure AZ and Policy** y cambie la información de AZ del host reinstalado a la AZ planificado en **Paso 6**.

Paso 9 Espere cinco minutos y compruebe si la alarma está desactivada.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 10**.

Recopilar información de fallas.

Paso 10 En FusionInsight Manager, elija **O&M** > **Log** > **Download**.

Paso 11 Expanda la lista desplegable junto al campo **Service**. En el cuadro de diálogo **Services** que se muestra, seleccione **ClickHouseServer** para el clúster de destino.

Paso 12 Expanda la lista **Hosts**. En el cuadro de diálogo **Select Host** que se muestra, seleccione el host anormal y haga clic en **OK**.

Paso 13 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 1 hora antes y después del tiempo de generación de alarma, respectivamente. A continuación, haga clic en **Download**.

Paso 14 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

Información relacionada

Ninguna

9.272 ALM-45434 Existe una única réplica en la tabla de datos de ClickHouse

Descripción

Esta alarma se genera cuando se detecta una única réplica en un clúster lógico personalizado después de que el clúster lógico personalizado esté habilitado para ClickHouse.

Esta alarma se borra automáticamente cuando el sistema detecta que el clúster lógico personalizado utiliza varias réplicas.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
45434	Grave	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster o sistema para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.

Nombre	Significado
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

Si se produce un error de hardware, los datos no se pueden restaurar.

Causas posibles

El archivo **metrika.xml** del directorio de configuración ClickHouse contiene la configuración de réplica única.

Procedimiento

Compruebe si la configuración en metrika.xml de la instancia ClickHouse es correcta.

Paso 1 En la lista de alarmas del FusionInsight Manager, busque la fila que contiene la alarma y haga clic en ⌄ para ver el nombre del host para el que se genera la alarma. En la página **Hosts**, vea la dirección IP del host basada en el nombre del host.

Paso 2 Inicie sesión en el host donde la instancia ClickHouse es anormal, vaya al directorio de configuración de la instancia ClickHouse y ejecute los siguientes comandos:

cd ${BIGDATA_HOME}/**FusionInsight_ClickHouse_***Version*/x_x_**ClickHouseServer/etc**

cat metrika.xml

Paso 3 Vea el número de particiones en cada clúster lógico personalizado y compruebe que existe una única réplica. A continuación, vaya a **Paso 4**.

NOTA

Si una partición contiene solo un nodo, existe una única réplica en un clúster lógico, como se muestra a continuación:

```
<shard>
  <internal_replication>true</internal_replication>
  <replica>
    <host>host-name1</host>
    <port>port</port>
    <user>clickhouse</user>
    <password/>
  </replica>
</shard>
```

Recopilar información de fallas.

Paso 4 En FusionInsight Manager, seleccione **O&M**. En el panel de navegación de la izquierda, elija **Log** > **Download**.

Paso 5 Expanda la lista desplegable **Service** y seleccione **ClickHouse** para el clúster de destino.

Paso 6 Expanda la lista desplegable **Hosts**. En el cuadro de diálogo **Select Host** que se muestra, seleccione el host anormal y haga clic en **OK**.

Paso 7 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 1 hora antes y después del tiempo de generación de alarma, respectivamente. A continuación, haga clic en **Download**.

Paso 8 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

Información relacionada

Ninguna

9.273 ALM-45585 Servicio IoTDB no disponible

Descripción

El sistema comprueba el estado del servicio IoTDB cada 300 segundos. Esta alarma se genera cuando el servicio IoTDB no está disponible. Esta alarma se borra cuando se recupera el servicio IoTDB.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
45585	Crítica	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

Los usuarios no pueden usar el servicio IoTDB correctamente.

Causas posibles

- El servicio KrbServer es anormal.
- Más del 50% de las instancias de IoTDBServer son defectuosas.

Procedimiento

Compruebe si el servicio KrbServer del que depende IoTDB es anormal.

Paso 1 En FusionInsight Manager, seleccione **O&M** > **Alarm** > **Alarms**.

Paso 2 En la lista de alarmas, compruebe si existe ALM-25500 Servicio KrbServer no disponible.

- En caso afirmativo, vaya a **Paso 3**.
- Si no, vaya a **Paso 5**.

Paso 3 Maneje la alarma haciendo referencia a "ALM-25500 Servicio KrbServer no disponible."

Paso 4 Después de que el ALM-25500 se haya borrado, espere unos minutos y compruebe si el servicio HetuServer de alarma no disponible está borrado.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 5**.

Compruebe si hay instancias IoTDBServer defectuosas.

Paso 5 En FusionInsight Manager, elija **Cluster** > *Name of the desired cluster* > **Service** > **IoTDB** > **Instance**.

Paso 6 Compruebe si el porcentaje de instancias de IoTDBServer defectuosas supera el 50%. En caso afirmativo, reinicie las instancias de IoTDBServer defectuosas y compruebe si se ha restaurado el estado.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 7**.

Recopilar información de fallas.

Paso 7 En FusionInsight Manager, seleccione **O&M**. En el panel de navegación de la izquierda, elija **Log** > **Download**.

Paso 8 Expanda la lista desplegable **Service**, seleccione **IoTDB** para el clúster de destino y haga clic en **OK**.

Paso 9 Haga clic en  en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 30 minutos antes y después del tiempo de generación de alarmas respectivamente. A continuación, haga clic en **Download**.

Paso 10 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

Información relacionada

Ninguna

9.274 ALM-45586 El uso de memoria de heap de IoTDBServer supera el umbral

Descripción

El sistema comprueba el estado del proceso IoTDBServer cada 60 segundos. La alarma se genera cuando el uso de memoria heap del proceso IoTDBServer excede el umbral (90% de la memoria máxima).

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
45586	Grave	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

Si la memoria heap de procesos IoTDBServer disponible es insuficiente, se produce un desbordamiento de memoria y el servicio se interrumpe.

Causas posibles

La memoria heap del proceso IoTDBServer se utiliza en exceso o la memoria heap se asigna de forma inadecuada.

Procedimiento

Comprobar el uso de memoria heap.

Paso 1 Inicie sesión en FusionInsight Manager y elija **O&M**. En el panel de navegación de la izquierda, elija **Alarm** > **Alarms**. En la página que se muestra, busque la fila que contiene la alarma cuyo **Alarm ID** es **45586**, vea el nombre del rol en **Location** y compruebe la dirección IP de la instancia.

Paso 2 Elija **Cluster** > *Name of the desired cluster* > **Service** > **IoTDB** > **Instance**. Haga clic en IoTDBServer para el que se genera la alarma para ir a **Dashboard**. Haga clic en la lista desplegable en la esquina superior derecha del área del gráfico y elija **Customize** > **Memory**. En el cuadro de diálogo que se muestra, seleccione **IoTDBServer Heap Memory Resource Percentage** y haga clic en **OK**. Comprueba si la memoria no-heap utilizada por el proceso IoTDBServer alcanza el 90% (por defecto) de la memoria no-heap máxima especificada para IoTDBServer.

- En caso afirmativo, vaya a **Paso 3**.
- Si no, vaya a **Paso 5**.

Paso 3 Elija **Cluster** > *Name of the desired cluster* > **Service** > **IoTDB** > **Configuration**, haga clic en **All Configurations**, elija **IoTDBServer** > **System** y aumente el valor de **-Xmx** en el parámetro **GC_OPTS**.

NOTA

- El valor predeterminado de **Xmx** es **2G**.
- Si esta alarma se genera ocasionalmente, aumente el valor en 0.5 veces. Si esta alarma se genera con frecuencia, duplique el valor.
- En el caso de un gran volumen de servicio y una alta simultaneidad de servicio, se recomienda agregar instancias.

Paso 4 Verifique si la alarma se ha borrado.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 5**.

Recopilar información de fallas.

Paso 5 En FusionInsight Manager, seleccione **O&M**. En el panel de navegación de la izquierda, elija **Log** > **Download**.

Paso 6 Expanda la lista desplegable **Service**, seleccione **IoTDB** para el clúster de destino y haga clic en **OK**.

Paso 7 Haga clic en  en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 30 minutos antes y después del tiempo de generación de alarmas respectivamente. A continuación, haga clic en **Download**.

Paso 8 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

Información relacionada

Ninguna

9.275 ALM-45587 La duración de GC de IoTDBServer supera el umbral

Descripción

El sistema comprueba la duración de GC del proceso IoTDBServer cada 60 segundos. Esta alarma se genera cuando la duración de GC excede el umbral (12 segundos por defecto) durante tres veces consecutivas. Puede elegir **O&M** > **Alarm** > **Threshold Configuration** > *Name of the desired cluster* > **IoTDB** > **GC** > **Total GC duration of IoTDBServer process (IoTDBServer)** para cambiar el umbral. Esta alarma se borra cuando la duración de GC es menor que el umbral.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
45587	Grave	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger Condition	Especifica el umbral para activar la alarma.

Impacto en el sistema

Una larga duración de GC del proceso IoTDBServer puede interrumpir los servicios.

Causas posibles

La memoria heap del proceso IoTDBServer se usa en exceso o se asigna de forma inadecuada, lo que provoca la ocurrencia frecuente del proceso GC.

Procedimiento

Comprobar la duración del GC.

Paso 1 Inicie sesión en FusionInsight Manager y elija **O&M**. En el panel de navegación de la izquierda, elija **Alarm** > **Alarms**. En la página que se muestra, busque la fila que contiene la alarma cuyo **Alarm ID** es **45587**, vea el nombre del rol en **Location** y compruebe la dirección IP de la instancia.

Paso 2 Elija **Cluster** > *Name of the desired cluster* > **Service** > **IoTDB** > **Instance**. Haga clic en IoTDBServer para el que se genera la alarma para ir a **Dashboard**. Haga clic en la lista desplegable situada en la esquina superior derecha del área del gráfico y elija **Customize** > **GC**. En el cuadro de diálogo que se muestra, seleccione **Garbage Collection (GC) Time of IoTDBServer** y haga clic en **OK**. Compruebe si el tiempo de GC del proceso IoTDBServer es superior a 12 segundos.

- En caso afirmativo, vaya a **Paso 3**.
- Si no, vaya a **Paso 5**.

Paso 3 Elija **Cluster** > *Name of the desired cluster* > **Service** > **IoTDB** > **Configuration**, haga clic en **All Configurations**, elija **IoTDBServer** > **System** y aumente el valor de **-Xmx** en el parámetro **GC_OPTS**.

NOTA

- El valor predeterminado de **Xmx** es **2G**.
- Si esta alarma se genera ocasionalmente, aumente el valor en 0.5 veces. Si esta alarma se genera con frecuencia, duplique el valor.
- En el caso de un gran volumen de servicio y una alta simultaneidad de servicio, se recomienda agregar instancias.

Paso 4 Verifique si la alarma se ha borrado.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 5**.

Recopilar información de fallas.

Paso 5 En FusionInsight Manager, seleccione **O&M**. En el panel de navegación de la izquierda, elija **Log** > **Download**.

Paso 6 Expanda la lista desplegable **Service**, seleccione **IoTDB** para el clúster de destino y haga clic en **OK**.

Paso 7 Haga clic en  en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 30 minutos antes y después del tiempo de generación de alarmas respectivamente. A continuación, haga clic en **Download**.

Paso 8 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

Información relacionada

Ninguna

9.276 ALM-45588 El uso de memoria directa de IoTDBServer supera el umbral

Descripción

El sistema comprueba el uso de memoria directa del servicio IoTDBServer cada 60 segundos. Esta alarma se genera cuando el uso de memoria de la instancia de IoTDBServer excede el umbral (90% de la memoria máxima) durante cinco veces consecutivas. Esta alarma se borra cuando el uso de memoria directa de IoTDBServer es menor o igual que el umbral.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
45588	Grave	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger Condition	Especifica el umbral para activar la alarma.

Impacto en el sistema

El desbordamiento de la memoria directa puede provocar una falla en el servicio.

Causas posibles

La memoria directa del proceso IoTDBServer se utiliza en exceso o la memoria directa se asigna de forma inadecuada.

Procedimiento

Comprobar el uso de la memoria directa.

Paso 1 Inicie sesión en FusionInsight Manager y elija **O&M**. En el panel de navegación de la izquierda, elija **Alarm** > **Alarms**. En la página que se muestra, busque la fila que contiene la alarma cuyo **Alarm ID** es **45588**, vea el nombre del rol en **Location** y compruebe la dirección IP de la instancia.

Paso 2 Elija **Cluster** > *Name of the desired cluster* > **Service** > **IoTDB** > **Instance**. Haga clic en IoTDBServer para el que se genera la alarma para ir a **Dashboard**. Haga clic en la lista desplegable en la esquina superior derecha del área del gráfico y elija **Customize** > **Memory**. En el cuadro de diálogo que se muestra, seleccione **IoTDBServer Direct Buffer Resource Percentage** y haga clic en **OK**.

Paso 3 Compruebe si la memoria directa utilizada por el IoTDBServer alcanza el umbral (90% de la memoria directa máxima de forma predeterminada).

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Paso 6**.

Paso 4 En FusionInsight Manager, elija **Cluster** > *Name of the desired cluster* > **Service** > **IoTDB** > **Configuration**, haga clic en **All Configurations**, y elija **IoTDBServer** > **System**, aumente el valor de **-XX:MaxDirectMemorySize** en el parámetro **GC_OPTS** según sea necesario y guarde la configuración.

NOTA

- Si se genera esta alarma, la memoria directa configurada para el proceso IoTDBServer no puede cumplir con los requisitos del proceso IoTDBServer.
- Se recomienda establecer **-XX:MaxDirectMemorySize** en **GC_OPTS** al doble de la memoria directa utilizada por el proceso IoTDBServer. (Puede cambiar el valor según el escenario de servicio real.)
- Para obtener el tamaño de la memoria directa utilizada por el proceso IoTDBServer, elija **Customize** > **Memory** > **IoTDBServer Direct Memory Resource Status**. Si **GC_OPTS** no contiene el parámetro **-XX:MaxDirectMemorySize**, agréguelo manualmente.

Paso 5 Reinicie los servicios o instancias afectados y compruebe si la alarma está desactivada.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 6**.

Recopilar información de fallas.

Paso 6 En FusionInsight Manager, seleccione **O&M**. En el panel de navegación de la izquierda, elija **Log** > **Download**.

Paso 7 Expanda la lista desplegable **Service** y seleccione **IoTDBServer** para el clúster de destino.

Paso 8 Haga clic en  en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 9 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

Información relacionada

Ninguna

9.277 ALM-45589 El uso de memoria heap de ConfigNode supera el umbral

Descripción

El sistema comprueba el uso de memoria heap del proceso ConfigNode cada 60 segundos. Esta alarma se genera cuando el uso de memoria heap del proceso ConfigNode excede el umbral (90% de la memoria máxima). Esta alarma se borra cuando el uso de memoria heap del proceso ConfigNode es menor que el umbral.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
45589	Grave	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

Si el uso de memoria heap del proceso ConfigNode es demasiado alto, el rendimiento del proceso ConfigNode se ve afectado, e incluso el proceso ConfigNode no está disponible debido al desbordamiento de memoria.

Causas posibles

La memoria heap configurada para el nodo es incorrecta. Como resultado, el uso excede el umbral.

Procedimiento

Comprobar la configuración de memoria heap.

Paso 1 Inicie sesión en FusionInsight Manager, seleccione **O&M** > **Alarm** > **Alarms**. En la lista de alarmas en tiempo real, haga clic en delante de esta alarma y vea el nombre del rol y la dirección IP de la instancia en **Location**.

Paso 2 Elija **Cluster** >**Services** >**IoTDB**. Haga clic en **Instance**, haga clic en ConfigNode correspondiente a la dirección IP obtenida en **Paso 1**, y compruebe si **ConfigNode Heap Memory Usage** en la página de pestaña **Dashboard** alcanza el umbral especificado para el proceso ConfigNode.

Si no se muestra el gráfico, haga clic en la lista desplegable en la esquina superior derecha del área del gráfico y elija **Customize** > **Memory**. En el cuadro de diálogo que se muestra, seleccione **ConfigNode Heap Memory Usage** y haga clic en **OK**.

NOTA

Puede elegir **O&M** > **Alarm** > **Threshold Configuration** > *Name of the desired cluster* > **IoTDB** > **Memory** > **ConfigNode Heap Memory Usage (ConfigNode)** para ver el umbral.

- En caso afirmativo, vaya a **Paso 3**.
- Si no, vaya a **Paso 6**.

Paso 3 Elija **Cluster** >**Services** >**IoTDB**. Haga clic en **Configurations**, luego en **All Configurations**, haga clic en **ConfigNode**, y elija **System**. Establezca **-Xmx** en **GC_OPTS** en un valor mayor y guarde la configuración.

NOTA

- El valor predeterminado de **Xmx** es **2G**.
- Si esta alarma se genera ocasionalmente, aumente el valor de **-Xmx** en 0.5 veces. Si esta alarma se genera con frecuencia, duplique el valor de **-Xmx**.
- En el caso de un gran volumen de servicio y una alta simultaneidad de servicio, se recomienda agregar instancias.

Paso 4 Haga clic en **Dashboard**. Haga clic en **Restart Service** para reiniciar el servicio IoTDB para que la configuración surta efecto.

Paso 5 Espere unos 120 segundos y compruebe si la alarma está desactivada.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 6**.

Recopilar información de fallas.

Paso 6 En FusionInsight Manager, elija **O&M** > **Log** > **Download**.

Paso 7 Expanda la lista desplegable **Service**, seleccione **IoTDB** para el clúster de destino y haga clic en **OK**.

Paso 8 Expanda la lista desplegable **Hosts**. En el cuadro de diálogo **Select Host** que se muestra, seleccione los hosts a los que pertenece el rol y haga clic en **OK**.

Paso 9 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 30 minutos antes y después del tiempo de generación de alarmas respectivamente. A continuación, haga clic en **Download**.

Paso 10 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

Información relacionada

Ninguna

9.278 ALM-45590 La duración de GC de ConfigNode supera el umbral

Descripción

El sistema comprueba la duración GC del proceso ConfigNode cada 60 segundos. Esta alarma se genera cuando la duración de GC excede el umbral (12 segundos por defecto) durante tres veces consecutivas. Esta alarma se borra cuando la duración de GC es menor que el umbral.

NOTA

Puede elegir **O&M** > **Alarm** > **Threshold Configuration** > *Name of the desired cluster* > **IoTDB** > **GC** > **Total GC duration of ConfigNode process (ConfigNode)** para aumentar el umbral en un 20% cada vez.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
45590	Grave	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger Condition	Especifica el umbral para activar la alarma.

Impacto en el sistema

Una larga duración de GC del proceso ConfigNode puede interrumpir los servicios.

Causas posibles

La memoria heap configurada en el nodo es incorrecta. Como resultado, la GC ocurre con frecuencia.

Procedimiento

Comprobar la configuración de memoria heap.

Paso 1 Inicie sesión en FusionInsight Manager, seleccione **O&M** > **Alarm** > **Alarms**. En la lista de alarmas en tiempo real, haga clic en en la fila que contiene esta alarma y vea el nombre del rol y la dirección IP de la instancia de **Location**.

Paso 2 Elija **Cluster** >**Services** >**IoTDB**. Haga clic en **Instance** y haga clic en el ConfigNode correspondiente a la dirección IP obtenida por **Paso 1**. Cambie a la página de la pestaña **Dashboard**, busque el gráfico **Total GC Duration of ConfigNode** y compruebe si la duración de GC del proceso ConfigNode excede el umbral.

Si no se muestra la duración GC de ConfigNode, haga clic en la lista desplegable en la esquina superior derecha del área del gráfico y elija **Customize** > **GC**. En el cuadro de diálogo que se muestra, seleccione **Total GC Duration of ConfigNode** y haga clic en **OK**.

NOTA

Puede elegir **O&M** > **Alarm** > **Threshold Configuration** > *Name of the desired cluster* > **IoTDB** > **GC** > **Total GC duration of ConfigNode process (ConfigNode)** para ver el umbral.

- En caso afirmativo, vaya a **Paso 3**.
- Si no, vaya a **Paso 6**.

Paso 3 Elija **Cluster** >**Services** >**IoTDB**. Haga clic en **Configurations**, luego en **All Configurations**, haga clic en **ConfigNode**, y elija **System**. Establezca **-Xmx** en **GC_OPTS** en un valor mayor y guarde la configuración.

NOTA

- El valor predeterminado de **Xmx** es **2G**.
- Si esta alarma se genera ocasionalmente, aumente el valor en 0.5 veces. Si esta alarma se genera con frecuencia, duplique el valor.
- En el caso de un gran volumen de servicio y una alta simultaneidad de servicio, se recomienda agregar instancias.

Paso 4 Haga clic en **Dashboard**. Haga clic en **Restart Service** para reiniciar el servicio IoTDB para que la configuración surta efecto.

Paso 5 Verifique si la alarma se ha borrado.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 6**.

Recopilar información de fallas.

Paso 6 En FusionInsight Manager, elija **O&M** > **Log** > **Download**.

Paso 7 Expanda la lista desplegable **Service**, seleccione **IoTDB** para el clúster de destino y haga clic en **OK**.

Paso 8 Expanda la lista desplegable **Hosts**. En el cuadro de diálogo **Select Host** que se muestra, seleccione los hosts a los que pertenece el rol y haga clic en **OK**.

Paso 9 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 30 minutos antes y después del tiempo de generación de alarmas respectivamente. A continuación, haga clic en **Download**.

Paso 10 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

Información relacionada

Ninguna

9.279 ALM-45591 El uso de memoria directa de ConfigNode supera el umbral

Descripción

El sistema comprueba el uso de memoria directa del proceso ConfigNode cada 60 segundos. Esta alarma se genera cuando el uso de memoria directa del ConfigNode excede el umbral durante cinco veces consecutivas. Es decir, la memoria directa configurada para ConfigNode no puede cumplir con los requisitos de servicio. Esta alarma se borra cuando el uso de memoria directa de ConfigNode es menor o igual que el umbral.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
45591	Grave	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.

Nombre	Significado
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.
Trigger Condition	Especifica el umbral para activar la alarma.

Impacto en el sistema

El desbordamiento de la memoria directa puede hacer que la instancia de IoTDB no esté disponible.

Causas posibles

La memoria directa configurada para el nodo es incorrecta. Como resultado, el uso excede el umbral.

Procedimiento

Comprobar la configuración de memoria directa.

Paso 1 Inicie sesión en FusionInsight Manager, seleccione **O&M** > **Alarm** > **Alarms**. En la lista de alarmas en tiempo real, haga clic en delante de esta alarma y vea el nombre del rol y la dirección IP de la instancia en **Location**.

Paso 2 Elija **Cluster** >**Services** >**IoTDB**. Haga clic en **Instance**, haga clic en el ConfigNode correspondiente a la dirección IP obtenida en **Paso 1** y compruebe si **ConfigNode Direct Memory Usage** en la página de pestaña **Dashboard** alcanza el umbral especificado para el proceso ConfigNode (90% del máximo de memoria directa de forma predeterminada).

Si no se muestra el gráfico, haga clic en la lista desplegable en la esquina superior derecha del área del gráfico y elija **Customize** > **Memory**. En el cuadro de diálogo que se muestra, seleccione **ConfigNode Direct Memory Usage** y haga clic en **OK**.

- En caso afirmativo, vaya a **Paso 3**.
- Si no, vaya a **Paso 5**.

Paso 3 En FusionInsight Manager, seleccione **Cluster** > *Name of the desired cluster* > **Services** > **IoTDB**. Haga clic en **Configurations** y luego en **All Configurations**. Haga clic en **ConfigNode** y seleccione **System**. Establezca **-XX:MaxDirectMemorySize** en **GC_OPTS** en un valor mayor según sea necesario y guarde la configuración.

NOTA

- Se recomienda establecer **-XX:MaxDirectMemorySize** en **GC_OPTS** al doble de la memoria directa utilizada por el proceso ConfigNode. (Puede cambiar el valor según el escenario de servicio real.)
- Para obtener el tamaño de la memoria directa utilizada por el proceso ConfigNode, elija **Customize** > **Memory** > **ConfigNode Direct Memory Resource Status**.
- Si **GC_OPTS** no contiene el parámetro **-XX:MaxDirectMemorySize**, agréguelo.

Paso 4 Reinicie el servicio o instancias de IoTDB afectados y compruebe si la alarma está borrada.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 5**.

Recopilar información de fallas.

Paso 5 En FusionInsight Manager, elija **O&M** > **Log** > **Download**.

Paso 6 Expanda la lista desplegable **Service** y seleccione **ConfigNode** para el clúster de destino.

Paso 7 Expanda la lista desplegable **Hosts**. En el cuadro de diálogo **Select Host** que se muestra, seleccione los hosts a los que pertenece el rol y haga clic en **OK**.

Paso 8 Haga clic en  en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 9 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

Información relacionada

Ninguna

9.280 ALM-45592 La duración de ejecución de IoTDBServer RPC supera el umbral

Descripción

El sistema comprueba la duración de ejecución de RPC del proceso IoTDBServer cada 60 segundos. Esta alarma se genera cuando la duración de ejecución excede el umbral. Esta alarma se borra cuando el tiempo de ejecución de RPC del proceso IoTDBServer es menor que el umbral.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
45592	Grave	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

El rendimiento de ejecución del proceso IoTDBServer se ve afectado.

Causas posibles

La duración de procesamiento de una solicitud IoTDBServer RPC excede el umbral. Los registros necesitan ser analizados más a fondo para localizar la causa.

Procedimiento

Recopilar información de fallas.

Paso 1 Inicie sesión en FusionInsight Manager, seleccione **O&M** > **Alarm** > **Alarms**. En la lista de alarmas en tiempo real, haga clic en delante de esta alarma y vea el nombre del rol y la dirección IP de la instancia en **Location**.

Paso 2 Elija **O&M** >**Log** >**Download**.

Paso 3 Expanda la lista desplegable **Service**, seleccione **IoTDB** para el clúster de destino y haga clic en **OK**.

Paso 4 Expanda la lista desplegable **Hosts**. En el cuadro de diálogo **Select Host** que se muestra, seleccione el host consultado en **Paso 1** y haga clic en **OK**.

Paso 5 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 30 minutos antes y después del tiempo de generación de alarmas respectivamente. A continuación, haga clic en **Download**.

Paso 6 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

Información relacionada

Ninguna

9.281 ALM-45593 La duración de ejecución de descarga de IoTDBServer supera el umbral

Descripción

Esta alarma se genera cuando la duración de flush de datos excede el umbral. Esta alarma se borra cuando la duración de flush es menor que el umbral.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
45593	Grave	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

La escritura de datos se bloquea y el rendimiento de la operación de escritura se ve afectado.

Causas posibles

El flushing de IoTDB en el nodo es lento. Es necesario analizar más a fondo los registros.

Procedimiento

Recopilar información de fallas.

Paso 1 Inicie sesión en FusionInsight Manager, seleccione **O&M** > **Alarm** > **Alarms**. En la lista de alarmas en tiempo real, haga clic en delante de esta alarma y vea el nombre del rol y la dirección IP de la instancia en **Location**.

Paso 2 Elija **O&M** >**Log** >**Download**.

Paso 3 Expanda la lista desplegable **Service**, seleccione **IoTDB** para el clúster de destino y haga clic en **OK**.

Paso 4 Expanda la lista desplegable **Hosts**. En el cuadro de diálogo **Select Host** que se muestra, seleccione el host consultado en **Paso 1** y haga clic en **OK**.

Paso 5 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 30 minutos antes y después del tiempo de generación de alarmas respectivamente. A continuación, haga clic en **Download**.

Paso 6 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

Información relacionada

Ninguna

9.282 ALM-45594 La duración de la fusión intraespacial de IoTDBServer supera el umbral

Descripción

Esta alarma se genera cuando la duración de fusión en el espacio excede el umbral. Esta alarma se borra cuando la duración de fusión en el espacio es menor que el umbral.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
45594	Grave	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.

Nombre	Significado
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

La escritura de datos se bloquea y el rendimiento de la operación de escritura se ve afectado.

Causas posibles

La tarea de fusión en el espacio IoTDB del nodo es lenta. Es necesario analizar más a fondo los registros.

Procedimiento

Recopilar información de fallas.

Paso 1 Inicie sesión en FusionInsight Manager, seleccione **O&M** > **Alarm** > **Alarms**. En la lista de alarmas en tiempo real, haga clic en delante de esta alarma y vea el nombre del rol y la dirección IP de la instancia en **Location**.

Paso 2 Elija **O&M** >**Log** >**Download**.

Paso 3 Expanda la lista desplegable **Service**, seleccione **IoTDB** para el clúster de destino y haga clic en **OK**.

Paso 4 Expanda la lista desplegable **Hosts**. En el cuadro de diálogo **Select Host** que se muestra, seleccione el host consultado en **Paso 1** y haga clic en **OK**.

Paso 5 Haga clic en  en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 30 minutos antes y después del tiempo de generación de alarmas respectivamente. A continuación, haga clic en **Download**.

Paso 6 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

Información relacionada

Ninguna

9.283 ALM-45595 La duración de la fusión entre espacios de IoTDBServer supera el umbral

Descripción

Esta alarma se genera cuando la duración de fusión de espacio cruzado excede el umbral. Esta alarma se borra cuando la duración de la fusión entre espacios es menor que el umbral.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
45595	Grave	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

La escritura de datos se bloquea y el rendimiento de la operación de escritura se ve afectado.

Causas posibles

La tarea de combinación de espacios cruzados de IoTDB en el nodo es lenta. Es necesario analizar más a fondo los registros.

Procedimiento

Recopilar información de fallas.

Paso 1 Inicie sesión en FusionInsight Manager, seleccione **O&M** > **Alarm** > **Alarms**. En la lista de alarmas en tiempo real, haga clic en delante de esta alarma y vea el nombre del rol y la dirección IP de la instancia en **Location**.

Paso 2 Elija **O&M** >**Log** >**Download**.

Paso 3 Expanda la lista desplegable **Service**, seleccione **IoTDB** para el clúster de destino y haga clic en **OK**.

Paso 4 Expanda la lista desplegable **Hosts**. En el cuadro de diálogo **Select Host** que se muestra, seleccione el host consultado en **Paso 1** y haga clic en **OK**.

Paso 5 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 30 minutos antes y después del tiempo de generación de alarmas respectivamente. A continuación, haga clic en **Download**.

Paso 6 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

Información relacionada

Ninguna

9.284 ALM-45615 Servicio CDL no disponible

Descripción

El sistema comprueba el estado de salud de la CDL cada 60 segundos. Esta alarma se genera cuando el estado de salud de CDL es **DOWN**. Esta alarma se borra cuando el sistema detecta que el estado de salud de CDL es **UP**.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
45615	Crítica	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.

Nombre	Significado
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

El servicio de CDL es anormal. No puede utilizar FusionInsight Manager para realizar operaciones de clúster en el servicio CDL. La función de servicio CDL no está disponible.

Causas posibles

Todas las instancias de CDLService o CDLConnector del servicio CDL son anormales y el servicio Kafka no está disponible.

Procedimiento

Compruebe si el servicio Kafka del que depende el servicio CDL es anormal.

Paso 1 En FusionInsight Manager, seleccione **O&M** > **Alarm** > **Alarms**.

Paso 2 En la lista de alarmas, compruebe si existe ALM-38000 Servicio Kafka no disponible.

- En caso afirmativo, vaya a **Paso 3**.
- Si no, vaya a **Paso 5**.

Paso 3 Manejar la alarma haciendo referencia a "ALM-38000 Servicio Kafka no disponible".

Paso 4 Después de que la alarma esté desactivada, espere unos minutos y compruebe si la alarma Servicio HetuServer no disponible está borrada.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 5**.

Compruebe si las instancias CDL están defectuosas.

Paso 5 En FusionInsight Manager, elija **Cluster** > *Name of the desired cluster* > **Service** > **CDL** > **Instance**.

Paso 6 Compruebe si todas las instancias CDLService y CDLConnector son defectuosas.

- En caso afirmativo, reinicie el servicio CDL y elija **Cluster** > *Name of the desired cluster* > **Services** > **CDL** > **More** > **Restart Service**. Si la falla persiste después del reinicio, vaya a **Paso 7** y póngase en contacto con el personal de O&M para verificar los registros de CDL.
- Si no, vaya a **Paso 7**.

Recopilar información de fallas.

Paso 7 En FusionInsight Manager, seleccione **O&M**. En el panel de navegación de la izquierda, elija **Log** > **Download**.

Paso 8 Expanda la lista desplegable **Service** y seleccione **CDL** para el clúster de destino.

Paso 9 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 30 minutos antes y después del tiempo de generación de alarmas respectivamente. A continuación, haga clic en **Download**.

Paso 10 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Después de que se restablezca el servicio, el sistema borra automáticamente la alarma.

Información relacionada

Ninguna

9.285 ALM-45616 Excepción de ejecución de trabajo de CDL

Descripción

El sistema comprueba si un trabajo de CDL es normal cada 60 segundos. Esta alarma se notifica cuando el trabajo de CDL es anormal. Esta alarma se borra cuando se restablece o se detiene el trabajo.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
45616	Grave	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
JobName	Especifica el trabajo para el que se genera la alarma.
Username	Especifica el nombre de usuario del trabajo para el que se genera la alarma.

Impacto en el sistema

Esta alarma no tiene impacto en el sistema.

Causas posibles

La tarea CDL no se puede ejecutar debido a una configuración de parámetros incorrecta u otras razones. En la página **Job Management** de la interfaz de usuario web de CDL, busque la fila donde se encuentra el trabajo y haga clic en **Failed**/**Abnormal running** en la columna **Status** para ver la causa de error o ver la causa de error en los registros.

Procedimiento

Paso 1 Inicie sesión en FusionInsight Manager como un usuario que tiene el permiso de creación de trabajos de CDL o administrador.

Paso 2 Elija **O&M**. En el panel de navegación de la izquierda, elija **Alarm** > **Alarms**, haga clic en en la fila donde **Alarm ID** es **45616**, y vea el nombre del trabajo para el que se genera esta alarma en **Location**.

Paso 3 Elija **Cluster** > **Services** > **CDL** y haga clic en el enlace situado junto a la **CDLService UI** para ir a la interfaz de usuario web de CDL.

Paso 4 Busque la fila en la que se encuentra el trabajo fallido en función del nombre del trabajo obtenido en **Paso 2** y haga clic en **Abnormal running** o **Failed** en al columna **Status**.

Paso 5 En la página que se muestra, vea la información de error y rectifique el error. Por ejemplo, **Figura 9-123** muestra que la tarea que se ejecuta en Yarn se elimina manualmente. Para obtener más información, consulte la información de error de seguimiento, como se muestra en **Figura 9-124**.

Figura 9-123 Excepción de trabajo de CDL

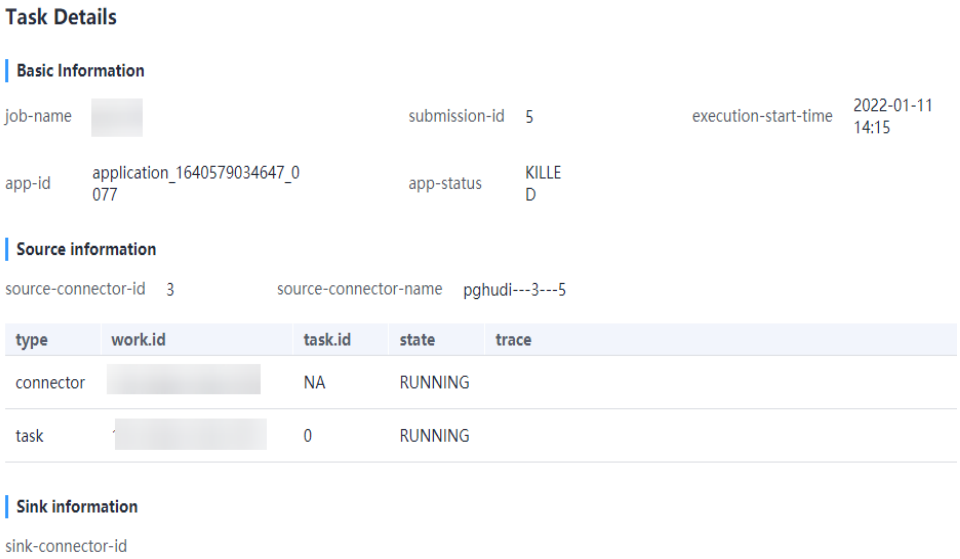
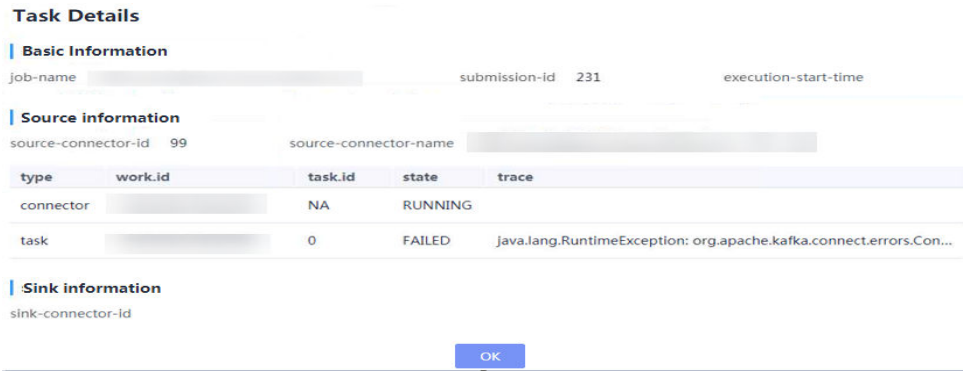


Figura 9-124 Rastrear información de error



Paso 6 Rectifique el error basado en la información de error, ejecute la tarea de nuevo y compruebe si la tarea se puede ejecutar correctamente.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 7**.

Recopilar información de fallas.

Paso 7 En FusionInsight Manager, seleccione **O&M**. En el panel de navegación de la izquierda, elija **Log** > **Download**.

Paso 8 Seleccione **CDL** en el clúster necesario para **Service**.

Paso 9 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 30 minutos antes y después del tiempo de generación de alarmas respectivamente. A continuación, haga clic en **Download**.

Paso 10 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Después de que el trabajo se restablezca o se detenga con éxito, la alarma se borra si se ha notificado.

Información relacionada

Ninguna

9.286 ALM-45617 Los datos en cola en la ranura de replicación CDL superan el umbral

Descripción

Si un gran número de registros de escritura anticipada (WAL) se apilan en la base de datos de PostgreSQL, el espacio de disco PostgreSQL puede ser utilizado. El sistema comprueba si la cantidad de datos en cola en la ranura de replicación configurada para un trabajo de CDL excede el umbral cada 5 minutos. Esta alarma se genera cuando la cantidad de datos en cola

en la ranura de replicación excede el umbral. Esta alarma se borra cuando el número de datos en cola en la ranura de replicación cae por debajo del umbral.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
45617	Grave	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
JobName	Especifica el trabajo para el que se genera la alarma.
DBName	Especifica la base de datos para la que se genera la alarma.
SlotName	Especifica la ranura de replicación de la base de datos para la que se genera la alarma.
Lag	Especifica los datos en cola en la ranura.

Impacto en el sistema

Los WAL se acumulan continuamente en la base de datos PostgreSQL de origen, lo que provoca que se agote el espacio en disco de la base de datos de origen.

Causas posibles

El trabajo de CDL es anormal y el procesamiento de datos se detiene; la base de datos de origen se actualiza rápidamente y el procesamiento de datos de CDL es lento.

Procedimiento

Paso 1 Inicie sesión en FusionInsight Manager como un usuario que tiene el permiso de creación de trabajos de CDL o administrador.

Paso 2 Elija **O&M**. En el panel de navegación de la izquierda, elija **Alarm** > **Alarms**, haga clic en en la fila donde **Alarm ID** es **45617**, y vea el nombre del trabajo para el que se genera esta alarma en **Location**.

Paso 3 Compruebe si aparece **ALM-45616 CDL Job Execution Exception** en la lista de alarmas.

- En caso afirmativo, maneje la alarma realizando las operaciones previstas para el **ALM-45616 Excepción de ejecución de trabajo CDL**.
- Si no, vaya a **Paso 4**.

Paso 4 Elija **Cluster** >**Services** >**CDL**. Haga clic en el enlace junto a **CDLService UI** para ir a la interfaz de usuario web de CDL y comprobar si el trabajo se muestra en la lista de trabajos basándose en su nombre obtenido en **Paso 2**.

- En caso afirmativo, verifique si el trabajo es anormal.
  - Si es anormal, vaya a **Paso 5**.
  - Si no lo es, el procesamiento de datos es lento. Póngase en contacto con .
- Si no, vaya a **Paso 7**.

Paso 5 Haga clic en **Abnormal** o **Failed** en la fila donde se encuentra el trabajo y rectifique el error basándose en la información de error mostrada en la página.

Paso 6 Después de rectificar la falla, vuelva a ejecutar el trabajo y compruebe si el trabajo se puede ejecutar correctamente.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 7**.

Recopilar información de fallas.

Paso 7 En FusionInsight Manager, seleccione **O&M**. En el panel de navegación de la izquierda, elija **Log** > **Download**.

Paso 8 Seleccione **CDL** en el clúster necesario para **Service**.

Paso 9 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 30 minutos antes y después del tiempo de generación de alarmas respectivamente. A continuación, haga clic en **Download**.

Paso 10 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra cuando la cantidad de datos en cola en la ranura de replicación es menor que el umbral. No es necesario borrar manualmente la alarma.

Información relacionada

Ninguna

9.287 ALM-45635 Error de ejecución de trabajos de FlinkServer

Esta sección se aplica a MRS 3.1.2 o posterior.

Descripción

El sistema comprueba si los trabajos de FlinkServer no se ejecutan cada 10 segundos. Esta alarma se genera cuando falla un trabajo de FlinkServer. Esta alarma se borra cuando el trabajo se reinicia correctamente.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
45635	Grave	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
JobName	Especifica el trabajo para el que se genera la alarma.

Impacto en el sistema

Esta alarma no tiene impacto en el sistema.

Causas posibles

Puede ver las causas de errores en registros específicos.

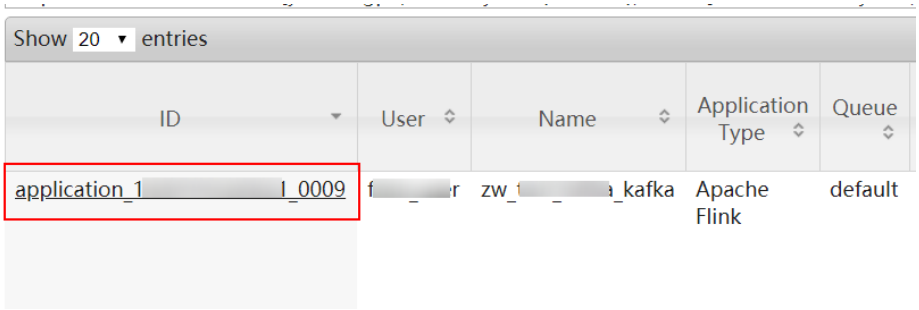
Procedimiento

Paso 1 Inicie sesión en Manager como un usuario que tiene el permiso de gestión FlinkServer.

Paso 2 Elija **Cluster** > **Services** > **Yarn** y haga clic en el enlace junto a **ResourceManager WebUI** para ir a la página de Yarn.

Paso 3 Localice el trabajo que ha fallado basándose en su nombre mostrado en **Location**, busque y registre el ID de aplicación del trabajo que ha fallado y compruebe si los registros del trabajo están disponibles en la página Yarn.

Figura 9-125 ID de aplicación de un trabajo



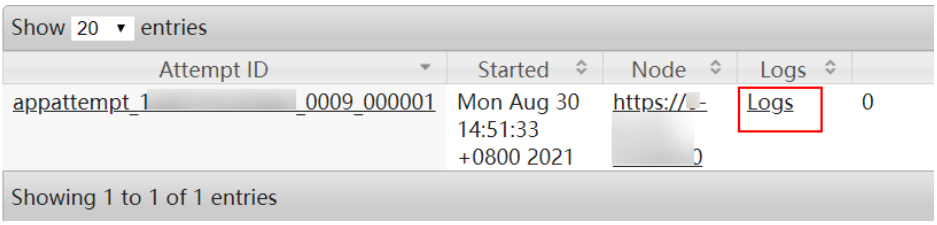
En caso afirmativo, vaya a **Paso 4**.

Si no, vaya a **Paso 6**.

Paso 4 Haga clic en el ID de aplicación del trabajo que ha fallado para ir a la página de trabajo.

1. Haga clic en **Logs** en la columna **Logs** para ver los registros de JobManager.

Figura 9-126 Hacer clic en los registros



2. Haga clic en el ID en la columna **Attempt ID** y haga clic en **Logs** en la columna **Logs** para ver los registros de TaskManager.

Figura 9-127 Haga clic en el ID en la columna Attempt ID

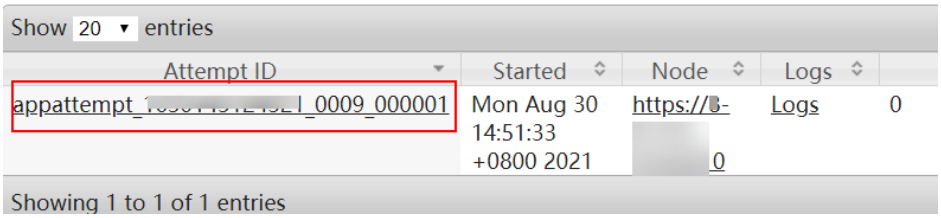
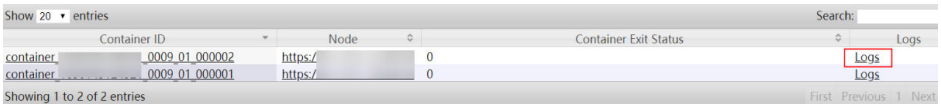


Figura 9-128 Hacer clic en los registros



NOTA

También puede iniciar sesión en Manager como un usuario que tiene el permiso de gestión FlinkServer, elija **Cluster** > **Services** > **Flink**, haga clic en el enlace junto a **Flink WebUI**. En la interfaz de usuario web de Flink mostrada, haga clic en **Job Management** y elija **More** > **Job Monitoring** en la columna **Operation** para ver los registros TaskManager.

Paso 5 Vea los registros del trabajo fallido para rectificar el fallo, o póngase en contacto con el personal del y envíe los registros de fallas recopiladas. No se requiere ninguna otra acción.

Si los registros no están disponibles en la página Yarn, descargue los registros desde HDFS.

Paso 6 En Administrador, elija **Cluster** > **Services** > **HDFS**, haga clic en el enlace junto a **NameNode WebUI** para ir a la página HDFS, seleccione **Utilities** > **Browse the file system**, y descargue los registros en el directorio **/tmp/logs/***User name*/**logs/***Application ID of the failed job*.

Paso 7 Vea los registros del trabajo fallido para rectificar el fallo, o póngase en contacto con el personal del y envíe los registros de fallas recopiladas.

----Fin

Eliminación de alarmas

Después de que el trabajo se reinicie correctamente, la alarma se borra si se ha notificado.

Información relacionada

Ninguna

9.288 ALM-45636 Checkpoints de trabajo de FlinkServer siguen fallando

Esta sección se aplica a MRS 3.1.2 o posterior.

Descripción

El sistema comprueba el número de fallas de checkpoint consecutivos basándose en el intervalo de comprobación de alarma configurado. Esta alarma se genera cuando el número de fallas de checkpoint consecutivos de un trabajo de FlinkServer alcanza el umbral configurado. Esta alarma se borra cuando se recuperan checkpoints o el trabajo se reinicia correctamente.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
45636	Menor	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
JobName	Especifica el trabajo para el que se genera la alarma.

Impacto en el sistema

Esta alarma no tiene impacto en el sistema.

Causas posibles

Puede ver las causas de errores en registros específicos.

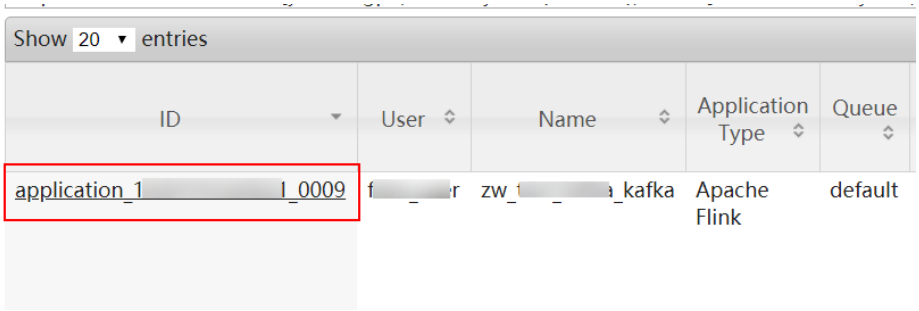
Procedimiento

Paso 1 Inicie sesión en Manager como un usuario que tiene el permiso de gestión FlinkServer.

Paso 2 Elija **Cluster** > **Services** > **Yarn** y haga clic en el enlace junto a **ResourceManager WebUI** para ir a la página de Yarn.

Paso 3 Localice el trabajo que ha fallado basándose en su nombre mostrado en **Location**, busque y registre el ID de aplicación del trabajo que ha fallado y compruebe si los registros del trabajo están disponibles en la página Yarn.

Figura 9-129 ID de aplicación de un trabajo



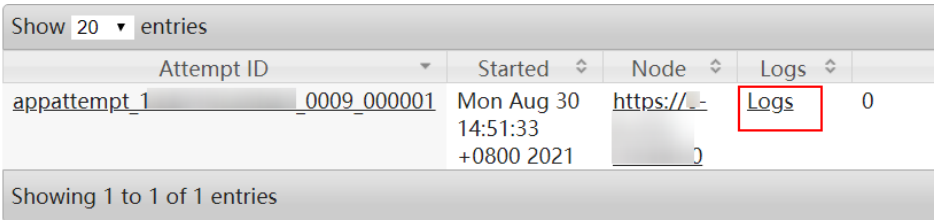
En caso afirmativo, vaya a **Paso 4**.

Si no, vaya a **Paso 6**.

Paso 4 Haga clic en el ID de aplicación del trabajo que ha fallado para ir a la página de trabajo.

1. Haga clic en **Logs** en la columna **Logs** para ver los registros de JobManager.

Figura 9-130 Hacer clic en los registros



2. Haga clic en el ID en la columna **Attempt ID** y haga clic en **Logs** en la columna **Logs** para ver los registros de TaskManager.

Figura 9-131 Haga clic en el ID en la columna Attempt ID

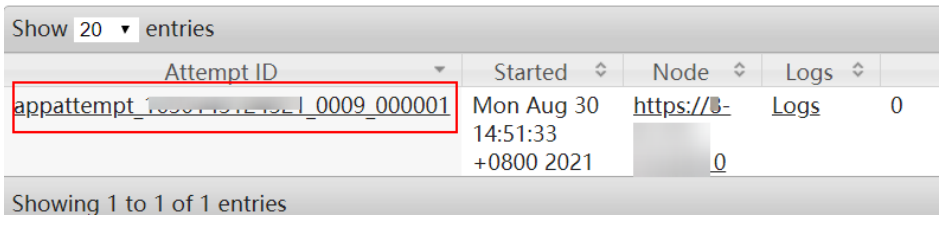
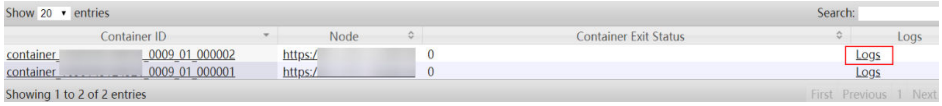


Figura 9-132 Hacer clic en los registros



NOTA

También puede iniciar sesión en Manager como un usuario que tiene el permiso de gestión FlinkServer, elija **Cluster** > **Services** > **Flink**, haga clic en el enlace junto a **Flink WebUI**. En la interfaz de usuario web de Flink mostrada, haga clic en **Job Management** y elija **More** > **Job Monitoring** en la columna **Operation** para ver los registros TaskManager.

Paso 5 Vea los registros del trabajo fallido para rectificar el fallo, o póngase en contacto con el personal del y envíe los registros de fallas recopiladas. No se requiere ninguna otra acción.

Si los registros no están disponibles en la página Yarn, descargue los registros desde HDFS.

Paso 6 En Administrador, elija **Cluster** > **Services** > **HDFS**, haga clic en el enlace junto a **NameNode WebUI** para ir a la página HDFS, seleccione **Utilities** > **Browse the file system**, y descargue los registros en el directorio **/tmp/logs/***User name*/**logs/***Application ID of the failed job*.

Paso 7 Vea los registros del trabajo fallido para rectificar el fallo, o póngase en contacto con el personal del y envíe los registros de fallas recopiladas.

----Fin

Eliminación de alarmas

Esta alarma se borra cuando se recuperan los checkpoints de trabajos de FlinkServer o el trabajo se reinicia correctamente.

Información relacionada

Ninguna

9.289 ALM-45637 Task de FlinkServer está continuamente bajo presión de retorno

Esta sección se aplica a MRS 3.1.2 o posterior.

Descripción

El sistema comprueba la duración de la contrapresión de tasks de FlinkServer basándose en el intervalo de comprobación de alarma configurado. Esta alarma se genera cuando la duración de la contrapresión de una task de FlinkServer alcanza el umbral configurado. Esta alarma se borra cuando se recupera la contrapresión de la task o el trabajo se reinicia correctamente.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
45637	Menor	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
JobName	Especifica el trabajo para el que se genera la alarma.

Impacto en el sistema

Esta alarma no tiene impacto en el sistema.

Causas posibles

Puede ver las causas en los registros específicos.

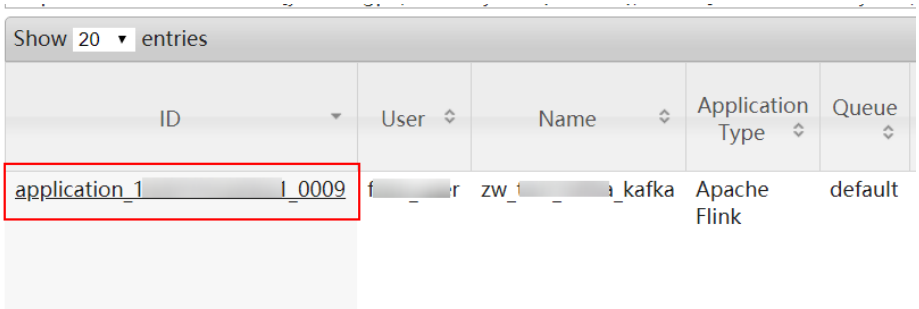
Procedimiento

Paso 1 Inicie sesión en Manager como un usuario que tiene el permiso de gestión FlinkServer.

Paso 2 Elija **Cluster** > **Services** > **Yarn** y haga clic en el enlace junto a **ResourceManager WebUI** para ir a la página de Yarn.

Paso 3 Localice el trabajo que ha fallado basándose en su nombre mostrado en **Location**, busque y registre el ID de aplicación del trabajo que ha fallado y compruebe si los registros del trabajo están disponibles en la página Yarn.

Figura 9-133 ID de aplicación de un trabajo



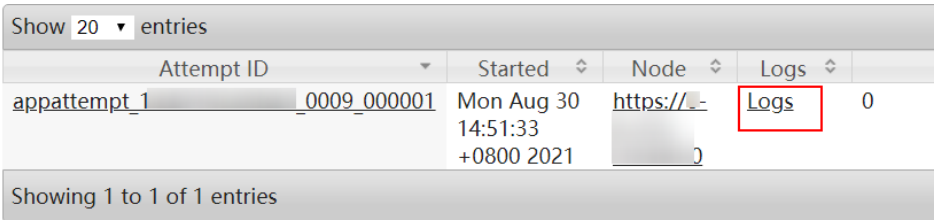
En caso afirmativo, vaya a **Paso 4**.

Si no, vaya a **Paso 6**.

Paso 4 Haga clic en el ID de aplicación del trabajo que ha fallado para ir a la página de trabajo.

1. Haga clic en **Logs** en la columna **Logs** para ver los registros de JobManager.

Figura 9-134 Hacer clic en los registros



2. Haga clic en el ID en la columna **Attempt ID** y haga clic en **Logs** en la columna **Logs** para ver los registros de TaskManager.

Figura 9-135 Haga clic en el ID en la columna Attempt ID

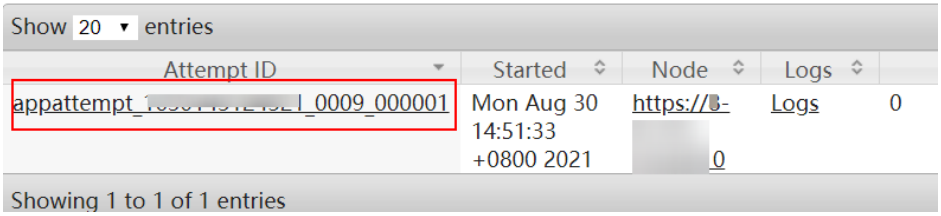
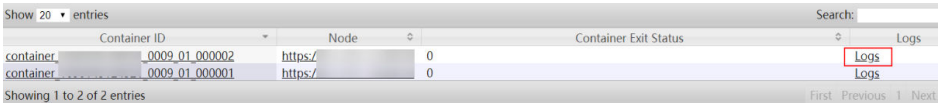


Figura 9-136 Hacer clic en los registros



NOTA

También puede iniciar sesión en Manager como un usuario que tiene el permiso de gestión FlinkServer, elija **Cluster** > **Services** > **Flink**, haga clic en el enlace junto a **Flink WebUI**. En la interfaz de usuario web de Flink mostrada, haga clic en **Job Management** y elija **More** > **Job Monitoring** en la columna **Operation** para ver los registros TaskManager.

Paso 5 Vea los registros del trabajo fallido para rectificar el fallo, o póngase en contacto con el personal del y envíe los registros de fallas recopiladas. No se requiere ninguna otra acción.

Si los registros no están disponibles en la página Yarn, descargue los registros desde HDFS.

Paso 6 En Administrador, elija **Cluster** > **Services** > **HDFS**, haga clic en el enlace junto a **NameNode WebUI** para ir a la página HDFS, seleccione **Utilities** > **Browse the file system**, y descargue los registros en el directorio **/tmp/logs/***User name*/**logs/***Application ID of the failed job*.

Paso 7 Vea los registros del trabajo fallido para rectificar el fallo, o póngase en contacto con el personal del y envíe los registros de fallas recopiladas.

----Fin

Eliminación de alarmas

Esta alarma se borra cuando se recupera la contrapresión de task de FlinkServer o se reinicia correctamente el trabajo.

Información relacionada

Ninguna

9.290 ALM-45638 El número de reinicios tras fallas de trabajo de FlinkServer supera el umbral

Esta sección se aplica a MRS 3.1.2 o posterior.

Descripción

El sistema comprueba el número de reinicios de trabajo de FlinkServer en función del intervalo de comprobación de alarma. Esta alarma se genera cuando el número excede el umbral configurado. Esta alarma se borra cuando se reinicia el trabajo.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
45638	Menor	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
JobName	Especifica el trabajo para el que se genera la alarma.

Impacto en el sistema

Esta alarma no tiene impacto en el sistema.

Causas posibles

Puede ver las causas en los registros específicos.

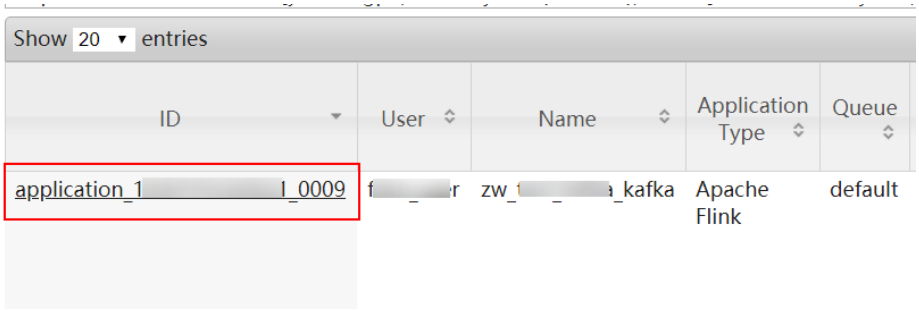
Procedimiento

Paso 1 Inicie sesión en Manager como un usuario que tiene el permiso de gestión FlinkServer.

Paso 2 Elija **Cluster** > **Services** > **Yarn** y haga clic en el enlace junto a **ResourceManager WebUI** para ir a la página de Yarn.

Paso 3 Localice el trabajo que ha fallado basándose en su nombre mostrado en **Location**, busque y registre el ID de aplicación del trabajo que ha fallado y compruebe si los registros del trabajo están disponibles en la página Yarn.

Figura 9-137 ID de aplicación de un trabajo



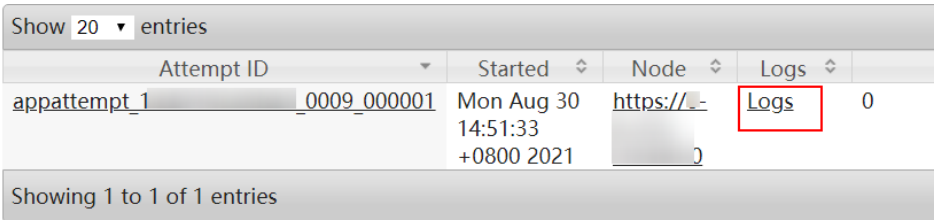
En caso afirmativo, vaya a **Paso 4**.

Si no, vaya a **Paso 6**.

Paso 4 Haga clic en el ID de aplicación del trabajo que ha fallado para ir a la página de trabajo.

1. Haga clic en **Logs** en la columna **Logs** para ver los registros de JobManager.

Figura 9-138 Hacer clic en los registros



2. Haga clic en el ID en la columna **Attempt ID** y haga clic en **Logs** en la columna **Logs** para ver los registros de TaskManager.

Figura 9-139 Haga clic en el ID en la columna Attempt ID

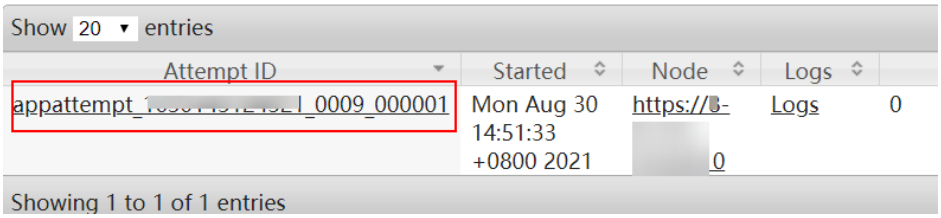
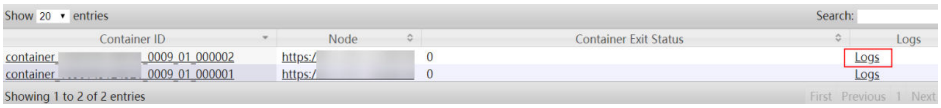


Figura 9-140 Hacer clic en los registros



NOTA

También puede iniciar sesión en Manager como un usuario que tiene el permiso de gestión FlinkServer, elija **Cluster** > **Services** > **Flink**, haga clic en el enlace junto a **Flink WebUI**. En la interfaz de usuario web de Flink mostrada, haga clic en **Job Management** y elija **More** > **Job Monitoring** en la columna **Operation** para ver los registros TaskManager.

Paso 5 Vea los registros del trabajo fallido para rectificar el fallo, o póngase en contacto con el personal del y envíe los registros de fallas recopiladas. No se requiere ninguna otra acción.

Si los registros no están disponibles en la página Yarn, descargue los registros desde HDFS.

Paso 6 En Administrador, elija **Cluster** > **Services** > **HDFS**, haga clic en el enlace junto a **NameNode WebUI** para ir a la página HDFS, seleccione **Utilities** > **Browse the file system**, y descargue los registros en el directorio **/tmp/logs/***User name*/**logs/***Application ID of the failed job*.

Paso 7 Vea los registros del trabajo fallido para rectificar el fallo, o póngase en contacto con el personal del y envíe los registros de fallas recopiladas.

----Fin

Eliminación de alarmas

Esta alarma se borra cuando el trabajo FlinkServer se reinicia correctamente.

Información relacionada

Ninguna

9.291 ALM-45639 Checkpointing of a Flink Job Times Out

Description

The system checks the checkpointing timeout of Flink jobs every 30 seconds. This alarm is generated if the checkpointing timeout of a Flink job is longer than the threshold (600 seconds by default). This alarm is cleared when the checkpointing timeout of a job is less than or equal to the threshold.

Attribute

Alarm ID	Alarm Severity	Auto Clear
45639	Minor	Yes

Parameters

Name	Meaning
Source	Specifies the cluster for which the alarm is generated.
ServiceName	Specifies the service for which the alarm is generated.
JobName	Specifies the job for which the alarm is generated.
UserName	Specifies the username for which the alarm is generated.

Impact on the System

This alarm has no impact on the system.

Possible Causes

The job may be in the sub-healthy state. The possible causes are as follows:

- The memory for the TaskManager of the job is insufficient.
- The state memory is too large, making checkpointing time-consuming.

Procedure

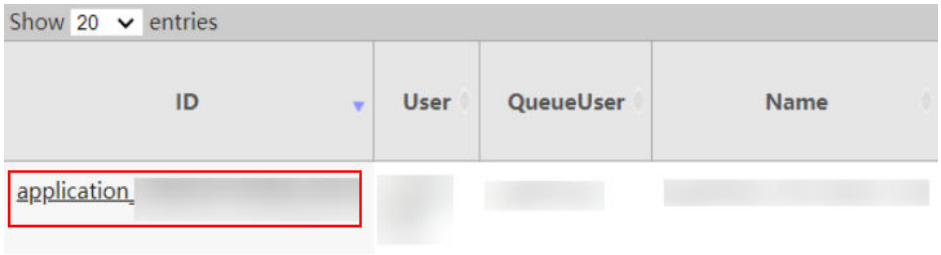
Paso 1 Log in to Manager as a user who has the FlinkServer management permission.

Paso 2 Choose **O&M** > **Alarm** > **Alarms** > **ALM-45639 Checkpointing of a Flink Job Times Out**, view **Location**, and obtain the name of the task for which the alarm is generated.

Paso 3 Choose **Cluster** > **Services** > **Yarn** and click the link next to **ResourceManager WebUI** to go to the native Yarn page.

Paso 4 Locate the failed task based on its name displayed in **Location**, search for and record the application ID of the job, and check whether the job logs are available on the Yarn page.

Figura 9-141 Application ID of a job

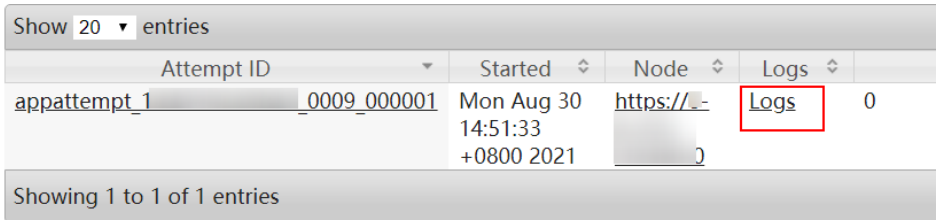


- If yes, go to **Paso 5**.
- If no, go to **Paso 7**.

Paso 5 Click the application ID of the failed job to go to the job page.

1. Click **Logs** in the **Logs** column to view JobManager logs.

Figura 9-142 Clicking Logs



2. Click the ID in the **Attempt ID** column and click **Logs** in the **Logs** column to view TaskManager logs.

Figura 9-143 Clicking the ID in the Attempt ID column

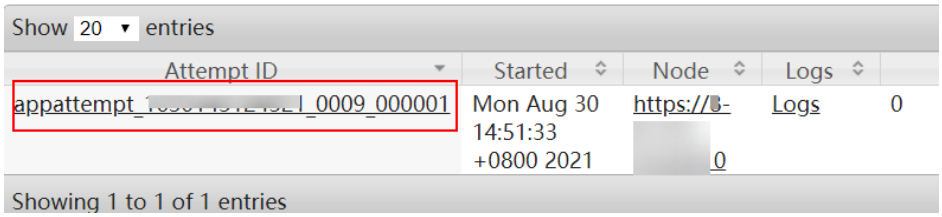
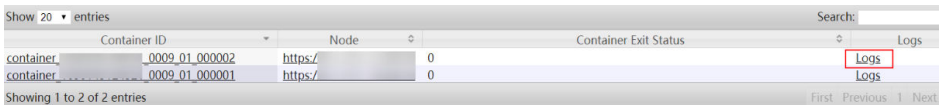


Figura 9-144 Clicking Logs



NOTA

You can also log in to Manager as a user who has the FlinkServer management permission. Choose **Cluster** > **Services** > **Flink**, and click the link next to **Flink WebUI**. On the displayed Flink web UI, click **Job Management**, click **More** in the **Operation** column, and select **Job Monitoring** to view TaskManager logs.

Paso 6 View the logs of the failed job to rectify the fault, or contact the and send the collected fault logs. No further action is required.

If logs are unavailable on the Yarn page, download logs from HDFS.

Paso 7 On Manager, choose **Cluster** > **Services** > **HDFS**, click the link next to **NameNode WebUI** to go to the HDFS page, choose **Utilities** > **Browse the file system**, and download logs in the **/tmp/logs/***Username*/**logs/***Application ID of the failed job* directory.

Paso 8 View the logs of the failed job to rectify the fault, or contact the and send the collected fault logs.

----Fin

Alarm Clearing

This alarm is cleared when the checkpointing timeout a Flink job is less than or equal to the threshold.

Related Information

None

9.292 ALM-45640 Interrupción de latidos de FlinkServer entre los nodos activos y en espera

Esta sección se aplica a MRS 3.2.0 o posterior.

Descripción

Esta alarma se genera cuando el nodo activo o el nodo en espera de FlinkServer no recibe mensajes de latidos del extremo opuesto durante 30 segundos (duración de interrupción de latidos configurado en Keepalive).

Esta alarma se borra cuando se recupera el latido del corazón.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
45640	Menor	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

Durante la interrupción del latido de FlinkServer, solo un nodo puede proporcionar el servicio. Si este nodo es defectuoso, no hay ningún nodo en espera disponible para la conmutación por error y el servicio no está disponible.

Causas posibles

- La instancia de FlinkServer activa o en espera está en el estado detenido.
- La NIC de la dirección IP flotante del sistema HA utilizado por el nodo FlinkServer está configurada incorrectamente. FlinkServer no se inicia.

- El enlace entre los nodos FlinkServer activo y en espera es anormal.

Procedimiento

Comprobar el estado de instancias de FlinkServer activas y en espera.

Paso 1 Inicie sesión en FusionInsight Manager, elija **Cluster** > **Services** > **Flink** > **Instance** y compruebe que el estado de FlinkServer es normal.

- En caso afirmativo, vaya a **Paso 3**.
- Si no, vaya a **Paso 2**.

Paso 2 Seleccione la instancia anormal de FlinkServer e inicie la instancia. Después de iniciar la instancia, compruebe si la alarma está borrada.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 3**.

Comprobar si el enlace entre los nodos FlinkServer en espera es normal.

Paso 3 Elija **Cluster** > **Services** > **Flink** > **Instance** y compruebe las dos direcciones IP de servicio de FlinkServer.

Paso 4 Inicie sesión en el servidor donde se encuentra la instancia anormal de FlinkServer como usuario **root**.

Paso 5 Ejecute el siguiente comando para comprobar si el servidor de la otra instancia de FlinkServer es accesible:

ping *IP address of the other FlinkServer instance*

- En caso afirmativo, vaya a **Paso 8**.
- Si no, vaya a **Paso 6**.

Paso 6 Pida al administrador de red que maneje la excepción de red.

Paso 7 Verifique si la alarma se ha borrado.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 8**.

Comprobar si los registros del nodo en el que se encuentra la instancia de FlinkServer anormal contienen información sobre errores.

Paso 8 Inicie sesión en el servidor donde se encuentra la instancia anormal de FlinkServer como usuario **root**.

Paso 9 Abra el archivo de registro en el directorio predeterminado **/var/log/Bigdata/flink/flinkserver/prestart.log** y compruebe si hay un mensaje de error **Float ip** *x.x.x.x* **is invalid**.

- En caso afirmativo, vaya a **Paso 10**.
- Si no, vaya a **Paso 12**.

Paso 10 En FusionInsight Manager, elija **Cluster** > **Services** > **Flink** > **Configurations** > **All Configurations** y busque **flink.ha.floatip**. Cambie el valor del parámetro a la dirección IP flotante correcta, guarde la configuración y reinicie el servicio Flink.

NOTA

Póngase en contacto con el ingeniero de red para obtener la nueva dirección IP flotante.

Paso 11 Verifique si la alarma se ha borrado.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 12**.

Recopilar información de fallas.

Paso 12 En FusionInsight Manager, seleccione **O&M** > **Log** > **Download**.

Paso 13 Seleccione el servicio de Flink en el clúster necesario para **Service**.

Paso 14 Expanda la lista desplegable **Hosts**. En el cuadro de diálogo **Select Host** que se muestra, seleccione los hosts a los que pertenece el rol y haga clic en **OK**.

Paso 15 Haga clic en  en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 16 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

Información relacionada

Ninguna

9.293 ALM-45641 Excepción de sincronización de datos entre los nodos FlinkServer activo y en espera

Esta sección se aplica a MRS 3.2.0 o posterior.

Descripción

El sistema comprueba la sincronización de datos entre los nodos FlinkServer activo y en espera cada 60 segundos. Esta alarma se genera cuando el nodo FlinkServer en espera no puede sincronizar archivos con el nodo FlinkServer activo.

Esta alarma se borra cuando FlinkServer en espera sincroniza los archivos con FlinkServer activo.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
45641	Grave	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster o sistema para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

Debido a que los archivos de configuración del FlinkServer en espera no se actualizan, algunas configuraciones se perderán después de una conmutación activa/en espera. FlinkServer y algunos componentes pueden no funcionar correctamente.

Causas posibles

- Se interrumpe el enlace entre los nodos FlinkServer activo y en espera.
- El archivo de sincronización no existe o se requiere el permiso del archivo.

Procedimiento

Comprobar si la red entre el FlinkServer activo y en espera se encuentra en estado normal.

Paso 1 En FusionInsight Manager, elija **Cluster** > **Services** > **ClickHouse** > **Instance**. Vea y registre las direcciones IP de los FlinkServer activos y en espera.

Paso 2 Inicie sesión en el nodo FlinkServer activo como usuario **root**.

Paso 3 Ejecute el siguiente comando para comprobar si el FlinkServer en espera es accesible:

ping *IP address of the standby FlinkServer*

- En caso afirmativo, vaya a **Paso 6**.
- Si no, vaya a **Paso 4**.

Paso 4 Póngase en contacto con el administrador de la red para comprobar si la red es defectuosa.

- En caso afirmativo, vaya a **Paso 5**.
- Si no, vaya a **Paso 6**.

Paso 5 Rectifique la falla de la red y compruebe si la alarma está borrada de la lista de alarmas.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 6**.

Comprobar si el espacio de almacenamiento del directorio /srv/BigData/LocalBackup está lleno.

Paso 6 Ejecute el siguiente comando para comprobar si el espacio de almacenamiento del directorio **/srv/BigData/LocalBackup** está lleno:

df -hl /srv/BigData/LocalBackup

- En caso afirmativo, vaya a **Paso 7**.
- Si no, vaya a **Paso 10**.

Paso 7 Ejecute el siguiente comando para borrar archivos de copia de respaldo innecesarios:

rm -rf *Directory to be cleared*

Los siguientes son dos ejemplos:

rm -rf /srv/BigData/LocalBackup/0/default-oms_20191211143443

Paso 8 En FusionInsight Manager, seleccione **O&M** > **Backup and Restoration** > **Backup Management**.

En la columna **Operation** de la tarea de copia de respaldo, haga clic en **Configure** y cambie el valor de **Maximum Number of Backup Copies** para reducir el número de conjuntos de archivos de copia de respaldo.

Paso 9 Espere 1 minuto y compruebe si la alarma se ha eliminado.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 10**.

Comprobar si el archivo de sincronización existe y si el permiso del archivo es válido.

Paso 10 Ejecute el siguiente comando para comprobar si existe el archivo de sincronización:

find /srv/BigData/ -name "sed*"

find /opt -name "sed*"

- En caso afirmativo, vaya a **Paso 11**.
- Si no, vaya a **Paso 12**.

Paso 11 Ejecute el siguiente comando para comprobar la información del archivo de sincronización y los permisos consultados en **Paso 10**:

ll *Path of the file you want to search for*

- Si el tamaño del archivo es 0 y todos los valores de la columna de permisos son -, el archivo es un archivo no deseado. Ejecute el siguiente comando para eliminarlo:

  rm -rf *Files to be deleted*

  Espere varios minutos y compruebe si la alarma está desactivada. Si la alarma persiste, vaya a **Paso 12**.
- Si el tamaño del archivo no es 0, vaya a **Paso 12**.

Paso 12 Vea el archivo de registro generado cuando se notifica la alarma.

1. Ejecute el siguiente comando para ir a la ruta del archivo de registro de ejecución de HA del clúster actual:

   cd /var/log/Bigdata/flink/flinkserver/ha/runlog
2. Descomprima el archivo de registro y vea los registros generados cuando se notifica la alarma.

Por ejemplo, si el nombre del archivo es **ha.log.2021-03-22_12-00-07.gz**, ejecute el siguiente comando:

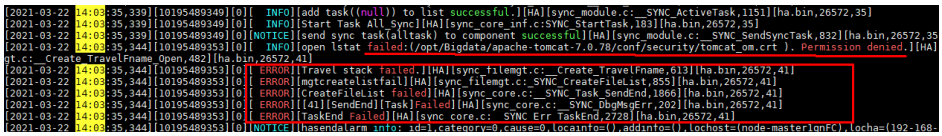
gunzip *ha.log.2021-03-22_12-00-07.gz*

vi *ha.log.2021-03-22_12-00-07*

Compruebe si la información de error se muestra antes y después del tiempo de generación de alarmas en los registros.

- Si se muestra, rectifique el error basándose en la información de error. Vaya a **Paso 13**.

  Por ejemplo, si se muestra la siguiente información de error, se requiere el permiso de directorio. En este caso, obtenga el permiso de directorio que es el mismo que el permiso en un nodo normal.



- Si no, vaya a **Paso 14**.

Paso 13 Espere unos 10 minutos y compruebe si la alarma está desactivada.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 14**.

Recopilar información de fallas.

Paso 14 En FusionInsight Manager, elija **O&M** > **Log** > **Download**.

Paso 15 Seleccione la información de FlinkServer de **Services** y haga clic en **OK**.

Paso 16 Expanda la lista desplegable **Hosts**. En el cuadro de diálogo **Select Host** que se muestra, seleccione los hosts a los que pertenece el rol y haga clic en **OK**.

Paso 17 Haga clic en en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 10 minutos antes y después del tiempo de generación de alarmas, respectivamente. A continuación, haga clic en **Download**.

Paso 18 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

Información relacionada

Ninguna

9.294 ALM-45736 Servicio Guardian no disponible

Descripción

El módulo de alarma comprueba el estado del servicio Guardian cada 60 segundos. Esta alarma se genera si Guardian no está disponible.

Esta alarma se borra después de que Guardian se recupere.

Atributo

ID de alarma	Severidad de alarma	Borrar automáticamente
45275	Crítica	Sí

Parámetros

Nombre	Significado
Source	Especifica el clúster para el que se genera la alarma.
ServiceName	Especifica el servicio para el que se genera la alarma.
RoleName	Especifica el rol para el que se genera la alarma.
HostName	Especifica el host para el que se genera la alarma.

Impacto en el sistema

Guardian no puede funcionar correctamente.

Causas posibles

- El servicio HDFS del que depende el servicio Guardian es anormal.
- La instancia de rol TokenServer es anormal.

Procedimiento

Comprobar el estado de servicio HDFS.

Paso 1 Inicie sesión en FusionInsight Manager y elija **O&M** > **Alarm** > **Alarms**. En la página que se muestra, compruebe si se notifica "ALM-14000 Servicio HDFS no disponible".

- En caso afirmativo, vaya a **Paso 2**.

- Si no, vaya a **Paso 3**.

Paso 2 Borre esta alarma de acuerdo con la ayuda de alarma.

Después de que se desactive la alarma, espere unos minutos y compruebe si la alarma GuardianService no disponible está despejado.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 3**.

Comprobar todas las instancias de TokenServer.

Paso 3 Inicie sesión en el nodo donde reside la instancia TokenServer como usuario **omm** y ejecute el comando **ps -ef|grep "com.huawei.guardian.token.server.Server"** para comprobar si el proceso TokenServer existe en el nodo.

- En caso afirmativo, vaya a **Paso 5**.
- Si no, reinicie la instancia de TokenServer defectuosa y vaya a **Paso 4**.

Paso 4 En la lista de alarmas, compruebe si la alarma "Servicio Guardian no disponible" está desactivada.

- En caso afirmativo, no es necesario hacer nada más.
- Si no, vaya a **Paso 5**.

Recopilar información de fallas.

Paso 5 En FusionInsight Manager, elija **O&M** > **Log** > **Download**.

Paso 6 Expanda la lista desplegable **Service** y seleccione **Guardian** para el clúster de destino.

Paso 7 Haga clic en  en la esquina superior derecha y establezca **Start Date** y **End Date** para la recopilación de registros en 1 hora antes y después del tiempo de generación de alarma, respectivamente. A continuación, haga clic en **Download**.

Paso 8 Póngase en contacto con y proporcione los registros recopilados.

----Fin

Eliminación de alarmas

Esta alarma se borra automáticamente después de rectificar la falla.

Información relacionada

Ninguna

10 Descripción de seguridad

10.1 Sugerencias de configuración de seguridad para clústeres con autenticación de Kerberos deshabilitada

La versión de la comunidad de Hadoop proporciona dos modos de autenticación: autenticación de Kerberos (modo de seguridad) y autenticación Simple (modo normal). Al crear un clúster, puede optar por habilitar o deshabilitar la autenticación de Kerberos.

Los clústeres en modo de seguridad utilizan el protocolo de Kerberos para la autenticación de seguridad.

En modo normal, los componentes del clúster MRS utilizan un mecanismo de autenticación de código abierto nativo, que es típicamente autenticación Simple. Si se utiliza autenticación Simple, la autenticación se realiza automáticamente por un usuario de cliente (por ejemplo, usuario **root**) de forma predeterminada cuando un cliente se conecta a un servidor. La autenticación es imperceptible para el administrador o usuario del servicio. Además, cuando se ejecuta, el cliente puede incluso pretender ser cualquier usuario (incluido **superuser**) mediante la inyección de **UserGroupInformation**. Las API de gestión de recursos de clúster y control de datos no se autentican en el servidor y son fácilmente explotadas y atacadas por piratas informáticos.

Por lo tanto, en el modo normal, los permisos de acceso a la red deben controlarse estrictamente para garantizar la seguridad del clúster. Se recomienda realizar las siguientes operaciones para garantizar la seguridad del clúster.

- Despliegue aplicaciones de servicio en ECS en la misma VPC y subred y evite el acceso a clústeres MRS a través de una red externa.
- Configure las reglas de grupo de seguridad para controlar estrictamente el ámbito de acceso. No configure reglas de acceso que permitan **Any** o **0.0.0.0** para la dirección entrante de los puertos del clúster MRS.
- Si desea acceder a las páginas nativas de los componentes del clúster desde el externo, siga las instrucciones en **Creación de un canal de SSH para conectarse a un clúster de MRS y configurar el navegador** para la configuración.

10.2 Aviso de seguridad

10.2.1 Guía para solucionar la vulnerabilidad de ejecución remota de código de Apache Log4j2 (CVE-2021-44228)

Esta sección describe cómo solucionar la vulnerabilidad de Apache log4j2 CVE-2021-44228. Actualmente, puede utilizar cualquiera de los siguientes métodos para corregir la vulnerabilidad:

- **Instalación del parche en nodos de clúster existentes**
- **Instalación del parche en nuevos nodos**

Prerrequisitos

- Ha descargado el paquete de la herramienta de parche **MRS_Log4j_Patch.tar.gz** de la ruta de OBS. Haga clic en **aquí** para descargar.
- Ha determinado el nodo OMS activo en el clúster.

  NOTA

  Generalmente, OMS se despliega en dos nodos, master1 y master2. Puede utilizar los siguientes comandos para determinar el nodo OMS activo. El nodo cuya salida del comando contiene active es el nodo OMS activo, y el nodo cuya salida del comando contiene espera es el nodo OMS en espera.

  Para los clústeres cuya versión es anterior a MRS 3.*x*, utilice el siguiente comando:

  sh /opt/Bigdata/*/workspace0/ha/module/hacom/script/get_harole.sh

  Para los clústeres cuya versión es posterior a MRS 3.*x*, utilice el siguiente comando:

  sh /opt/Bigdata/om-server*/OMS/workspace0/ha/module/hacom/script/get_harole.sh

Instalación del parche en nodos de clúster existentes

Paso 1 Cargue **MRS_Log4j_Patch.tar.gz** en el directorio **/home/omm** del nodo OMS activo. Para obtener más información, consulte **¿Cómo cargo un archivo local a un nodo dentro de un clúster?**.

Paso 2 Ejecute los siguientes comandos para iniciar sesión en el nodo OMS activo como usuario **root**, modifique el permiso de la herramienta de parche, cambie a usuario **omm** y descomprima el paquete de herramienta de parche en el directorio actual:

chown omm:wheel -R /home/omm/MRS_Log4j_Patch.tar.gz

su - omm

cd /home/omm

tar -zxf MRS_Log4j_Patch.tar.gz

Paso 3 En el archivo **/home/omm/MRS_Log4j_Patch/bin/ips.ini**, configure las direcciones IP (direcciones IP de todos los nodos del clúster actual) de los nodos donde se va a instalar el parche.

NOTA

Configure una dirección IP en cada línea. No se permite ninguna línea vacía.

Paso 4 Ejecute los siguientes scripts para instalar el parche:

cd /home/omm/MRS_Log4j_Patch/bin

nohup sh install.sh upgrade &

Ejecute el comando **tail -f nohup.out** para comprobar el estado de ejecución. Si se muestra "upgrade patch success.", la ejecución se ha completado.

Paso 5 Inicie sesión en Manager. Para obtener más información, consulte **Acceder a Manager**. Reinicie los componentes afectados (se le aconseja realizar esta operación durante las horas no pico). Para obtener más información, consulte **Lista de componentes afectados**.

Paso 6 (Opcional) Si desea instalar el parche para el cliente recién descargado, ejecute primero los siguientes comandos para instalar el parche para el paquete de componentes:

su - omm

cd /home/omm/MRS_Log4j_Patch/bin

nohup sh install.sh upgrade_package &

Ejecute el comando **tail -f nohup.out** para comprobar el estado de ejecución. Si se muestra "upgrade_package patch success.", la ejecución está completa.

Una vez completada la ejecución, el cliente descargado es el que tiene el parche instalado.

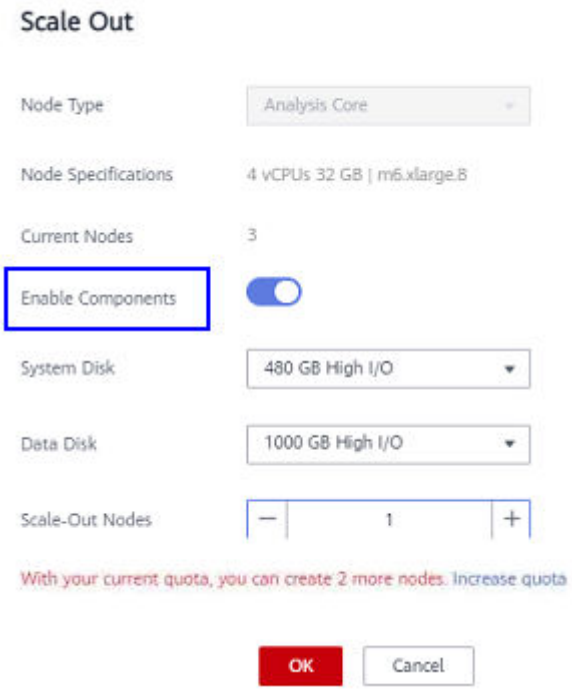
⚠ ATENCIÓN

Este paso toma un largo período de tiempo y no es necesario reiniciar el componente después de realizar este paso.

----Fin

Instalación del parche en nuevos nodos

Paso 1 Deshabilite **Enable Component** durante el escalado horizontal. Para obtener más información sobre cómo escalar un clúster, consulte **Escalamiento horizontal de un clúster**.



Paso 2 Cargue **MRS_Log4j_Patch.tar.gz** en el directorio **/home/omm** del nodo OMS activo. Para obtener más información, consulte **¿Cómo cargo un archivo local a un nodo dentro de un clúster?**.

Paso 3 Ejecute los siguientes comandos para iniciar sesión en el nodo OMS activo como usuario **root**, modifique el permiso de la herramienta de parche, cambie a usuario **omm** y descomprima el paquete de herramienta de parche en el directorio actual:

chown omm:wheel -R /home/omm/MRS_Log4j_Patch.tar.gz

su - omm

cd /home/omm

tar -zxf MRS_Log4j_Patch.tar.gz

Paso 4 En el archivo **/home/omm/MRS_Log4j_Patch/bin/ips.ini**, configure las direcciones IP (Direcciones IP de los nuevos nodos en el clúster actual) de los nodos donde se va a instalar el parche.

NOTA

Configure una dirección IP en cada línea. No se permite ninguna línea vacía.

Paso 5 Ejecute los siguientes scripts para instalar el parche:

cd /home/omm/MRS_Log4j_Patch/bin

nohup sh install.sh upgrade &

Ejecute el comando **tail -f nohup.out** para comprobar el estado de ejecución. Si se muestra "upgrade patch success.", la ejecución se ha completado.

Paso 6 Inicie sesión en Manager. Para obtener más información, consulte **Acceder a Manager**. Inicie las instancias en los nuevos nodos.

----Fin

Desinstalación del parche

Paso 1 Inicie sesión en el nodo OMS activo como usuario **root** y ejecute los siguientes comandos para desinstalar el parche:

su - omm

cd /home/omm/MRS_Log4j_Patch/bin

nohup sh install.sh rollback &

Ejecute el comando **tail -f nohup.out** para comprobar el estado de ejecución. Si se muestra "rollback patch success.", la ejecución está completa.

Paso 2 Inicie sesión en Manager. Para obtener más información, consulte **Acceder a Manager**. Reinicie los componentes afectados (se le aconseja realizar esta operación durante las horas no pico). Para obtener más información, consulte **Lista de componentes afectados**.

Paso 3 Realice la siguiente operación si ha realizado **Paso 6** en **Instalación del parche en nodos de clúster existentes** durante la instalación del parche y desea deshacer la modificación en el paquete de componentes:

Inicie sesión en el nodo OMS activo como usuario **root** y ejecute los siguientes comandos:

su - omm

cd /home/omm/MRS_Log4j_Patch/bin

nohup sh install.sh rollback_package &

Ejecute el comando **tail -f nohup.out** para comprobar el estado de ejecución. Si se muestra "rollback_package patch success.", la ejecución está completa.

----Fin

(Opcional) Actualización del complemento de restablecimiento de contraseña de ECS

Huawei Cloud ECS proporciona la función de restablecimiento de contraseña con un solo clic. Si la contraseña de un ECS se pierde o caduca, puede utilizar esta función para restablecer la contraseña con unos pocos clics. El complemento de restablecimiento de contraseña es un proceso cliente que se ejecuta en el ECS y no proporciona ningún servicio de red externo. El complemento de restablecimiento de contraseña CloudResetPwdUpdateAgent utiliza el componente Log4j2 de Apache. Según el análisis y verificación del laboratorio de seguridad de Huawei Cloud, el complemento de restablecimiento de contraseña ECS no tiene riesgos de seguridad.

Para actualizar la versión de Log4j2 en este complemento, realice los siguientes pasos:

Paso 1 Cargue **MRS_Log4j_Patch.tar.gz** en el directorio **/home/omm** del nodo OMS activo. Para obtener más información, consulte **¿Cómo cargo un archivo local a un nodo dentro de un clúster?**.

Paso 2 Ejecute los siguientes comandos para iniciar sesión en el nodo OMS activo como usuario **root**, modifique el permiso de la herramienta de parche, cambie a usuario **omm** y descomprima el paquete de herramienta de parche en el directorio actual:

chown omm:wheel -R /home/omm/MRS_Log4j_Patch.tar.gz

su - omm

cd /home/omm

tar -zxf MRS_Log4j_Patch.tar.gz

Paso 3 En el archivo **/home/omm/MRS_Log4j_Patch/bin/ips.ini**, configure las direcciones IP (direcciones IP de todos los nodos del clúster actual) de los nodos donde se va a instalar el parche.

NOTA

Configure una dirección IP en cada línea. No se permite ninguna línea vacía.

Paso 4 Realice los siguientes pasos basados en el modo de inicio de sesión del nodo:

- **Password login**

  Ejecute el siguiente comando:

  nohup sh install.sh upgrade_resetpwdagent passwd:*Login password* **&**

  Por ejemplo, si la contraseña es **xyz123**, ejecute el siguiente comando:

  nohup sh install.sh upgrade_resetpwdagent passwd:xyz123 &

  Ejecute el comando **tail -f nohup.out** para comprobar el estado de ejecución. Si se muestra "upgrade_resetpwdagent patch success.", la ejecución está completa.

- **Key login**

  a. Cargue el archivo de clave privada del usuario **root** al directorio **/home/omm/MRS_Log4j_Patch/bin** y asegúrese de que el grupo de propietarios del archivo sea **root:root**. Luego, ejecute los siguientes comandos:

  chown root:root /home/omm/MRS_Log4j_Patch/bin/*Key file*

  chmod 644 /home/omm/MRS_Log4j_Patch/bin/*Key file*

  b. Ejecute los siguientes comandos:

  su - omm

  cd /home/omm/MRS_Log4j_Patch/bin

  nohup sh install.sh upgrade_resetpwdagent privatekey:*Path of the private key file &*

  Por ejemplo, si la ruta del archivo de clave privada es **/home/omm/MRS_Log4j_Patch/bin/abc.pem**, ejecute el siguiente comando:

  nohup sh install.sh upgrade_resetpwdagent privatekey:/home/omm/MRS_Log4j_Patch/bin/abc.pem &

  Ejecute el comando **tail -f nohup.out** para comprobar el estado de ejecución. Si se muestra "upgrade_resetpwdagent patch success.", la ejecución está completa.

----Fin

Lista de componentes afectados

Versión de clúster de MRS	Componente afectado
MRS 3.1.1	Hive, Oozie, Flink, Ranger y Tez
MRS 3.1.0	Hive, Flink, Spark, Tez, Impala, Ranger, Presto y Oozie
MRS 3.0.5	Hive, Flink, Spark, Tez, Impala, Ranger, Presto, Oozie, Storm, y Loader
MRS 3.0.2	Hive, Flink, Spark, Tez, Ranger, Oozie, Storm, y Loader
MRS 2.1.1	Hive, Tez, Storm, Loader, Impala, y Presto
MRS 2.1.0	Loader, Hive, Storm, Presto, Impala, Tez, Spark, y HBase
MRS 1.9.3	Loader, Hive, Tez, Spark, y Flink
MRS 1.9.2	Loader, Hive, Tez, Spark, Flink, y Impala
MRS 1.9.0	Loader, Hive, Spark, y Flink
MRS 1.8.10	Loader y Storm
MRS 1.7.1	Loader y Storm

10.2.2 Guía de remediación de vulnerabilidades de MRS Fastjson

10.2.2.1 Descripción

Síntoma

Se divulga una vulnerabilidad de ejecución remota de código de deserialización en Fastjson 1.2.80 y versiones anteriores. Un atacante puede utilizar esta vulnerabilidad para omitir la restricción autoType de modo que pueda ejecutar de forma remota cualquier código.

Impacto y Riesgo

Si se ataca un servicio con una vulnerabilidad, los atacantes pueden ejecutar código arbitrario de forma remota en la plataforma de servicio.

Medidas preventivas y sugerencias

Antes de proponer cualquier solución, se recomienda tomar las siguientes medidas preventivas:

1. Reforzar los límites de seguridad de los dispositivos físicos para evitar el acceso directo desde redes externas y ataques al plano de gestión de red interna.
2. Compruebe si cada nodo componente de la plataforma utiliza la contraseña predeterminada. Si es así, cambie la contraseña.
3. Fortalecer la gestión de cuentas y contraseñas en el plano de gestión para garantizar que la información no se divulgue o difunda.
4. Algunos proveedores de seguridad han proporcionado medidas preventivas para esta vulnerabilidad. Establecer reglas de bloqueo en los dispositivos de seguridad para evitar tales ataques.

10.2.2.2 Impacto

Versión involucrada

MRS 3.x

Módulos involucrados

- Plano de gestión: esta vulnerabilidad no está involucrada.
- Plano de tenant: Manager (Web+Controller+nodeagent), Kafka, Flink y Redis

NOTA

- Para MRS 3.1.0.*x*, realice las operaciones en las siguientes secciones:
  - **Remediación de Manager Web**
  - **Remediación de Manager Controller**
  - **Remediación de Manager NodeAgent**
- Para MRS 3.1.2.*x*, realice las operaciones en las siguientes secciones:
  - **Remediación de Manager Web**
  - **Remediación de Manager Controller**
  - **Remediación de Manager NodeAgent**
  - **Remediación de Kafka**
  - **Remediación de Flink**

10.2.2.3 Remediación de Manager Web

Prerrequisitos

Ha obtenido la URL y la cuenta de admin para iniciar sesión en FusionInsight Manager.

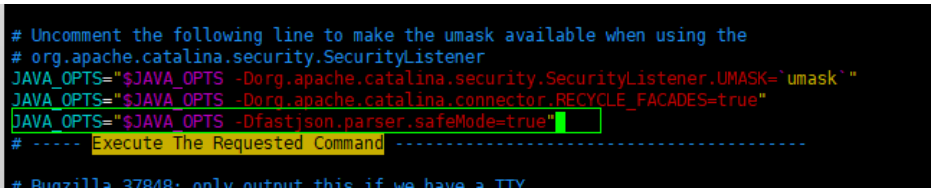
Procedimiento

Paso 1 Inicie sesión en el nodo OMS activo como usuario **omm** y haga una copia de respaldo del archivo **$OM_TOMCAT_HOME/bin/catalina.sh**.

cp $OM_TOMCAT_HOME/bin/catalina.sh /tmp

Paso 2 Ejecute el comando **vi $OM_TOMCAT_HOME/bin/catalina.sh**, busque la línea donde se encuentra **Execute The Requested Command** y agregue el siguiente contenido encima de la línea:

```
JAVA_OPTS="$JAVA_OPTS -Dfastjson.parser.safeMode=true"
```



Paso 3 Ejecute los siguientes comandos en el nodo OMS activo como usuario **omm** para reiniciar el servicio Web Manager:

$OMS_RUN_PATH/workspace/ha/module/harm/plugin/script/tomcat stop

$OMS_RUN_PATH/workspace/ha/module/harm/plugin/script/tomcat start

Paso 4 Ejecute el siguiente comando para comprobar el proceso en el nodo OMS activo:

ps -ef |grep tomcat | grep om-server

Si existe el parámetro **-Dfastjson.parser.safeMode=true**, la vulnerabilidad se ha mitigado.

Paso 5 Realice **1** y **2** en el nodo OMS en espera como usuario **omm**.

----Fin

10.2.2.4 Remediación de Manager Controller

Prerrequisitos

Ha obtenido la URL y la cuenta de admin para iniciar sesión en FusionInsight Manager.

Procedimiento

Paso 1 Inicie sesión en el nodo OMS activo como usuario **omm** y haga una copia de respaldo del archivo **$CONTROLLER_HOME/sbin/controller.sh**.

cp $CONTROLLER_HOME/sbin/controller.sh /tmp

Paso 2 Ejecute el comando **vi $CONTROLLER_HOME/sbin/controller.sh**, busque la línea donde se encuentra **JVM_ARGS=** y agregue el siguiente contenido debajo de la línea:

```
JVM_ARGS="$JVM_ARGS -Dfastjson.parser.safeMode=true"
```

Paso 3 Ejecute los siguientes comandos en el nodo OMS activo como **omm** de usuario para reiniciar el servicio Manager Controller:

sh /opt/Bigdata/om-server/om/sbin/restart-controller.sh

Paso 4 Ejecute el siguiente comando para comprobar el proceso en el nodo OMS activo:

ps -ef |grep ControllerService

Si existe el parámetro **-Dfastjson.parser.safeMode=true**, la vulnerabilidad se ha mitigado.

Paso 5 Repita **1** y **2** en el nodo OMS en espera como usuario **omm**.

----Fin

10.2.2.5 Remediación de Manager NodeAgent

Prerrequisitos

Ha obtenido la URL y la cuenta de admin para iniciar sesión en FusionInsight Manager.

Procedimiento

Paso 1 Inicie sesión en el nodo OMS activo como usuario **omm** y haga una copia de respaldo del archivo **$NODE_AGENT_HOME/bin/nodeagent_ctl.sh**.

cp $NODE_AGENT_HOME/bin/nodeagent_ctl.sh /tmp

Paso 2 Ejecute el comando **vi $NODE_AGENT_HOME/bin/nodeagent_ctl.sh**, busque la línea donde se encuentra **JVM_ARGS=** y agregue el siguiente contenido debajo de la línea:

```
JVM_ARGS="$JVM_ARGS -Dfastjson.parser.safeMode=true"
```

Paso 3 Realice **1** y **2** en todos los nodos del clúster.

Puede sobrescribir manualmente el archivo **$NODE_AGENT_HOME/bin/nodeagent_ctl.sh** modificado en todos los nodos como usuario **omm**.

Paso 4 Ejecute el siguiente comando en el nodo OMS activo como usuario **omm** para reiniciar todas las NodeAgents del clúster:

$CONTROLLER_HOME/inst/restartAllNoes.sh

Paso 5 Inicie sesión en el nodo del clúster para comprobar el proceso.

ps -ef |grep NodeAgent

Si existe el parámetro **-Dfastjson.parser.safeMode=true**, la vulnerabilidad se ha mitigado.

----Fin

10.2.2.6 Remediación de Kafka

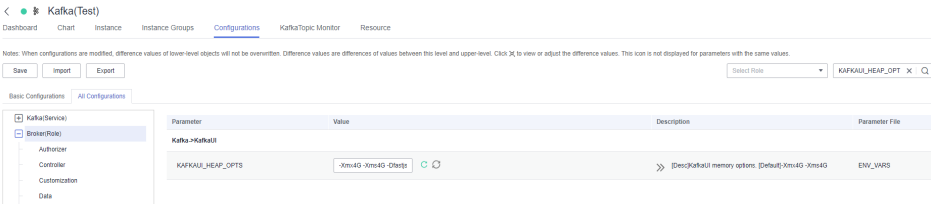
Prerrequisitos

Ha obtenido la URL y la cuenta de admin para iniciar sesión en FusionInsight Manager.

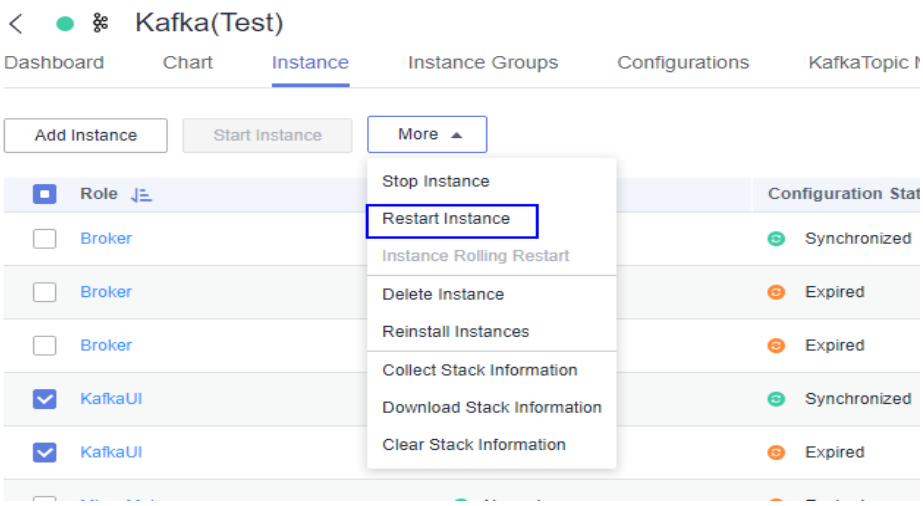
Procedimiento

Paso 1 Inicie sesión en FusionInsight Manager y elija **Cluster** > **Services** > **Kafka**. Haga clic en **Configurations** y luego en **All Configurations**. En esta página de subpestaña, busque el parámetro **KAFKAUI_HEAP_OPTS**. Agregue **-Dfastjson.parser.safeMode=true** a la columna **Value** de **KAFKAUI_HEAP_OPT** (deje un espacio entre el valor existente y **-Dfastjson.parser.safeMode=true**).

Por ejemplo, si el valor existente es **-Xmx4G -Xms4G**, el nuevo valor será **-Xmx4G -Xms4G -Dfastjson.parser.safeMode=true**.



Paso 2 Haga clic en **Save**. En la página de pestaña **Instance**, seleccione todas las instancias de KafkaUI y elija **More** > **Restart Instance**.



Paso 3 Inicie sesión en cualquier nodo de KafkaUI como usuario **omm** y compruebe el proceso:

ps -ef | grep KafkaUI

Si existe el parámetro **-Dfastjson.parser.safeMode=true**, la vulnerabilidad se ha mitigado.

----Fin

10.2.2.7 Remediación de Flink

Prerrequisitos

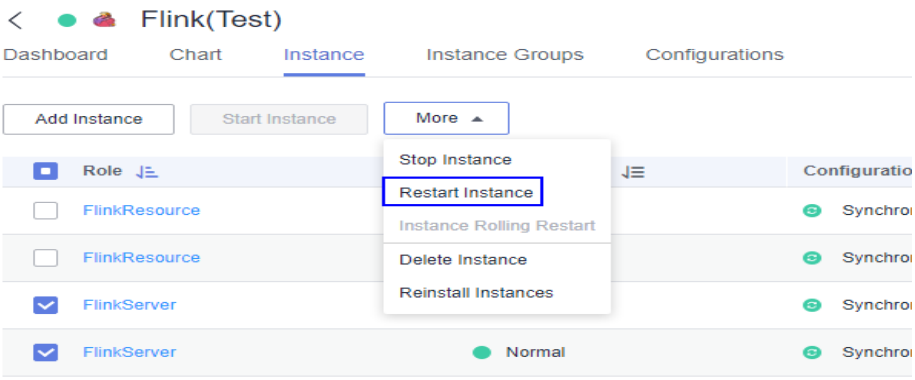
Ha obtenido la URL y la cuenta de admin para iniciar sesión en FusionInsight Manager.

Procedimiento

Paso 1 Inicie sesión en FusionInsight Manager y elija **Cluster** > **Services** > **Flink**. Haga clic en **Configurations** y luego en **All Configurations**. En esta página de subpestaña, busque el parámetro **FLINK_SERVER_GC_OPTS** y añada **-Dfastjson.parser.safeMode=true** a la columna **Value** de **FLINK_SERVER_GC_OPTS**. (Deje un espacio entre el valor existente y **-Dfastjson.parser.safeMode=true**.)

Por ejemplo, si el valor existente es *xxx*, el nuevo valor será *xxx* **-Dfastjson.parser.safeMode=true**.

Paso 2 Haga clic en **Save**. En la página de pestaña **Instance**, seleccione todas las instancias de FlinkServer y elija **More** > **Restart Instance**.



Paso 3 Inicie sesión en cualquier nodo de FlinkServer como usuario **omm** y compruebe el proceso:

ps -ef | grep FlinkServer

Si existe el parámetro **-Dfastjson.parser.safeMode=true**, la vulnerabilidad se ha mitigado.

----Fin

11 Interconectar Jupyter Notebook con MRS usando Python personalizado

11.1 Descripción

La configuración de Jupyter Notebook en MRS para usar Pyspark mejora la eficiencia del aprendizaje automático, la exploración de datos y el desarrollo de aplicaciones ETL.

Esta sección describe cómo configurar Jupyter Notebook en MRS para usar Pyspark. El procedimiento es el siguiente:

1. **Instalación de un cliente en un nodo fuera del clúster**
2. **Instalación de Python 3**
3. **Configuración del cliente MRS**
4. **Instalación de Jupyter Notebook**
5. **Verificación de que Jupyter Notebook puede acceder a MRS**

NOTA

Esta sección solo se aplica a MRS 3.*x* o posterior.

11.2 Instalación de un cliente en un nodo fuera del clúster

Paso 1 Prepare un ECS de Linux fuera del clúster. Para obtener más información sobre los requisitos, consulte **Instalación de un cliente en un nodo fuera de un clúster**.

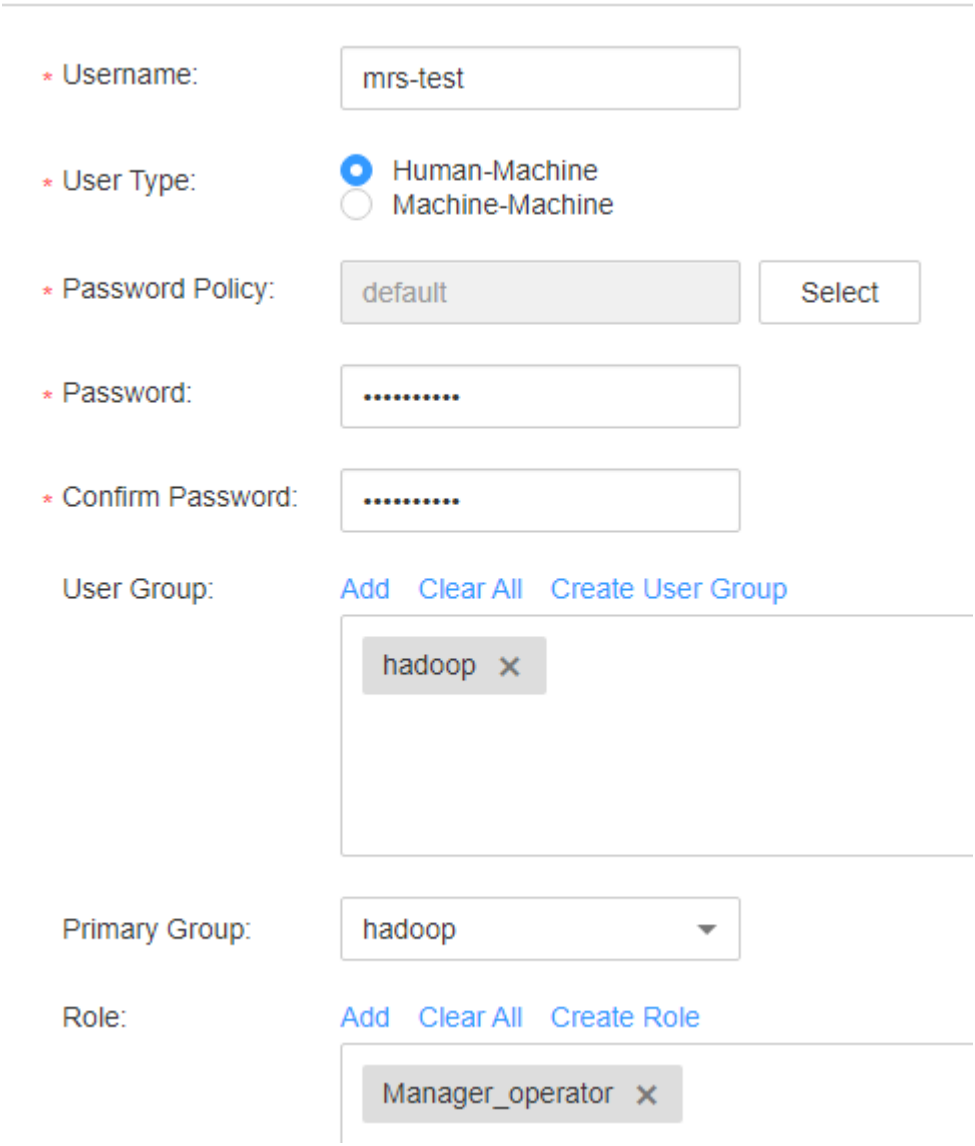
Paso 2 Instale el cliente en un directorio, por ejemplo, **/opt/client** en el nodo fuera del clúster haciendo referencia a **Instalación de un cliente en un nodo fuera de un clúster**.

Paso 3 Compruebe si la autenticación de Kerberos está habilitada para el clúster.

- En caso afirmativo, vaya a **Paso 4**.
- Si no, vaya a **Instalación de Python 3**.

Paso 4 Inicie sesión en FusionInsight Manager consultando a **Acceder a FusionInsight Manager (MRS 3.x o posterior)**.

Paso 5 Cree un usuario, por ejemplo, **mrs-test**. Establezca **User Group** en **hadoop**, **Primary Group** en **hadoop** y **Role** en **Manager_operator**.



Paso 6 Inicie sesión en el nodo cliente como usuario **root** y ejecute los siguientes comandos para configurar las variables de entorno para la autenticación de seguridad:

source /opt/client/bigdata_env

kinit *mrs-test*

NOTA

Cambie la contraseña en la primera autenticación.

----Fin

11.3 Instalación de Python 3

Paso 1 Inicie sesión en el nodo cliente fuera del clúster como usuario **root** y ejecute el siguiente comando para comprobar si Python 3 está instalado:

python3 --version

```
[root@ecs-notebook FusionInsight_Cluster_1_Services_ClientConfig]# python3 --version
-bash: python3: command not found
```

- En caso afirmativo, vaya a **Configuración del cliente MRS**.
- Si no, vaya a **Paso 2**.

Paso 2 Instale Python. Python 3.6.6 se utiliza como ejemplo.

1. Ejecute los siguientes comandos para instalar dependencias:

   yum install zlib zlib-devel zip -y

   yum install gcc-c++

   yum install openssl-devel

   yum install sqlite-devel -y

   Si la biblioteca pandas requiere las siguientes dependencias:

   yum install -y xz-devel

   yum install bzip2-devel

2. Ejecute el comando **wget https://www.python.org/ftp/python/3.6.6/Python-3.6.6.tgz** para descargar el código fuente de Python.
3. Ejecute el siguiente comando para descomprimir el paquete de código fuente de Python, por ejemplo, en el directorio **opt**:

   cd /opt

   tar –xvf Python-3.6.6.tgz

4. Cree un directorio de instalación de Python, por ejemplo, **/opt/python36**:

   mkdir /opt/python36

5. Compile Python.

   cd /opt/python-3.6.6

   ./configure --prefix=/opt/python36

   Se muestra la siguiente información si los comandos se ejecutan correctamente:

   ```
   configure: creating ./config.status
   config.status: creating Makefile.pre
   config.status: creating Modules/Setup.config
   config.status: creating Misc/python.pc
   config.status: creating Misc/python-config.sh
   config.status: creating Modules/ld_so_aix
   config.status: creating pyconfig.h
   creating Modules/Setup
   creating Modules/Setup.local
   creating Makefile


   If you want a release build with all stable optimizations active (PGO, etc),
   please run ./configure --enable-optimizations
   ```

   Ejecute el comando **make -j8**. Se muestra la siguiente información si el comando se ejecuta correctamente:


```
creating build/scripts-3.6
copying and adjusting /tmp/python366/Python-3.6.6/Tools/scripts/pydoc3 -> build/scripts-3.6
copying and adjusting /tmp/python366/Python-3.6.6/Tools/scripts/idle3 -> build/scripts-3.6
copying and adjusting /tmp/python366/Python-3.6.6/Tools/scripts/2to3 -> build/scripts-3.6
copying and adjusting /tmp/python366/Python-3.6.6/Tools/scripts/pyvenv -> build/scripts-3.6
changing mode of build/scripts-3.6/pydoc3 from 644 to 755
changing mode of build/scripts-3.6/idle3 from 644 to 755
changing mode of build/scripts-3.6/2to3 from 644 to 755
changing mode of build/scripts-3.6/pyvenv from 644 to 755
renaming build/scripts-3.6/pydoc3 to build/scripts-3.6/pydoc3.6
renaming build/scripts-3.6/idle3 to build/scripts-3.6/idle3.6
renaming build/scripts-3.6/2to3 to build/scripts-3.6/2to3-3.6
renaming build/scripts-3.6/pyvenv to build/scripts-3.6/pyvenv-3.6
```

Ejecute el comando **make install**. Se muestra la siguiente información si el comando se ejecuta correctamente:

```
rm -f /opt/python36/share/man/man1/python3.1
(cd /opt/python36/share/man/man1; ln -s python3.6.1 python3.1)
if test "xupgrade" != "xno"  ; then \
        case upgrade in \
                upgrade) ensurepip="--upgrade" ;; \
                install|*) ensurepip="" ;; \
        esac; \
         ./python -E -m ensurepip \
                $ensurepip --root=/ ; \
fi
Looking in links: /tmp/tmp6ldv525m
Collecting setuptools
Collecting pip
Installing collected packages: setuptools, pip
Successfully installed pip-10.0.1 setuptools-39.0.1
```

6. Ejecute los siguientes comandos para configurar el entorno de Python:

   export PYTHON_HOME=/opt/python36

   export PATH=$PYTHON_HOME/bin:$PATH

7. Ejecute el comando **python3 --version**. Python se ha instalado si se muestra la siguiente información:

```
[root@ecs-notebook Python-3.6.6]# python3 --version
Python 3.6.6
```

Paso 3 Verifique Python 3.

pip3 install helloword

python3

import helloworld

helloworld.say_hello("test")

```
[root@ecs-notebook Python-3.6.6]# pip3 install helloword
Collecting helloword
  Downloading https://files.pythonhosted.org/packages/1b/bf/f0f69f122158e0e98b5d95987a7ef5add3f8a340c6eb78d5871f855ca04e/helloword-0.0.1-py3-none-any.whl
Installing collected packages: helloword
Successfully installed helloword-0.0.1
You are using pip version 10.0.1, however version 21.3.1 is available.
You should consider upgrading via the 'pip install --upgrade pip' command.
[root@ecs-notebook Python-3.6.6]# python3
Python 3.6.6 (default, Dec 15 2021, 06:12:40)
[GCC 4.8.5 20150623 (Red Hat 4.8.5-44)] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> import helloworld
helloworld.say_hello("test")Hello, Sara!
>>>
'Hello, test!'
>>>
```

Paso 4 Instale bibliotecas de Python de terceros, como pandas y sklearn.

pip3 install pandas


```
[root@ecs-mrs-test Python-3.6.6]# pip3 install pandas
Collecting pandas
  Downloading https://files.pythonhosted.org/packages/c3/e2/00cacecafbab071c787019f00ad84ca3185952f6bb9bca9550ed83870d4d/pandas-1.1.5-cp36-cp36m-man
_x86_64.whl (9.5MB)
    100% |                                | 9.5MB 6.5MB/s
Collecting pytz>=2017.2 (from pandas)
  Downloading https://files.pythonhosted.org/packages/60/2e/dec1cc18c51b8df33c7c4d0a321b084cf38e1733b98f9d15018880fb4970/pytz-2022.1-py2.py3-none-an
503kB)
    100% |                                | 512kB 47.2MB/s
Collecting python-dateutil>=2.7.3 (from pandas)
  Downloading https://files.pythonhosted.org/packages/36/7a/87837f39d0296e723bb9b62bbb257d0355c7f6128853c78955f57342a56d/python_dateutil-2.8.2-py2.p
-any.whl (247kB)
    100% |                                | 256kB 54.5MB/s
Collecting numpy>=1.15.4 (from pandas)
  Downloading https://files.pythonhosted.org/packages/45/b2/6c7545bb7a38754d63048c7696804a0d947328125d81bf12beaa692c3ae3/numpy-1.19.5-cp36-cp36m-man
_x86_64.whl (13.4MB)
    100% |                                | 13.4MB 4.2MB/s
Collecting six>=1.5 (from python-dateutil>=2.7.3->pandas)
  Downloading https://files.pythonhosted.org/packages/d9/5a/e7c31adbe875f2abbb91bd84cf2dc52d792b5a01506781dbcf25c91daf11/six-1.16.0-py2.py3-none-any
Installing collected packages: pytz, six, python-dateutil, numpy, pandas
Successfully installed numpy-1.19.5 pandas-1.1.5 python-dateutil-2.8.2 pytz-2022.1 six-1.16.0
You are using pip version 10.0.1, however version 21.3.1 is available.
You should consider upgrading via the 'pip install --upgrade pip' command.
```

pip3 install backports.lzma

```
[root@ecs-mrs-test Python-3.6.6]# pip3 install backports.lzma
Collecting backports.lzma
  Using cached https://files.pythonhosted.org/packages/21/0f/1a9990233076d48aa2084100ba289ca162975e73a688f3a56c0ee2bb441a/backports.lzma-0.0.14.tar.gz
Installing collected packages: backports.lzma
  Running setup.py install for backports.lzma ... done
Successfully installed backports.lzma-0.0.14
You are using pip version 10.0.1, however version 21.3.1 is available.
You should consider upgrading via the 'pip install --upgrade pip' command.
```

pip3 install sklearn

```
[root@ecs-mrs-test Python-3.6.6]# pip3 install sklearn
Collecting sklearn
  Downloading https://files.pythonhosted.org/packages/1e/7a/dbb3be0ce9bd5c8b7e3d87328e79063f8b263b2b1bfa4774cb1147bfcd3f/sklearn-0.0.tar.
Collecting scikit-learn (from sklearn)
  Downloading https://files.pythonhosted.org/packages/f5/ef/bcd79e8d59250d6e8478eb1290dc6e05be42b3be8a86e3954146adbc171a/scikit_learn-0.2
ylinux1_x86_64.whl (20.0MB)
    100% |                                | 20.0MB 3.4MB/s
Collecting joblib>=0.11 (from scikit-learn->sklearn)
  Downloading https://files.pythonhosted.org/packages/3e/d5/0163eb0cfa0b673aa4fe1cd3ea9d8a81ea0f32e50807b0c295871e4aab2e/joblib-1.1.0-py2
(306kB)
    100% |                                | 307kB 46.5MB/s
Requirement already satisfied: scipy>=0.19.1 in /root/.local/lib/python3.6/site-packages (from scikit-learn->sklearn) (1.5.4)
Collecting threadpoolctl>=2.0.0 (from scikit-learn->sklearn)
  Downloading https://files.pythonhosted.org/packages/61/cf/6e354304bcb9c6413c4e02a747b600061c21d38ba51e7e544ac7bc66aecc/threadpoolctl-3.
nl
Requirement already satisfied: numpy>=1.13.3 in /opt/python36/lib/python3.6/site-packages (from scikit-learn->sklearn) (1.19.5)
Installing collected packages: joblib, threadpoolctl, scikit-learn, sklearn
  Running setup.py install for sklearn ... done
Successfully installed joblib-1.1.0 scikit-learn-0.24.2 sklearn-0.0 threadpoolctl-3.1.0
You are using pip version 10.0.1, however version 21.3.1 is available.
You should consider upgrading via the 'pip install --upgrade pip' command.
```

Paso 5 Ejecute el comando **python3 -m pip list** para comprobar el resultado de la instalación.

```
[root@ecs-mrs-test Python-3.6.6]# python3 -m pip list
Package         Version
--------------- -------
cycler          0.11.0
joblib          1.1.0
kiwisolver      1.3.1
numpy           1.19.5
pandas          1.1.5
pip             10.0.1
pyparsing       3.0.7
python-dateutil 2.8.2
pytz            2022.1
scikit-learn    0.24.2
scipy           1.5.4
setuptools      39.0.1
six             1.16.0
sklearn         0.0
threadpoolctl   3.1.0
```

Paso 6 Empaquételos en **Python.zip**.

cd /opt/python36/

zip -r python36.zip ./*

Paso 7 Cree un directorio HDFS y suba el paquete al directorio para su uso futuro.

hdfs dfs -mkdir /user/python

hdfs dfs -put python36.zip /user/python

----Fin

11.4 Configuración del cliente MRS

Vaya a **/opt/client/Spark2x/spark/conf** (directorio de instalación del cliente Spark) y configure los siguientes parámetros en el archivo **spark-defaults.conf**:

```
spark.pyspark.driver.python=/usr/bin/python3
spark.yarn.dist.archives=hdfs://hacluster/user/python/python36.zip#Python
```

11.5 Instalación de Jupyter Notebook

Paso 1 Inicie sesión en el nodo cliente como usuario **root** y ejecute el siguiente comando para instalar Jupyter Notebook:

pip3 install jupyter notebook

La instalación se realiza correctamente si se muestra el siguiente resultado del comando:

```
Successfully installed MarkupSafe-2.0.1 Send2Trash-1.8.0 argon2-cffi-21.3.0 argon2-cffi-bindings-21.2.0 async-generator-1.10 attrs-21.2.0 backcall-0.2.0 bleach-4.1.0 cffi-1.15.0 dataclasses-0.8 decorator-5.1.0 defusedxml-0.7.1 entrypoints-0.3 importlib-metadata-4.0.2 ipykernel-5.5.6 ipython-7.16.2 ipython-genutils-0.2.0 ipywidgets-7.6.5 jedi-0.17.2 jinja2-3.0.3 jsonschema-4.0.0 jupyter-1.0.0 jupyter-client-7.1.0 jupyter-console-6.4.0 jupyter-core-4.9.1 jupyterlab-pygments-0.1.2 jupyterlab-widgets-1.0.2 mistune-0.8.4 nbclient-0.5.9 nbconvert-6.0.7 nbformat-5.1.3 nest-asyncio-1.5.4 notebook-6.4.6 packaging-21.3 pandocfilters-1.5.0 parso-0.7.1 pexpect-4.8.0 pickleshare-0.7.5 prometheus-client-0.12.0 prompt-toolkit-3.0.24 ptyprocess-0.7.0 pycparser-2.21 pygments-2.10.0 pyparsing-3.0.6 pyrsistent-0.18.0 python-dateutil-2.8.2 pyzmq-22.3.0 qtconsole-5.2.2 qtpy-1.11.3 six-1.16.0 terminado-0.12.1 testpath-0.5.0 tornado-6.1 traitlets-4.3.3 typing-extensions-4.0.1 wcwidth-0.2.5 webencodings-0.5.1 widgetsnbextension-3.5.2 zipp-3.6.0
You are using pip version 10.0.1, however version 21.3.1 is available.
You should consider upgrading via the 'pip install --upgrade pip' command.
```

Paso 2 Para garantizar la seguridad, debe generar una contraseña de texto cifrado para iniciar sesión en Jupyter y colocarla en el archivo de configuración de Jupyter Notebook.

Ejecute el siguiente comando e introduzca la contraseña dos veces (salida en Out[3]):

ipython

```
[root@ecs-notebook python36]# ipython
Python 3.6.6 (default, Dec 20 2021, 09:32:25)
Type 'copyright', 'credits' or 'license' for more information
IPython 7.16.2 -- An enhanced Interactive Python. Type '?' for help.
In [1]: from notebook.auth import passwd
In [2]: passwd()
Enter password:
Verify password:
Out[2]: 'argon2:$argon2id$v=19$m=10240,t=10,p=8$g14BqLddl927n/unsyPlLQ
$YmoKJzbUfNG7LcxylJzm90bgbKWUIiHy6ZV+ObTzdcA
```

Paso 3 Ejecute el siguiente comando para generar el archivo de configuración de Jupyter:

jupyter notebook --generate-config

Paso 4 Modifique el archivo de configuración:

vi ~/.jupyter/jupyter_notebook_config.py

Agregue las siguientes configuraciones:

```
# -*- coding: utf-8 -*-
c.NotebookApp.ip='*' #Enter the internal IP address of the ECS.
c.NotebookApp.password = u'argon2:$argon2id
$v=19$m=10240,t=10,p=8$NmoAVwd8F6vFP2rX5ZbV7w$SyueJoC0a5TbCuHYzqfSx1vQcFvOTTryR
+0uk2MNNZA' # Enter the ciphertext generated at Out[2] in step 2.
c.NotebookApp.open_browser = False # Disable automatic browser opening.
c.NotebookApp.port = 9999 # Specified port number
c.NotebookApp.allow_remote_access = True
```

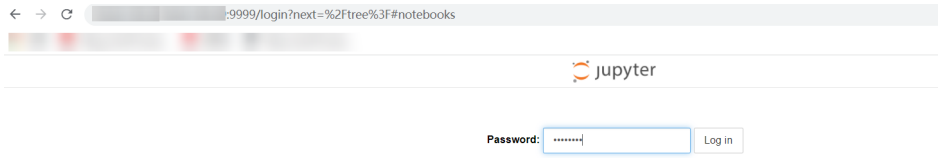
----Fin

11.6 Verificación de que Jupyter Notebook puede acceder a MRS

Paso 1 Ejecute el siguiente comando en el nodo cliente para iniciar Jupyter Notebook:

PYSPARK_PYTHON=./Python/bin/python3 PYSPARK_DRIVER_PYTHON=jupyter-notebook PYSPARK_DRIVER_PYTHON_OPTS="--allow-root" pyspark --master yarn --executor-memory 2G --driver-memory 1G

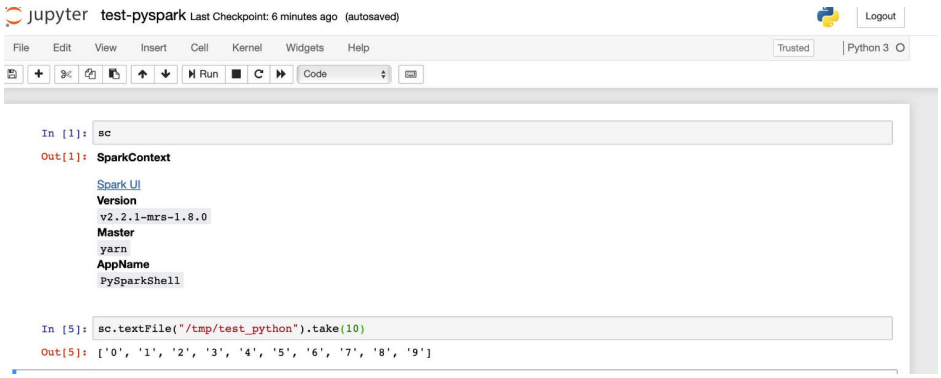
Paso 2 Usar *EIP*:**9999** para iniciar sesión en la interfaz de usuario web de Jupyter (asegúrese de que el grupo de seguridad ECS permita la dirección IP pública local y el puerto 9999). La contraseña de inicio de sesión es la contraseña configurada en **Paso 2**.



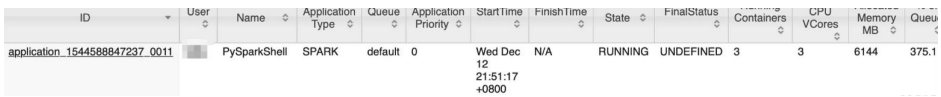
Paso 3 Crear código.

Cree una tarea de Python 3 y usa Spark para leer archivos.

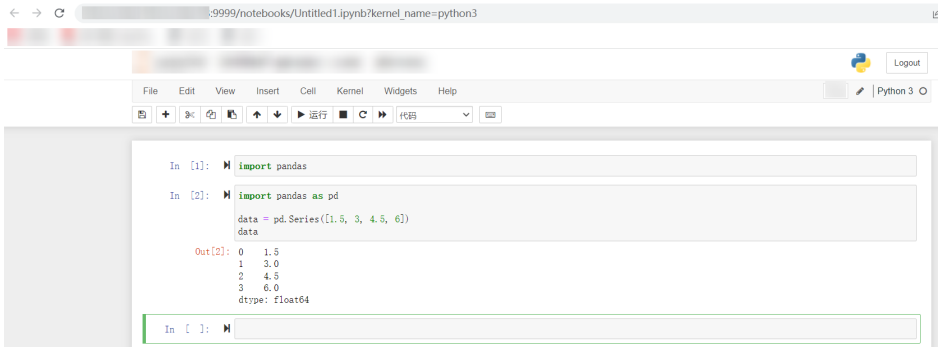
El resultado es el siguiente:



Inicie sesión en FusionInsight Manager y vea la solicitud de PySpark enviada en la interfaz de usuario web de YARN.



Paso 4 Verifique que se puede invocar a la biblioteca de pandas.

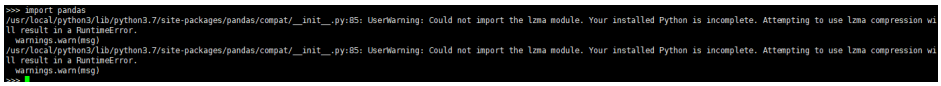


----Fin

11.7 Preguntas frecuentes

Pregunta

Cuando importo pandas desde una ruta local, se genera la siguiente alarma:



Procedimiento

Paso 1 Ejecute el comando **python -m pip install backports.lzma** para instalar el módulo LZMA.

```
[root@master ~]# python -m pip install backports.lzma
Looking in indexes: http://mirrors.aliyun.com/pypi/simple/
Requirement already satisfied: backports.lzma in /usr/local/python3/lib/python3.7/site-packages (0.0.14)
You are using pip version 10.0.1, however version 19.3.1 is available.
You should consider upgrading via the 'pip install --upgrade pip' command.
```

Paso 2 Vaya al directorio **/usr/local/python3/lib/python3.6** y edite el archivo **lzma.py**. El directorio varía dependiendo de los hosts. Puede ejecutar el comando **which** para consultar el directorio usado por Python.

Cambiar

```
from _lzma import *
from _lzma import _encode_filter_properties, _decode_filter_properties
```

En

```
try:
    from _lzma import *
    from _lzma import _encode_filter_properties, _decode_filter_properties
except ImportError:
    from backports.lzma import *
    from backports.lzma import _encode_filter_properties,
_decode_filter_properties
```

Antes de la modificación


```
"""Interface to the liblzma compression library.

This module provides a class for reading and writing compressed files,
classes for incremental (de)compression, and convenience functions for
one-shot (de)compression.

These classes and functions support both the XZ and legacy LZMA
container formats, as well as raw compressed data streams.
"""

__all__ = [
    "CHECK_NONE", "CHECK_CRC32", "CHECK_CRC64", "CHECK_SHA256",
    "CHECK_ID_MAX", "CHECK_UNKNOWN",
    "FILTER_LZMA1", "FILTER_LZMA2", "FILTER_DELTA", "FILTER_X86", "FILTER_IA64",
    "FILTER_ARM", "FILTER_ARMTHUMB", "FILTER_POWERPC", "FILTER_SPARC",
    "FORMAT_AUTO", "FORMAT_XZ", "FORMAT_ALONE", "FORMAT_RAW",
    "MF_HC3", "MF_HC4", "MF_BT2", "MF_BT3", "MF_BT4",
    "MODE_FAST", "MODE_NORMAL", "PRESET_DEFAULT", "PRESET_EXTREME",

    "LZMACompressor", "LZMADecompressor", "LZMAFile", "LZMAError",
    "open", "compress", "decompress", "is_check_supported",
]

import builtins
import io
import os
from _lzma import *
from _lzma import _encode_filter_properties, _decode_filter_properties
import _compression
```

Después de la modificación

```
These classes and functions support both the XZ and legacy LZMA
container formats, as well as raw compressed data streams.
"""

__all__ = [
    "CHECK_NONE", "CHECK_CRC32", "CHECK_CRC64", "CHECK_SHA256",
    "CHECK_ID_MAX", "CHECK_UNKNOWN",
    "FILTER_LZMA1", "FILTER_LZMA2", "FILTER_DELTA", "FILTER_X86", "FILTER_IA64",
    "FILTER_ARM", "FILTER_ARMTHUMB", "FILTER_POWERPC", "FILTER_SPARC",
    "FORMAT_AUTO", "FORMAT_XZ", "FORMAT_ALONE", "FORMAT_RAW",
    "MF_HC3", "MF_HC4", "MF_BT2", "MF_BT3", "MF_BT4",
    "MODE_FAST", "MODE_NORMAL", "PRESET_DEFAULT", "PRESET_EXTREME",

    "LZMACompressor", "LZMADecompressor", "LZMAFile", "LZMAError",
    "open", "compress", "decompress", "is_check_supported",
]

import builtins
import io
import os
#from _lzma import *
#from _lzma import _encode_filter_properties, _decode_filter_properties
try:
    from _lzma import *
    from _lzma import _encode_filter_properties, _decode_filter_properties
except ImportError:
    from backports.lzma import *
    from backports.lzma import _encode_filter_properties, _decode_filter_properties
import _compression
```

Paso 3 Guarde el archivo y salga. Luego, vuelve a importar pandas.

```
[root@master python3.7]# python
Python 3.7.0 (default, Oct 26 2019, 01:19:22)
[GCC 4.8.5 20150623 (Red Hat 4.8.5-36)] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> import pandas
>>>
```

----Fin

12 Apéndice

12.1 Especificaciones de ECS utilizadas por MRS

MRS utiliza ECS de los siguientes tipos en diferentes escenarios de aplicación.

- Cómputo-plus: C3, C3ne, C6, y C6s
- Memoria optimizada: M3, y M6
- E/S ultraaltas: I3 e IR3
- Cómputo-plus de Kunpeng: KC1

Reglas de nombramiento de las variantes de ECS

AB.C.D

Ejemplo: m2.8xlarge.8

En el variante anterior:

- **A** especifica el tipo de ECS. Por ejemplo, **s** indica un ECS de propósito general, **c** un ECS de cómputo, y **m** un ECS de memoria optimizada.
- **B** especifica el ID de tipo. Por ejemplo, el **1** de **s1** indica un ECS de primera generación de propósito general, y el **2** de **s2** indica un ECS de segunda generación de propósito general.
- **C** especifica un tamaño de variante y puede ser cualquiera de las siguientes opciones: medio, grande y xlarge.
- **D** especifica la relación de memoria a vCPUs expresada en un dígito. Por ejemplo, el valor **4** indica que la relación de memoria a vCPUs es 4.

Especificaciones

Tabla 12-1 Especificaciones de ECS de cómputo-plus (C) general

Tipo	vCPU	Memoria (GB)	Variante	Tipo de virtualización
C3	32	64	c3.8xlarge.2	KVM
C3	16	64	c3.4xlarge.4	KVM
C3	32	128	c3.8xlarge.4	KVM
C3	60	256	c3ne.15xlarge.4	KVM
C3ne	32	64	c3ne.8xlarge.2	KVM
C3ne	16	64	c3ne.4xlarge.4	KVM
C3ne	32	128	c3ne.8xlarge.4	KVM
C3ne	60	256	c3ne.15xlarge.4	KVM
C6	32	64	c6.8xlarge.2	KVM
C6	64	128	c6.16xlarge.2	KVM
C6	16	64	c6.4xlarge.4	KVM
C6	32	128	c6.8xlarge.4	KVM
C6	64	256	c6.16xlarge.4	KVM
C6s	32	64	c6s.8xlarge.2	KVM
C6s	64	128	c6s.16xlarge.2	KVM

Tabla 12-2 Especificaciones de ECS de memoria optimizada

Tipo	vCPU	Memoria (GB)	Variante	Tipo de virtualización
M3	8	64	m3.2xlarge.8	KVM
M3	16	128	m3.4xlarge.8	KVM
M3	32	256	m3.8xlarge.8	KVM
M3	60	512	m3.15xlarge.8	KVM
M6	8	64	m6.2xlarge.8	KVM
M6	16	128	m6.4xlarge.8	KVM

Tipo	vCPU	Memoria (GB)	Variante	Tipo de virtualización
M6	32	256	m6.8xlarge.8	KVM
M6	64	512	m6.16xlarge.8	KVM

Tabla 12-3 Especificaciones de ECS de E/S ultra altas

Tipo	vCPU	Memoria (GB)	Variante	Tipo de virtualización
I3	8	64	i3.2xlarge.8	KVM
I3	16	128	i3.4xlarge.8	KVM
I3	32	256	i3.8xlarge.8	KVM
I3	64	512	i3.16xlarge.8	KVM
IR3	16	64	ir3.4xlarge.4	KVM
IR3	32	128	ir3.8xlarge.4	KVM

12.2 Especificaciones de BMS utilizado por MRS

MRS utiliza el siguiente BMS en diferentes escenarios de aplicación.

Kunpeng V1 BMS

Especificaciones

Tabla 12-4 Especificaciones de Kunpeng V1 BMS

Variante/ID	vCPUs	Memoria (GB)	Red
physical.ks1ne.4xlarge	128	512	Distributed
physical.ks1ne.8xlarge	128	1024	

12.3 Solución de migración de datos

12.3.1 Hacer preparaciones

Esta sección describe cómo migrar datos de HDFS, HBase y Hive a un clúster MRS en diferentes escenarios. Durante la migración de datos, los datos pueden sobrescribirse, perderse o dañarse. Este documento es solo para referencia. Colabore con personal técnico de Huawei Cloud para formular e implementar una solución de migración de datos específica.

Realice preparativos en un clúster de origen antes de la migración de datos para evitar que el clúster de origen genere nuevos datos durante la migración de datos, evitando así la incoherencia de datos entre los clústeres de origen y destino después de la migración de datos. Antes de completar la migración de datos, el clúster de destino debe estar en el estado inicial y no puede ejecutar ningún otro servicio, excepto trabajos de migración de datos.

Detener los servicios de cluster y relacionados

- Si el servicio Kafka está involucrado en el clúster, detenga todos los trabajos que generan datos en Kafka. Espere hasta que las tareas de consumo de Kafka hayan consumido los datos de inventario en Kafka y, a continuación, realice el siguiente paso.
- Detenga todos los servicios y trabajos relacionados con HDFS, HBase y Hive, y detenga los servicios HBase y Hive.

Establecimiento de un canal de transmisión de datos

- Si el clúster de origen y el clúster de destino se despliegan en diferentes VPC en la misma región, cree una conexión de red entre las dos VPC para establecer un canal de transmisión de datos en la capa de red. Para obtener más información, consulte **Descripción de interconexión de VPC**.
- Si el clúster de origen y el clúster de destino se despliega en la misma VPC pero pertenecen a diferentes grupos de seguridad, agregue reglas de grupo de seguridad a cada grupo de seguridad en la consola de gestión de VPC. En las reglas de seguridad, **Protocol** está establecido en **ANY**, **Transfer Direction** está establecido en **Inbound** y **Source** está establecido en **Security Group** (el grupo de seguridad del clúster del mismo nivel).
  - Para agregar una regla entrante al grupo de seguridad del clúster de origen, seleccione el grupo de seguridad del clúster de destino de **Source**.
  - Para agregar una regla entrante al grupo de seguridad del clúster de destino, seleccione el grupo de seguridad del clúster de origen de **Source**.
- Si los clústeres de origen y destino se despliegan en el mismo grupo de seguridad de la misma VPC y la autenticación Kerberos está habilitada para ambos clústeres, configure la confianza mutua entre los dos clústeres.

12.3.2 Exportación de metadatos

Para garantizar que las propiedades de datos y los permisos del clúster de origen sean coherentes con los del clúster de destino, los metadatos del clúster de origen deben exportarse para restaurar los metadatos después de la migración de datos. Los metadatos que se van a exportar incluyen el propietario, el grupo y la información de permiso de los archivos HDFS y la descripción de la tabla Hive.

Exportación de metadatos HDFS

La información de metadatos de HDFS que se va a exportar incluye permisos de archivos y carpetas e información de propietario/grupo. Puede ejecutar el siguiente comando en el cliente HDFS para exportar los metadatos:

```
$HADOOP_HOME/bin/hdfs dfs -ls -R <migrating_path> > /tmp/hdfs_meta.txt
```

A continuación se proporciona una descripción de los parámetros del comando anterior.

- **$HADOOP_HOME**: directorio de instalación del cliente Hadoop en el clúster de origen
- **<migrating_path>**: directorio de datos de HDFS que se va a migrar
- **/tmp/hdfs_meta.txt**: ruta local para almacenar los metadatos exportados

NOTA

Si el clúster de origen puede comunicarse con el clúster de destino y ejecuta el comando **hadoop DistCp** como superadministrador para copiar datos, puede agregar el parámetro **-p** para habilitar DistCp para restaurar los metadatos del archivo correspondiente en el clúster de destino mientras copia datos. Si es así, omita este paso.

Exportación de metadatos de Hive

Los datos de la tabla Hive se almacenan en HDFS. Los datos de la tabla y los metadatos de los datos de la tabla son migrados centralmente en directorios por HDFS de una manera unificada. Los metadatos de las tablas Hive se pueden almacenar en diferentes tipos de bases de datos relacionales (como MySQL, PostgreSQL y Oracle) basadas en configuraciones de clúster. Los metadatos exportados de las tablas Hive en este documento son la descripción de la tabla Hive almacenada en la base de datos relacional.

Las ediciones principales de lanzamiento de big data en la industria soportan la instalación de Sqoop. Para los clústeres de big data locales de la versión de la comunidad, puede descargar el Sqoop de la versión de la comunidad para su instalación. Utilice Sqoop para desacoplar la fuerte dependencia entre los metadatos que se van a exportar y la base de datos relacional y exportar los metadatos de Hive a HDFS y migrarlos junto con los datos de la tabla para su restauración. El procedimiento es el siguiente:

Paso 1 Descargue la herramienta Sqoop desde el clúster de origen e instálela. Para obtener más información, véase **http://sqoop.apache.org/**.

Paso 2 Descargue el controlador JDBC de la base de datos relacional en el directorio **${Sqoop_Home}/lib**.

Paso 3 Ejecute el siguiente comando para exportar todas las tablas de metadatos de Hive: Todos los datos exportados se almacenan en **/user/<***user_name***>/<***table_name***>** directory en HDFS.

```
$Sqoop_Home/bin/sqoop import --connect jdbc:<driver_type>://<ip>:<port>/
<database> --table <table_name> --username <user> -password <passwd> -m 1
```

A continuación se proporciona una descripción de los parámetros del comando anterior.

- *$Sqoop_Home*: directorio de instalación de Sqoop
- *<driver_type>*: Tipo de base de datos
- **<ip>**: dirección IP de la base de datos en el clúster de origen
- **<port>**: número de puerto de la base de datos en el clúster de origen
- *<table_name>*: Nombre de la tabla que se va a exportar

- *<user>*: Nombre de usuario
- *<passwd>*: Contraseña de usuario

----Fin

12.3.3 Copia de datos

Según las regiones y la conectividad de red entre el clúster de origen y el clúster de destino, los escenarios de copia de datos se clasifican de la siguiente manera:

La misma región

Si el clúster de origen y el clúster de destino están en la misma región, siga las instrucciones en **Establecimiento de un canal de transmisión de datos** para configurar la red y configurar un canal de transmisión de red. Utilice la herramienta DistCp para ejecutar el siguiente comando para copiar los archivos de datos HDFS, HBase, Hive y los archivos de copia de respaldo de metadatos Hive del clúster de origen al clúster de destino.

```
$HADOOP_HOME/bin/hadoop distcp <src> <dist> -p
```

A continuación se proporciona una descripción de los parámetros del comando anterior.

- **$HADOOP_HOME**: directorio de instalación del cliente Hadoop en el clúster de destino
- **<src>**: directorio de HDFS del clúster de origen
- **<dist>**: directorio de HDFS del clúster de destino

Diferentes regiones

Si el clúster de origen y el clúster de destino están en diferentes regiones, utilice la herramienta DistCp para copiar los datos del clúster de origen en OBS y utilice la función de replicación entre regiones de OBS para copiar los datos en OBS en la región donde reside el clúster de destino. Para obtener más información, consulte **Replicación entre regiones**. Si se utiliza DistCp, la información de permiso, propietario y grupo no se puede establecer para los archivos en OBS. En este caso, debe exportar y copiar los metadatos de HDFS mientras exporta datos para evitar la pérdida de información de propiedades del archivo HDFS.

Migración de datos desde un clúster sin conexión a una nube

Puede utilizar las siguientes formas de migrar datos desde un clúster sin conexión a la nube.

- Direct Connect

  Cree un **Direct Connect** entre el clúster de origen y el clúster de destino, habilite la red entre el gateway de egress del clúster sin conexión y la VPC en línea y use DistCp para copiar los datos mediante referencia a **La misma región**.

12.3.4 Restauración de datos

Restauración de propiedades de archivos de HDFS

En función de la información de permiso exportada, ejecute los comandos HDFS en segundo plano del clúster de destino para restaurar el permiso de archivo y la información de propietario y grupo.


```
$HADOOP_HOME/bin/hdfs dfs -chmod <MODE> <path>
$HADOOP_HOME/bin/hdfs dfs -chown <OWNER> <path>
```

Restauración de metadatos de Hive

Instale Sqoop y ejecute el comando Sqoop en el clúster de destino para importar los metadatos de Hive exportados a DBService en el clúster MRS.

```
$Sqoop_Home/bin/sqoop export --connect jdbc:postgresql://<ip>:20051/hivemeta --
table <table_name> --username hive -password <passwd> --export-dir <export_from>
```

A continuación se proporciona una descripción de los parámetros del comando anterior.

- *$Sqoop_Home*: Directorio de instalación de Sqoop en el clúster de destino
- <*ip*>: Dirección IP de la base de datos en el clúster de destino
- <*table_name*>: Nombre de la tabla que se va a restaurar
- <*passwd*>: Contraseña del usuario **hive**
- <*export_from*>: Dirección HDFS de los metadatos en el clúster de destino

Reconstrucción de Tabla HBase

Reinicie el servicio HBase del clúster de destino para que la migración de datos surta efecto. Durante el reinicio, HBase carga los datos en el HDFS actual y regenera los metadatos. Una vez finalizado el reinicio, ejecute el siguiente comando en el cliente del nodo de Master para cargar los datos de la tabla HBase:

```
$HBase_Home/bin/hbase hbck -fixMeta -fixAssignments
```

Después de ejecutar el comando, ejecute el siguiente comando repetidamente para comprobar el estado de salud del clúster de HBase hasta que el estado de salud sea normal:

```
hbase hbck
```

12.4 Precauciones para MRS 3.x

Propósito

Custers de versiones anteriores a MRS 3.x utilizan MRS Manager para gestionar y monitorear clústeres de MRS. En la página Cluster Management de la consola de gestión de MRS, puede ver los detalles del clúster, gestionar nodos, componentes, alarmas, parches, archivos, trabajos, tenants y copias de respaldo y restauración. Además, puede configurar acciones de Bootstrap y gestionar etiquetas.

MRS 3.x utiliza FusionInsight Manager para gestionar y supervisar clústeres. En la página Cluster Management de la consola de gestión de MRS, puede ver los detalles del clúster, gestionar nodos, componentes, alarmas, archivos, trabajos, acciones de arranque y etiquetas.

Algunas operaciones de mantenimiento del clúster MRS 3.x son diferentes de las de versiones anteriores. Para más detalles, véase **Guía de operación de MRS Manager (Aplicable a versiones 2.x y anteriores)** y **Guía de operación del FusionInsight Manager (aplicable a 3.x)**.

Acceder a MRS Manager

- Para obtener más información acerca de cómo acceder al MRS Manager de versiones anteriores a MRS 3.x, consulte **Acceso a MRS Manager (MRS 2.x o anterior)**.

- Para obtener más información acerca de cómo acceder al FusionInsight Manager de MRS 3.x, consulte **Acceder a FusionInsight Manager (MRS 3.x o posterior)**.

Modificación de los parámetros de configuración del servicio de clúster de MRS

- Para versiones anteriores a MRS 3.x, puede modificar los parámetros de configuración del servicio en la página de gestión de clústeres de la consola de gestión de MRS.
  a. Inicie sesión en la consola de MRS. En el panel de navegación izquierdo, elija **Clusters** > **Active Clusters** y haga clic en un nombre de clúster.
  b. Elija **Components** > *Name of the desired service* > **Service Configuration**.

     La página de pestaña **Basic Configurations** se muestra de forma predeterminada. Para modificar más parámetros, haga clic en la pestaña **All Configurations**. El árbol de navegación muestra todos los parámetros de configuración del servicio. Los nodos de nivel 1 del árbol de navegación son nombres de servicio o nombres de rol. La categoría de parámetro se muestra después de expandir el nodo de nivel 1.
  c. En el árbol de navegación, seleccione la categoría de parámetros especificada y cambie los valores de los parámetros a la derecha.

     Si no está seguro de la ubicación de un parámetro, puede escribir el nombre del parámetro en el cuadro de búsqueda en la esquina superior derecha. El sistema busca el parámetro en tiempo real y muestra el resultado.
  d. Haga clic en **Save Configuration**. En el cuadro de diálogo que se muestra, haga clic en **OK**.
  e. Espere hasta que se muestre el mensaje "Operation succeeded". Haga clic en **Finish**. Se modifica la configuración.

     Compruebe si hay algún servicio cuya configuración ha caducado en el clúster. En caso afirmativo, reinicie la instancia de servicio o rol correspondiente para que la configuración surta efecto. También puede seleccionar **Restart the affected services or instances** al guardar la configuración.
- En MRS 3.x, debe iniciar sesión en FusionInsight Manager para modificar los parámetros de configuración del servicio.
  a. Inicie sesión en FusionInsight Manager.
  b. Elija **Cluster** > **Services**.
  c. Haga clic en el nombre del servicio especificado en la página de gestión de servicios.
  d. Haga clic en **Configurations**.

     La página de pestaña **Basic Configurations** se muestra de forma predeterminada. Para modificar más parámetros, haga clic en la pestaña **All Configurations**. El árbol de navegación muestra todos los parámetros de configuración del servicio. Los nodos de nivel 1 del árbol de navegación son nombres de servicio o nombres de rol. La categoría de parámetro se muestra después de expandir el nodo de nivel 1.
  e. En el árbol de navegación, seleccione la categoría de parámetros especificada y cambie los valores de los parámetros a la derecha.

     Si no está seguro de la ubicación de un parámetro, puede escribir el nombre del parámetro en el cuadro de búsqueda en la esquina superior derecha. El Manager busca el parámetro en tiempo real y muestra el resultado.
  f. Haga clic en **Save**. En el cuadro de diálogo de confirmación, haga clic en **OK**.
  g. Espere hasta que se muestre el mensaje "Operation succeeded". Haga clic en **Finish**. Se modifica la configuración.

Compruebe si hay algún servicio cuya configuración ha caducado en el clúster. En caso afirmativo, reinicie la instancia de servicio o rol correspondiente para que la configuración surta efecto.

