

Cloud Backup and Recovery

Guía del usuario

Edición 01
Fecha 2023-01-12



Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2024. Todos los derechos reservados.

Quedan terminantemente prohibidas la reproducción y/o la divulgación totales y/o parciales del presente documento de cualquier forma y/o por cualquier medio sin la previa autorización por escrito de Huawei Cloud Computing Technologies Co., Ltd.

Marcas registradas y permisos



El logotipo  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 Gestión de permisos.....	1
1.1 Creación de un usuario y concesión de permisos CBR.....	1
1.2 Creación de una política personalizada.....	2
2 Gestión de almacén.....	5
2.1 Consulta de un almacén.....	5
2.2 Eliminación de un almacén.....	8
2.3 Disociación de un recurso.....	9
2.4 Migración de un recurso.....	10
2.5 Ampliación de la capacidad del almacén.....	11
2.6 Reducción de la capacidad del almacén.....	13
2.7 Cambio del modo de facturación de pago por uso a anual/mensual.....	14
2.8 Cambio de las especificaciones de almacén.....	14
2.9 Replicación de un almacén.....	15
2.10 Gestión de etiquetas de almacén.....	18
2.11 Gestión del Proyecto empresarial de Vaults.....	19
3 Gestión de copias de respaldo.....	20
3.1 Consulta de una copia de respaldo.....	20
3.2 Compartir una copia de respaldo.....	22
3.3 Eliminación de una copia de respaldo.....	25
3.4 Uso de una copia de respaldo para crear una imagen.....	27
3.5 Uso de una copia de respaldo para crear un disco.....	28
3.6 Uso de una copia de respaldo para crear un sistema de archivos.....	29
3.7 Replicación de una copia de respaldo (en todas las regiones).....	30
4 Gestión de política.....	34
4.1 Creación de una política de copia de respaldo.....	34
4.2 Creación de una política de replicación.....	42
4.3 Modificación de una política.....	47
4.4 Eliminación de una política.....	49
4.5 Aplicación de una política a un almacén.....	49
4.6 Eliminación de una política de un almacén.....	50
5 Restauración de datos.....	52
5.1 Restauración de datos mediante una copia de respaldo de un servidor en la nube.....	52

5.2 Restauración de datos mediante una copia de respaldo en disco en la nube.....	54
5.3 Restauración de datos mediante una copia de respaldo en la nube híbrida.....	56
5.4 Restauración de datos mediante una copia de respaldo de archivos.....	57
6 Copias de respaldo consistentes con la aplicación.....	60
6.1 ¿Qué es la copia de respaldo consistente con las aplicaciones?.....	60
6.2 Cambio de un grupo de seguridad.....	64
6.3 Instalación del agente.....	66
6.4 Creación de una copia de respaldo consistente con las aplicaciones.....	73
6.5 Desinstalación del agente.....	74
7 Copia de respaldo de archivos.....	76
7.1 ¿Qué es la copia de respaldo de archivos?.....	76
7.2 Proceso de copia de respaldo de archivos.....	78
7.3 Creación de un almacén de copia de respaldo en la nube híbrida.....	80
7.4 Descarga e instalación del agente.....	82
7.5 Configuración de almacén.....	87
7.6 Adición de directorios.....	89
7.7 Creación de copias de respaldo de archivos.....	91
7.8 Restauración de datos mediante una copia de respaldo de archivos.....	92
7.9 Desinstalación del agente.....	94
7.10 Casos de resolución de problemas.....	95
8 (Opcional) Migración de recursos desde CSBS/VBS.....	99
9 Gestión de tareas.....	103
10 Monitoreo.....	104
10.1 Métricas de CBR.....	104
10.2 Creación de una regla de alarma.....	105
11 Auditoría.....	108
12 Cuotas.....	110
A Apéndice.....	112
A.1 Mantenimiento de la seguridad del agente.....	112
A.1.1 Cambiar la contraseña del usuario rdadmin.....	112
A.1.2 Cambio de la Contraseña de la Cuenta para Reportar Alarmas (SNMP v3).....	113
A.1.3 Sustitución del certificado de servidor.....	115
A.1.4 Sustitución de certificados de CA.....	117
A.2 Historial de cambios.....	119

1 Gestión de permisos

1.1 Creación de un usuario y concesión de permisos CBR

Esta sección describe cómo usar IAM para implementar un control de permisos detallado para sus recursos de CBR. Con IAM, usted puede:

- Crear usuarios de IAM para empleados en función de la estructura organizativa de su empresa. Cada usuario de IAM tendrá sus propias credenciales de seguridad para acceder a los recursos de CBR.
- Conceder sólo los permisos necesarios para que los usuarios realicen una tarea específica.
- Confiar una cuenta Huawei Cloud o un servicio en la nube para realizar operaciones eficientes en sus recursos de CBR.

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

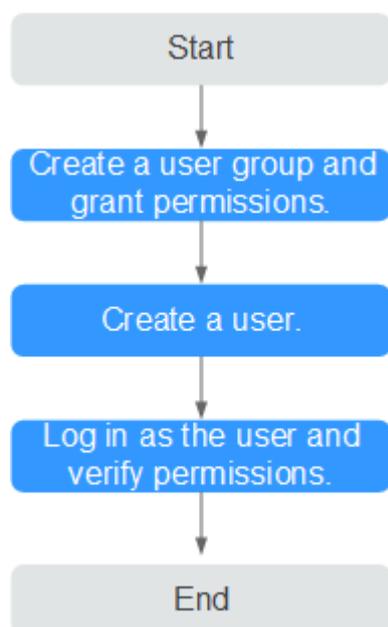
En esta sección se describe el procedimiento para conceder permisos (ver [Figura 1-1](#)).

Prerrequisitos

Obtenga información sobre los permisos (consulte [Permisos de CBR](#)) compatibles con CBR y elija políticas o roles de acuerdo con sus requisitos. Para ver las políticas del sistema de otros servicios, consulte [Permisos de sistema](#).

Flujo del proceso

Figura 1-1 Proceso de concesión de permisos CBR



1. **Crear un grupo de usuarios y asignar permisos**

Cree un grupo de usuarios en la consola de IAM y asigne la política **CBR ReadOnlyAccess** al grupo.

2. **Crear un usuario de IAM y agregarlo al grupo de usuario.**

Crear un usuario en la consola IAM y agregue el usuario al grupo creado en **1**.

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

Inicie sesión en la consola CBR con el usuario creado y compruebe que el usuario tiene permisos de solo lectura para CBR.

- Elija **Service List > Cloud Backup and Recovery**. A continuación, haga clic en **Buy Server Backup Vault** en la consola CBR. Si aparece un mensaje que indica que no tiene permisos suficientes para realizar la operación, la política **CBR ReadOnlyAccess** ya 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 **CBR ReadOnlyAccess** ya ha entrado en vigor.

1.2 Creación de una política personalizada

Se pueden crear políticas personalizadas para complementar las directivas definidas por el sistema de CBR. Para ver las acciones admitidas para las políticas personalizadas, consulte [Políticas de permisos y acciones admitidas](#).

Puede crear 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: Editar las políticas JSON desde cero o basándose en una política existente.

Esta sección proporciona ejemplos de políticas CBR comunes definidas por el usuario.

Ejemplo de políticas personalizadas

- Ejemplo 1: Permitir que los usuarios creen, modifiquen y eliminen bóvedas

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "cbr:*:get*",
        "cbr:*:list*",
        "cbr:vaults:update",
        "cbr:vaults:delete",
        "cbr:vaults:create"
      ]
    }
  ]
}
```

- Ejemplo 2: Negar a los usuarios que eliminen bóvedas y copias de seguridad

Una política con solo permisos "Deny" debe usarse junto con otras políticas para que surtan efecto. Si los permisos asignados a un usuario contienen tanto "Allow" y "Deny", los permisos "Deny" tienen prioridad sobre los permisos "Allow".

Se puede utilizar el siguiente método si necesita asignar permisos de la política **CBR FullAccess** a un usuario, pero desea evitar que el usuario elimine bóvedas y copias de seguridad. Crear una política personalizada para denegar la eliminación del almacén y de las copias de seguridad y adjunte ambas políticas al grupo al que pertenece el usuario. A continuación, el usuario puede realizar todas las operaciones en CBR, excepto la eliminación de bóvedas o copias de seguridad. A continuación se muestra un ejemplo de una política de denegación:

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "cbr:backups:delete",
        "cbr:vaults:delete"
      ]
    }
  ]
}
```

- Ejemplo 3: Definición de permisos para varios servicios en una política

Una política personalizada puede contener las acciones de varios servicios que son de tipo global o de nivel de proyecto. A continuación se muestra una política de ejemplo que contiene acciones de varios servicios:

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "cbr:vaults:create",
        "cbr:vaults:update",
        "cbr:vaults:delete"
      ]
    }
  ],
}
```

```
        "Effect": "Allow",  
        "Action": [  
            "sfs:shares:createShare"  
        ]  
    }  
]
```

2 Gestión de almacén

2.1 Consulta de un almacén

Puede establecer criterios de búsqueda para consultar los almacenes deseadas en la lista de almacenes.

Prerrequisitos

Se ha creado un almacén.

Consulta de detalles de almacén

Paso 1 Inicie sesión en la consola de CBR.

1. [Inicie sesión en la consola de gestión.](#)
2. Haga clic en  en la esquina superior izquierda y seleccione su región y proyecto.
3. Elija **Storage > Cloud Backup and Recovery**. Elija el tipo de copia de respaldo deseado en el panel de navegación izquierdo.

Paso 2 Vea la información básica sobre los almacenes. Los parámetros relacionados se describen en la siguiente tabla.

Tabla 2-1 Parámetros de información básica

Parámetro	Descripción
Name/ID	Nombre e ID del almacén. Haga clic en el nombre del almacén para ver detalles sobre el almacén.
Type	Tipo de almacén, que puede ser almacén de copia de respaldo y almacén de replicación <ul style="list-style-type: none">● Un almacén de copias de respaldo almacena copias de respaldo de servidores, sistemas de archivos y discos.● Un almacén de replicación almacena réplicas de copia de respaldo.

Parámetro	Descripción
Status	Estado de almacén. Tabla 2-2 describe los estados del almacén.
Specifications	Especificaciones de almacén, que pueden ser copias de respaldo del servidor y copias de respaldo consistentes con las aplicaciones <ul style="list-style-type: none"> ● Un almacén de copias de respaldo de servidor almacena copias de respaldo de servidores comunes. ● Un almacén de copias de respaldo consistentes con las aplicaciones almacena copias de respaldo de servidores de bases de datos.
Used/Total Vault Capacity (GB)	Capacidad utilizada por las copias de respaldo en el almacén. Muestra el espacio utilizado por las copias de respaldo y la capacidad de la almacén. Por ejemplo: si se muestra 20/100 , se han utilizado 20 GB de la capacidad del almacén de 100 GB.
Associated Servers/ File Systems/Disks	Número de servidores, sistemas de archivos, y discos asociados al almacén. Puede hacer clic en el número para ver los detalles de los recursos asociados. La capacidad asociada que se muestra en la página de detalles es la capacidad total de todos los recursos que se han asociado a este almacén.
Billing Mode	Modo de facturación de la almacén, que puede ser anual/mensual y de pago por uso . <ul style="list-style-type: none"> ● Anual/mensual es un modo de facturación prepagada. Se le factura en función de la duración de la suscripción que especifique. Este modo proporciona precios más bajos y es ideal cuando la duración del uso de recursos es predecible. ● El pago por uso es un modo de facturación pospago. Se le factura en función de su uso de recursos. Con este modo, puede aumentar o eliminar recursos en cualquier momento. Los cargos se deducen del saldo de su cuenta.

Paso 3 En cualquier página de copia de respaldo, haga clic en la pestaña **Vaults** y establezca criterios de filtro para ver los almacenes.

- Seleccione un valor de la lista desplegable de estado para consultar los almacenes por estado. [Tabla 2-2](#) describe los estados del almacén.

Tabla 2-2 Estado del almacén

Estado	Atributo de estado	Descripción
All statuses	--	Todos los almacenes se muestran si se selecciona este valor.

Estado	Atributo de estado	Descripción
Available	Un estado estable	Un estado estable después de completar una tarea de almacén. Este estado permite la mayoría de las operaciones.
Locked	Un estado intermedio	Un estado intermedio cuando está en curso una expansión de capacidad, un cambio de modo de facturación o un cambio de especificaciones. En este estado, no puede ampliar la capacidad del almacén, cambiar el modo de facturación o cambiar las especificaciones del almacén. Sin embargo, puede realizar otras operaciones, como aplicar una política y asociar servidores, sistemas de archivos, o discos. Una vez completada la ampliación de capacidad, el cambio de modo de facturación o el cambio de especificaciones, el estado del almacén se convierte en Available .
Deleting	Un estado intermedio	Estado intermedio cuando se elimina un almacén. En este estado, se muestra una barra de progreso que indica el progreso de la eliminación. Si la barra de progreso permanece sin cambios durante un tiempo prolongado, se ha producido una excepción. Póngase en contacto con atención de cliente.
Frozen	Un estado estable	Si sus recursos ingresan un período de eliminación pendiente en el caso de que su suscripción haya caducado o su cuenta esté en mora, o si los recursos no cumplen con los requisitos de respaldo, su almacén se pone en el estado Frozen . Si los recursos se congelan debido a atrasos, el estado estará Available después de que su cuenta se recargue. Los recursos se pueden utilizar normalmente. Si no recarga su cuenta a tiempo, el sistema eliminará automáticamente los recursos bloqueados después de que expire el período de retención. Si los recursos están congelados por razones de respaldo, póngase en contacto con atención de cliente.
Error	Un estado estable	Un almacén ingresa el estado Error cuando se produce una excepción durante la ejecución de una tarea. Puede hacer clic en Tasks en el panel de navegación de la izquierda para ver la causa del error. Si el error persiste, póngase en contacto con el atención de cliente.

- Busque en la almacén por su nombre o ID.
- Haga clic en **Search by Tag** en la esquina superior derecha para buscar almacenes por etiqueta.

- En la página de la pestaña **Search by Tag** que se muestra, introduzca una clave y un valor de etiqueta existentes y haga clic en . Los criterios de búsqueda de etiquetas añadidos se muestran bajo los cuadros de texto. Haga clic en **Search** en la esquina inferior derecha.
- Puede utilizar más de una etiqueta para una búsqueda combinada. Haga clic  cada vez que se introduzca una clave y un valor. Los criterios de búsqueda de etiquetas añadidos se muestran bajo los cuadros de texto. Cuando se añade más de una etiqueta, las etiquetas se aplicarán juntas para una búsqueda combinada. Se puede añadir un máximo de 10 etiquetas a la vez.
- Puede hacer clic en **Reset** en la esquina inferior derecha para restablecer los criterios de búsqueda.

Paso 4 Haga clic en el nombre del almacén para ver detalles sobre el almacén.

NOTA

Para los valores de capacidad utilizada y espacio de copia de respaldo, sólo se mantiene la parte entera y se redondea la parte decimal. Por ejemplo, el espacio de copia de respaldo utilizado se muestra como 0 GB, pero el espacio de copia de respaldo que se ha utilizado puede ser de 0.2 GB.

---Fin

2.2 Eliminación de un almacén

Puede eliminar los almacenes no deseadas para reducir el uso y los costos del espacio de almacenamiento.

Todas las copias de respaldo almacenadas en el almacén se eliminarán una vez que elimine un almacén.

Solo se pueden eliminar los almacenes de pago por uso. Las bóvedas anuales/mensuales deben darse de baja siguiendo las instrucciones en [¿Cómo cancelo la suscripción a un almacén?](#)

Prerrequisitos

- Existe al menos un almacén.
- El almacén se encuentra en el estado **Available** o **Error**.
- Una almacén de copia de respaldo en la nube híbrida solo se puede eliminar después de borrar las copias de seguridad correspondientes tanto en las instalaciones como en la nube.

Procedimiento

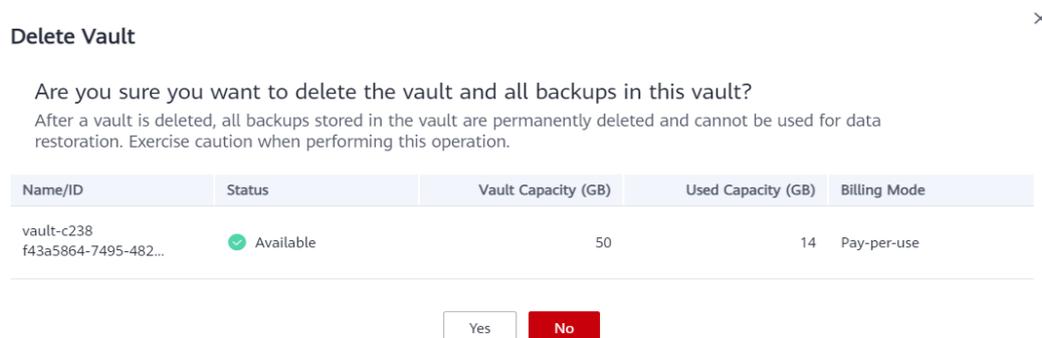
Paso 1 Inicie sesión en la consola de CBR.

1. [Inicie sesión en la consola de gestión.](#)
2. Haga clic en  en la esquina superior izquierda y seleccione su región y proyecto.
3. Elija **Storage > Cloud Backup and Recovery**. Elija el tipo de copia de respaldo deseado en el panel de navegación izquierdo.

Paso 2 En cualquier página de copia de respaldo, busque el almacén que desea eliminar y elija **More > Delete** en la columna **Operation**. Consulte [Figura 2-1](#). Todas las copias de respaldo

almacenadas en el almacén se eliminarán una vez que elimine un almacén. Tenga cuidado al realizar esta operación.

Figura 2-1 Eliminación de una almacén



Paso 3 Haga clic en **Yes**.

----Fin

2.3 Disociación de un recurso

Si ya no necesita realizar una copia de respaldo de un recurso asociado, disocielo del almacén.

Después de disociar un recurso, la política de copia de respaldo o replicación del almacén ya no tiene ningún efecto en el recurso. Además, se eliminarán todas las copias de seguridad manuales y automáticas de este recurso. Las copias de seguridad eliminadas no se pueden utilizar para la restauración de datos. Tenga cuidado al realizar esta operación.

La disociación de un recurso de un almacén no afecta al rendimiento de los servicios del recurso.

Procedimiento

Paso 1 Inicie sesión en la consola de CBR.

1. **Inicie sesión en la consola de gestión.**
2. Haga clic en  en la esquina superior izquierda y seleccione su región y proyecto.
3. Elija **Storage > Cloud Backup and Recovery**. Elija el tipo de copia de respaldo deseado en el panel de navegación izquierdo.

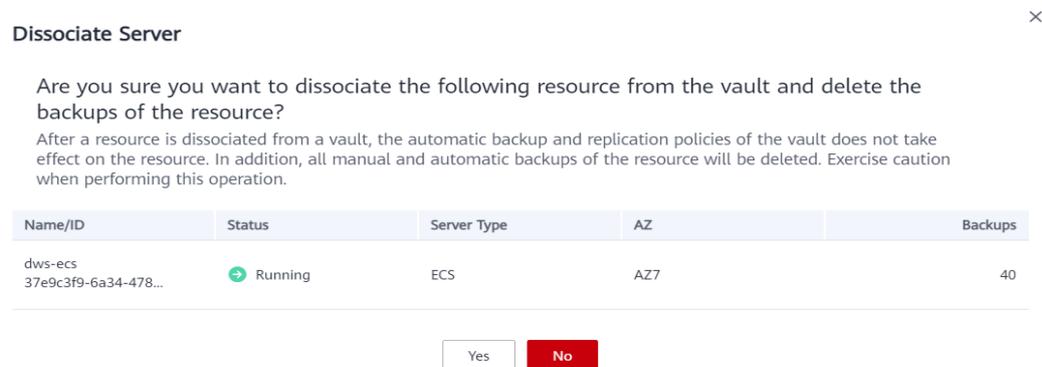
Paso 2 En cualquier página de copia de respaldo, busque el almacén de destino y haga clic en el nombre del almacén.

Paso 3 En este ejemplo, utilizaremos la página **Cloud Server Backups** para ilustrar el proceso. Haga clic en la pestaña **Associated Servers**. Busque el servidor de destino y haga clic en **Dissociate** en la columna **Operation**. Consulte **Figura 2-2**.

Después de disociar un recurso, la política de copia de respaldo o replicación del almacén ya no tiene ningún efecto en el recurso. Además, se eliminarán todas las copias de seguridad

manuales y automáticas de este recurso. Las copias de seguridad eliminadas no se pueden utilizar para la restauración de datos. Tenga cuidado al realizar esta operación.

Figura 2-2 Disociación de un servidor



Paso 4 Confirme la información y haga clic en **Yes**.

----Fin

2.4 Migración de un recurso

La migración de un recurso significa que se disocia un recurso de un almacén y, a continuación, se asocia a otro almacén. Todas las copias de respaldo del recurso se migrarán al almacén de destino.

Restricciones

- Los recursos sólo se pueden migrar cuando los almacenes de origen y destino están en el estado **Available** o **Locked**.
- Los almacenes de origen y destino para la migración de recursos deben tener las mismas especificaciones.
- La capacidad restante del almacén de destino debe ser mayor que el tamaño de las copias de respaldo de recursos que se van a migrar.
- Actualmente no se admite la migración de recursos entre cuentas.

Procedimiento

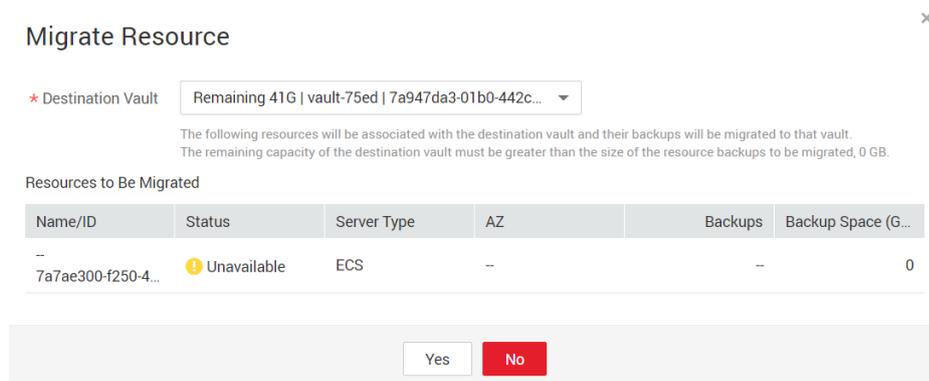
Paso 1 Inicie sesión en la consola de CBR.

1. **Inicie sesión en la consola de gestión.**
2. Haga clic en  en la esquina superior izquierda y seleccione su región y proyecto.
3. Elija **Storage > Cloud Backup and Recovery**. Elija el tipo de copia de respaldo deseado en el panel de navegación izquierdo.

Paso 2 En cualquier página de copia de respaldo, busque el almacén de destino y haga clic en el nombre del almacén. En este ejemplo, utilizaremos la página **Cloud Server Backups** para ilustrar el proceso.

Paso 3 Haga clic en la pestaña **Associated Servers**. Busque el servidor de destino y haga clic en **Migrate** en la columna **Operation**. Consulte [Figura 2-3](#).

Figura 2-3 Migración de un recurso



Paso 4 Seleccione el almacén de destino y haga clic en **Yes**.

Paso 5 Vea el progreso de la migración en la página **Tasks**. Si **Status** cambia a **Successful**, el recurso se ha migrado.

Paso 6 Vaya al almacén de destino para confirmar que el recurso se ha asociado al almacén y que todas sus copias de seguridad se han migrado a ese almacén.

----**Fin**

2.5 Ampliación de la capacidad del almacén

Puede ampliar el tamaño de un almacén si su capacidad total es insuficiente.

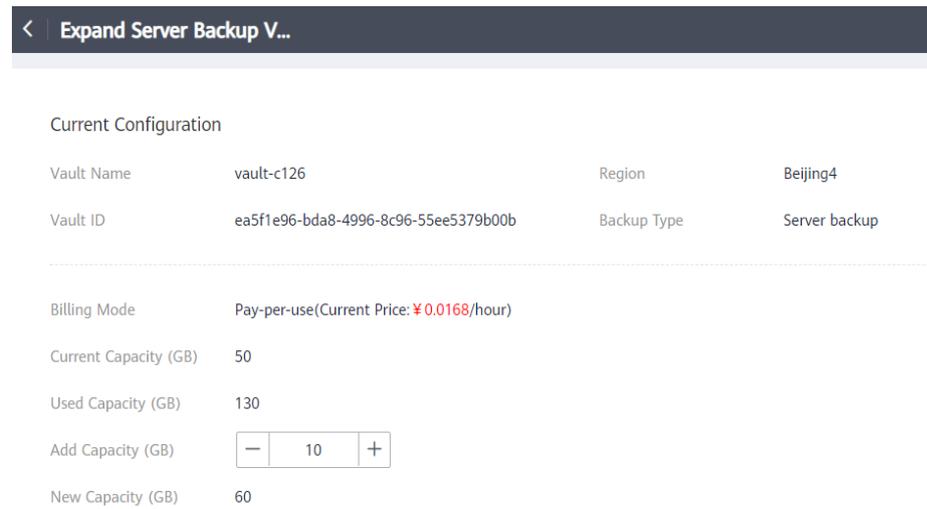
Procedimiento

Paso 1 Inicie sesión en la consola de CBR.

1. [Inicie sesión en la consola de gestión](#).
2. Haga clic en  en la esquina superior izquierda y seleccione su región y proyecto.
3. Elija **Storage > Cloud Backup and Recovery**. Elija el tipo de copia de respaldo deseado en el panel de navegación izquierdo.

Paso 2 En cualquier página de copia de respaldo, busque el almacén de destino y elija **More > Expand Capacity** en la columna **Operation**. Consulte [Figura 2-4](#).

Figura 2-4 Ampliación de la capacidad del almacén



Paso 3 Introduzca la capacidad que desea agregar. El valor mínimo es **1**.

Paso 4 Haga clic en **Next**. Confirme la configuración y haga clic en **Submit**.

Paso 5 Vuelva a la lista del almacén y compruebe que se ha ampliado la capacidad del almacén.

----Fin

Expansión automática de la capacidad

Si desea que un almacén se expanda automáticamente cuando se agote su capacidad, active la ampliación automática de capacidad.

Si esta función está habilitada, el tamaño del almacén se ampliará automáticamente a 1.25 veces la capacidad de la bóveda original cuando se haya alcanzado el límite de tamaño máximo.

Los almacenes anuales/mensuales no admiten la expansión automática de la capacidad.

Paso 1 Inicie sesión en la consola de CBR.

1. **Inicie sesión en la consola de gestión.**
2. Haga clic en  en la esquina superior izquierda y seleccione su región y proyecto.
3. Elija **Storage > Cloud Backup and Recovery**. Elija el tipo de copia de respaldo deseado en el panel de navegación izquierdo.

Paso 2 En cualquier página de copia de respaldo, haga clic en el nombre del almacén que desea expandir.

Paso 3 En la página de detalles del almacén, habilite **Auto Capacity Expansion**.

Paso 4 (Opcional) Deshabilite **Auto Capacity Expansion** si ya no lo necesita.

----Fin

2.6 Reducción de la capacidad del almacén

Puede reducir el tamaño de un almacén si su capacidad total es demasiado para usted.

Solo los almacenes de pago por uso pueden tener su capacidad reducida actualmente.

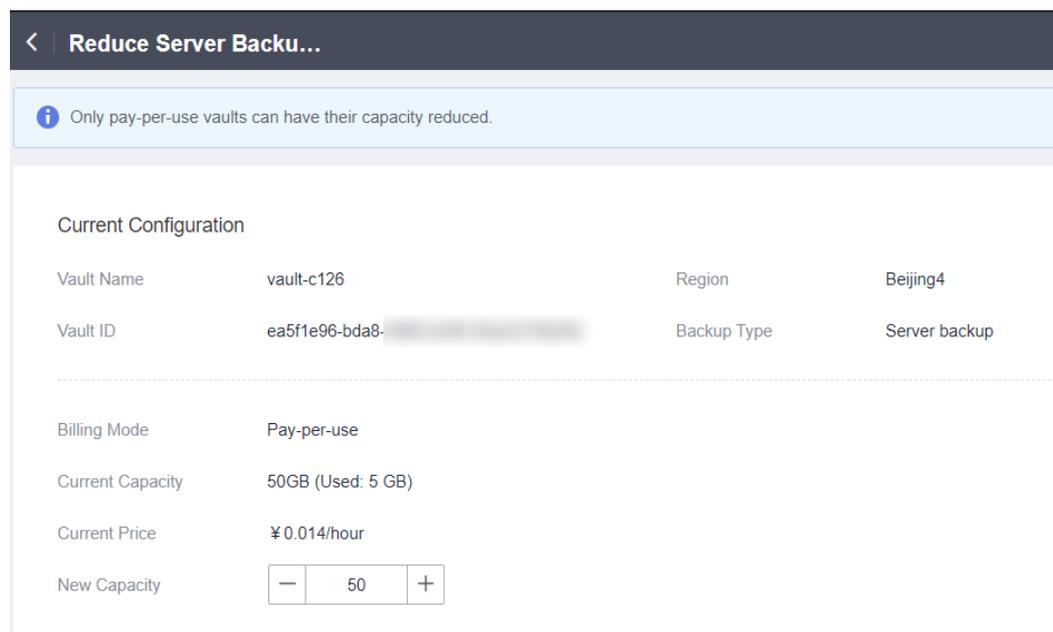
Procedimiento

Paso 1 Inicie sesión en la consola de CBR.

1. **Inicie sesión en la consola de gestión.**
2. Haga clic en  en la esquina superior izquierda y seleccione su región y proyecto.
3. Elija **Storage > Cloud Backup and Recovery**. Elija el tipo de copia de respaldo deseado en el panel de navegación izquierdo.

Paso 2 En cualquier página de copia de respaldo, busque el almacén de destino y elija **More > Reduce Capacity** en la columna **Operation**. Consulte [Figura 2-5](#).

Figura 2-5 Reducción de la capacidad del almacén



Paso 3 Introduzca la nueva capacidad después de la reducción. Asegurarse de que la nueva capacidad sea superior al 125% de la capacidad utilizada. O, la reducción de capacidad fallará.

Paso 4 Haga clic en **Next**. Confirme la configuración y haga clic en **Submit**.

Paso 5 Vuelva a la lista del almacén y compruebe que se ha reducido la capacidad de la bóveda.

----Fin

2.7 Cambio del modo de facturación de pago por uso a anual/mensual

- Anual/mensual es un modo de facturación prepagada. Se le factura en función de la duración de la suscripción que especifique. Este modo proporciona precios más bajos y es ideal cuando la duración del uso de recursos es predecible.
- El pago por uso es un modo de facturación pospago. Se le factura en función de su uso de recursos. Con este modo, puede aumentar o eliminar recursos en cualquier momento. Los cargos se deducen del saldo de su cuenta.

Si desea utilizar una bóveda durante mucho tiempo, puede cambiar su modo de facturación de pago por uso a anual/mensual para reducir costos. Para obtener más información sobre las operaciones, consulte esta sección.

Prerrequisitos

Un almacén está en el modo de facturación de pago por uso.

Procedimiento

Paso 1 Inicie sesión en la consola de CBR.

1. [Inicie sesión en la consola de gestión.](#)
2. Haga clic en  en la esquina superior izquierda y seleccione su región y proyecto.
3. Elija **Storage > Cloud Backup and Recovery**. Elija el tipo de copia de respaldo deseado en el panel de navegación izquierdo.

Paso 2 En cualquier página de copia de respaldo, busque el almacén de destino y elija **More > Change Billing Mode** en la columna **Operation**.

Paso 3 Seleccione la duración requerida para el almacén, confirme la información y haga clic en **Pay**.

Paso 4 Volver a la lista de almacén. Puede ver que **Billing Mode** del almacén ha cambiado a **Yearly/Monthly**.

----Fin

2.8 Cambio de las especificaciones de almacén

Los almacenes de copia de respaldo del servidor y los almacenes de replicación del servidor tienen dos especificaciones: las de las copias de seguridad/réplicas del servidor y las de las copias de seguridad/réplicas consistentes con la aplicación.

- Las copias de respaldo de servidores son de servidores comunes.
- Las copias de respaldo consistentes con las aplicaciones son copias de respaldo de servidores con bases de datos.

Si necesita realizar una copia de respaldo de un servidor que contiene una base de datos, cambie las especificaciones del almacén asociado de la copia de respaldo del servidor a la copia de respaldo consistente con las aplicaciones. Esta sección describe las operaciones detalladas.

Puede cambiar las especificaciones de un almacén de copias de seguridad del servidor a copias de seguridad compatibles con las aplicaciones, pero no al revés.

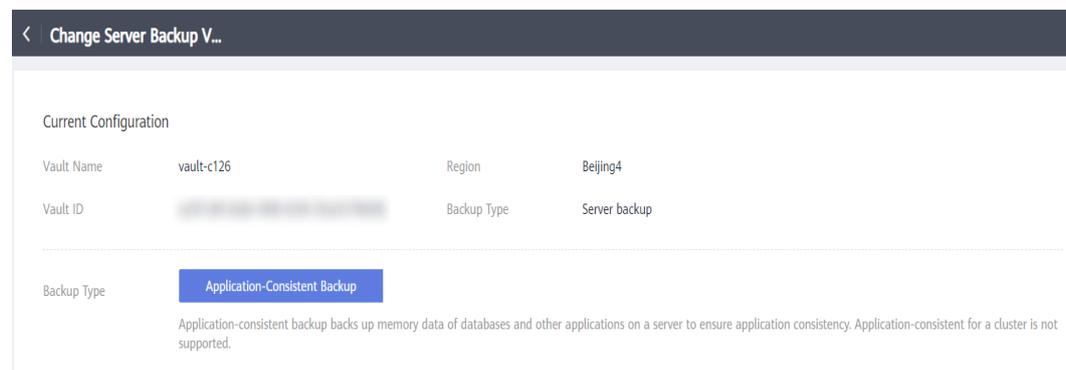
Procedimiento

Paso 1 Inicie sesión en la consola de CBR.

1. **Inicie sesión en la consola de gestión.**
2. Haga clic en  en la esquina superior izquierda y seleccione su región y proyecto.
3. Elija **Storage > Cloud Backup and Recovery**. Elija el tipo de copia de respaldo deseado en el panel de navegación izquierdo.

Paso 2 En la página **Cloud Server Backups**, localice el almacén de destino. Seleccione **More > Change Specifications** en la columna **Operation** del almacén. Consulte [Figura 2-6](#).

Figura 2-6 Cambio de especificaciones



Paso 3 Establezca **Backup Type** en **Application-Consistent Backup**. Haga clic en **Next**.

Paso 4 Haga clic en **Pay** y complete el pago. El sistema cambia automáticamente las especificaciones del almacén.

----**Fin**

2.9 Replicación de un almacén

CBR le permite replicar almacén de copia de respaldo de servidor, un almacén de copia de respaldo en la nube híbrida o un almacén de copia de respaldo SFS Turbo completamente en un almacén de replicación en otra región. Las réplicas de copias de respaldo de servidores en la región de destino se pueden utilizar para crear imágenes y aprovisionar servidores. Las réplicas de las copias de respaldo de sistemas de archivos SFS Turbo en la región de destino se pueden utilizar para crear sistemas de archivos.

Hay dos modos de replicación disponibles para replicar un almacén.

- Seleccione un almacén de copia de respaldo y replíquelo manualmente.
- Configure una política de replicación para replicar periódicamente backups que no se han replicado o que no se han replicado en la región de destino.

Restricciones

- Los almacenes de copia de respaldo en disco no se pueden replicar en otras regiones.
- Esta función solo está disponible en las regiones CN-Hong Kong, AP-Singapore y AP-Bangkok actualmente.
- La velocidad de replicación de un solo backup es de aproximadamente 80 MB/s. Se puede replicar un máximo de ocho backups a la vez.
- Los datos se pueden replicar en almacenes en diferentes regiones de destino. La creación de la réplica replicará todas las copias de respaldo del almacén de origen en el almacén de destino.
- Un almacén de copia de respaldo de servidor sólo se puede replicar si contiene al menos un backup que cumpla todas las condiciones siguientes:
 - a. La copia de respaldo es una copia de respaldo de ECS.
 - b. La copia de respaldo contiene datos del disco del sistema.
 - c. La copia de respaldo se encuentra en el estado **Available**.
- Sólo se pueden replicar almacenes de la región actual. Las réplicas no se pueden replicar de nuevo, pero se pueden utilizar para crear imágenes o sistemas de archivos.
- Un almacén de copia de respaldo se puede replicar en diferentes regiones de destino. La regla de replicación varía con el método de replicación:
 - Replicación manual: las copias de respaldo se pueden replicar en la región de destino siempre que su réplica se elimine de esa región.
 - Replicación basada en políticas: una vez que una copia de respaldo se ha replicado correctamente en la región de destino, no se puede replicar de nuevo en esa región, incluso si se ha eliminado su réplica.
- Sólo se pueden seleccionar regiones con capacidades de replicación como regiones de destino.

Procedimiento

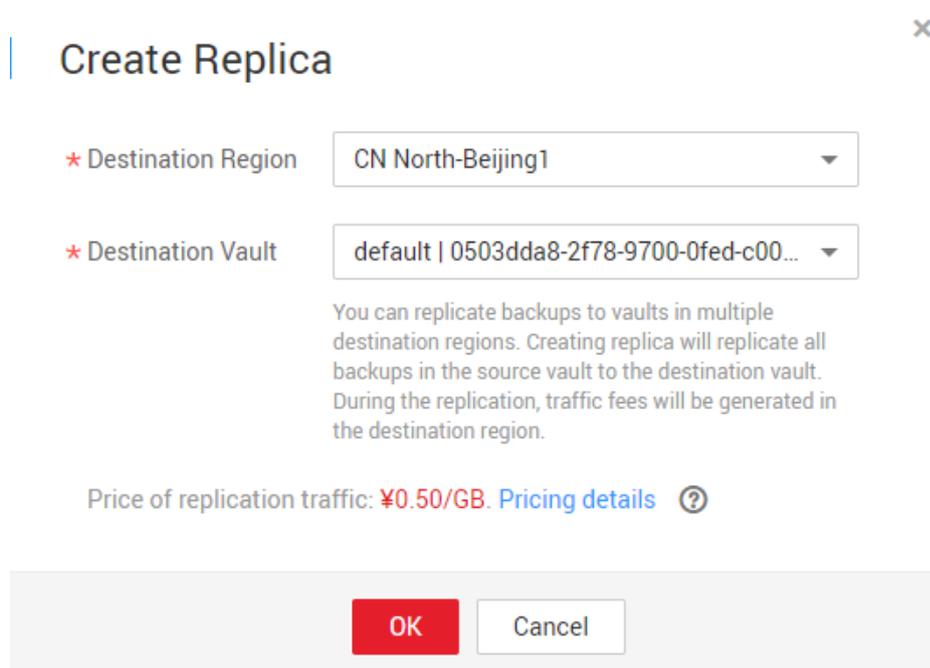
Paso 1 Inicie sesión en la consola de CBR.

1. [Inicie sesión en la consola de gestión](#).
2. Haga clic en  en la esquina superior izquierda y seleccione su región y proyecto.
3. Elija **Storage > Cloud Backup and Recovery**. Elija el tipo de copia de respaldo deseado en el panel de navegación izquierdo.

Paso 2 Haga clic en la pestaña **Vaults** y busque almacén de copia de respaldo de destino.

Paso 3 Haga clic en **More** y elija **Create Replica** en la columna **Operation** del almacén. Consulte [Figura 2-7](#).

Figura 2-7 Creación de una réplica



Paso 4 En el cuadro de diálogo que se muestra, establezca los parámetros como se describe en [Tabla 2-3](#).

Tabla 2-3 Descripción del parámetro

Parámetro	Descripción
Destination Region	Región en la que se replica el almacén Sólo se mostrarán las regiones que admitan replicación. <ul style="list-style-type: none"> ● Si la región seleccionada contiene sólo un proyecto, puede seleccionar directamente el nombre de la región. ● Si la región seleccionada tiene varios proyectos, el proyecto maestro de la región se selecciona de forma predeterminada. Puede seleccionar otro proyecto si es necesario.
Destination Vault	Un almacén de replicación en la región de destino

Paso 5 Haga clic en **OK**.

Paso 6 Una vez completada la replicación, puede cambiar a la región de destino para ver las réplicas generadas. Para más detalles, consulte [Consulta de un almacén](#). A continuación, puede utilizar réplicas para crear imágenes.

----**Fin**

2.10 Gestión de etiquetas de almacén

Puede agregar etiquetas a un almacén, así como editar y eliminar estas etiquetas. Las etiquetas Vault sólo se utilizan para filtrar y gestionar almacenes.

Procedimiento

Paso 1 Inicie sesión en la consola de CBR.

1. **Inicie sesión en la consola de gestión.**
2. Haga clic en  en la esquina superior izquierda y seleccione su región y proyecto.
3. Elija **Storage > Cloud Backup and Recovery**. Elija el tipo de copia de respaldo deseado en el panel de navegación izquierdo.

Paso 2 Haga clic en el nombre de un almacén y seleccione la pestaña **Tag** en la página de información del almacén que se muestra.

- Adición de una etiqueta
 - a. Haga clic en **Add Tag** en la esquina superior izquierda.
 - b. En el cuadro de diálogo que se muestra, establezca la clave y el valor de la nueva etiqueta.

Una etiqueta se representa en forma de un par clave-valor. Las etiquetas se utilizan para identificar, clasificar y buscar recursos en la nube. Las etiquetas Vault sólo se utilizan para filtrar y gestionar almacenes. Un almacén puede tener un máximo de 10 etiquetas.

Tabla 2-4 describe los parámetros de una etiqueta.

Tabla 2-4 Descripción del parámetro de etiqueta

Parámetro	Descripción	Valor de ejemplo
Key	Clave de etiqueta. Cada etiqueta de un almacén tiene una clave única. Puede personalizar la clave o seleccionar la clave de una etiqueta existente creada en TMS. Una clave de etiqueta: <ul style="list-style-type: none"> ■ Puede contener de 1 a 36 caracteres Unicode. ■ Puede contener solo letras, dígitos, guiones (-) y guiones bajos (_). 	Key_0001
Value	Un valor de etiqueta puede ser repetitivo o dejarse en blanco. Un valor de etiqueta: <ul style="list-style-type: none"> ■ Puede contener de 0 a 43 caracteres Unicode. ■ Puede contener solo letras, dígitos, guiones (-) y guiones bajos (_). 	Value_0001

- c. Haga clic en **OK**.
- Edición de una etiqueta
 - a. En la columna **Operation** de la etiqueta que desea editar, haga clic en **Edit**.
 - b. En el cuadro de diálogo **Edit Tag** que se muestra, modifique el valor de etiqueta. [Tabla 2-4](#) describe los parámetros.
 - c. Haga clic en **OK**.
- Eliminación de una etiqueta
 - a. En la columna **Operation** de la etiqueta que desea eliminar, haga clic en **Delete**.
 - b. En el cuadro de diálogo que se muestra, confirme la información de eliminación.
 - c. Haga clic en **OK**.

----Fin

2.11 Gestión del Proyecto empresarial de Vaults

Si necesita modificar el proyecto de empresa de un almacén, vaya a la página **Enterprise Management** para mover el almacén del proyecto de empresa original a uno nuevo.

Procedimiento

- Paso 1** Haga clic en **Enterprise** en la parte superior derecha de la página de consola. De forma predeterminada, se muestra la página **Overview** de Enterprise Management.
- Paso 2** En el panel de navegación de la página **Enterprise Management**, elija **Enterprise Project Management**.
- Paso 3** Busque el proyecto de empresa del que se eliminará el almacén. Haga clic en **View Resources** en la columna **Operation**. Se muestra la página de pestaña **Resources**. Puede ver los recursos en el proyecto de empresa actual.
- Paso 4** Seleccione **Single Resource** para el modo de eliminación.
- Paso 5** Seleccione el proyecto de empresa de destino al que se va a agregar el almacén y haga clic en **OK**.

Una vez eliminado el almacén del proyecto de empresa, puede verlo en la lista de recursos del proyecto de empresa de destino.

----Fin

3 Gestión de copias de respaldo

3.1 Consulta de una copia de respaldo

En la lista de copia de respaldo, puede establecer criterios de búsqueda para filtrar las copias de respaldo y ver los detalles de la copia de respaldo. Los resultados contienen tareas de copia de respaldo que se están ejecutando o que se han completado.

Prerrequisitos

Se ha creado una tarea de copia de respaldo.

Visualización de detalles de copias de respaldo

Paso 1 Inicie sesión en la consola de CBR.

1. [Inicie sesión en la consola de gestión.](#)
2. Haga clic en  en la esquina superior izquierda y seleccione su región y proyecto.
3. Elija **Storage > Cloud Backup and Recovery**. Elija el tipo de copia de respaldo deseado en el panel de navegación izquierdo.

Paso 2 En cualquier página de copia de respaldo, haga clic en la pestaña **Backups** y establezca criterios de filtro para ver las copias de respaldo.

La última hora activa mostrada en la lista de copia de respaldo de archivos muestra la última vez que el Agente informó de su estado al sistema.

- Puede buscar copias de seguridad seleccionando un estado en la lista desplegable **All statuses** en la esquina superior derecha de la lista de copias de seguridad. [Tabla 3-1](#) describe los estados de copia de respaldo.

Tabla 3-1 Estado de copia de respaldo

Estado	Atributo de estado	Descripción
All statuses	--	Todas las copias de respaldo se muestran si se selecciona este valor.
Available	A stable state	Un estado estable de una copia de respaldo después de que se crea la copia de respaldo, que indica que la copia de respaldo está disponible y que actualmente no se está utilizando. Este estado permite la mayoría de las operaciones.
Creating	An intermediate state	Estado intermedio de una copia de respaldo desde el inicio de un trabajo de copia de respaldo hasta la finalización de este trabajo. En la lista Tasks , se muestra una barra de progreso para una tarea de copia de respaldo en este estado. Si la barra de progreso permanece sin cambios durante un tiempo prolongado, se ha producido una excepción. Póngase en contacto con atención de cliente.
Restoring	An intermediate state	Un estado intermedio cuando se utiliza la copia de respaldo para restaurar datos. En la lista Tasks , se muestra una barra de progreso para una tarea de restauración en este estado. Si la barra de progreso permanece sin cambios durante un tiempo prolongado, se ha producido una excepción. Póngase en contacto con atención de cliente.
Deleting	An intermediate state	Un estado intermedio desde el inicio de la eliminación de la copia de respaldo hasta la finalización de la eliminación de la copia de respaldo. En la lista Tasks , se muestra una barra de progreso para una tarea de eliminación en este estado. Si la barra de progreso permanece sin cambios durante un tiempo prolongado, se ha producido una excepción. Póngase en contacto con atención de cliente.
Error	A stable state	Una copia de respaldo introduce el estado Error cuando se produce una excepción. Una copia de respaldo en este estado no se puede utilizar para la restauración y debe eliminarse manualmente. Si la eliminación manual falla, póngase en contacto con atención de cliente.

- Puede buscar copias de respaldo haciendo clic en **Advanced Search** en la esquina superior derecha de la lista de copias de respaldo.

Puede buscar especificando un estado de copia de respaldo, nombre de copia de respaldo, ID de copia de respaldo, ID de almacén, nombre de servidor, ID de servidor, tipo de servidor, si la copia de respaldo es una réplica, o la fecha de creación.

- Puede buscar copias de respaldo seleccionando un proyecto en la lista desplegable **All projects** en la esquina superior derecha de la lista de copias de respaldo.

Paso 3 Haga clic en el nombre de la copia de respaldo para ver detalles sobre la copia de respaldo.

----Fin

3.2 Compartir una copia de respaldo

Puede compartir una copia de respaldo de un servidor o disco con otros cuentas. Las copias de seguridad compartidas se pueden utilizar para crear servidores o discos.

Contexto

Sharer

- Las copias de seguridad solo se pueden compartir entre las cuentas de la misma región.
- Las copias de seguridad cifradas no se pueden compartir. Las copias de seguridad no se pueden compartir entre regiones. La cuenta en la que se comparte una copia de respaldo debe estar en la misma región que la copia de respaldo.
- Las copias de seguridad compartidas aceptadas se eliminarán una vez que el usuario haya eliminado la copia de respaldo original. Si se ha utilizado una copia de respaldo compartida para crear nuevos discos o servidores, los recursos creados no se eliminarán.

Recipient

- Un destinatario debe tener al menos un almacén de copia de respaldo para almacenar la copia de respaldo compartida aceptada, y el espacio restante del almacén debe ser mayor que el tamaño de la copia de respaldo que se va a aceptar.
- Un destinatario puede elegir si desea aceptar una copia de respaldo. Después de aceptar una copia de respaldo, el destinatario puede usar la copia de respaldo para crear nuevos servidores o discos.
- Las copias de seguridad compartidas aceptadas se eliminarán una vez que el usuario haya eliminado la copia de respaldo original. Si se ha utilizado una copia de respaldo compartida para crear nuevos discos o servidores, los recursos creados no se eliminarán.

Procedimiento para el sharer

Paso 1 Inicie sesión en la consola de CBR.

1. **Inicie sesión en la consola de gestión.**
2. Haga clic en  en la esquina superior izquierda y seleccione su región y proyecto.
3. Elija **Storage > Cloud Backup and Recovery**. Elija el tipo de copia de respaldo deseado en el panel de navegación izquierdo.

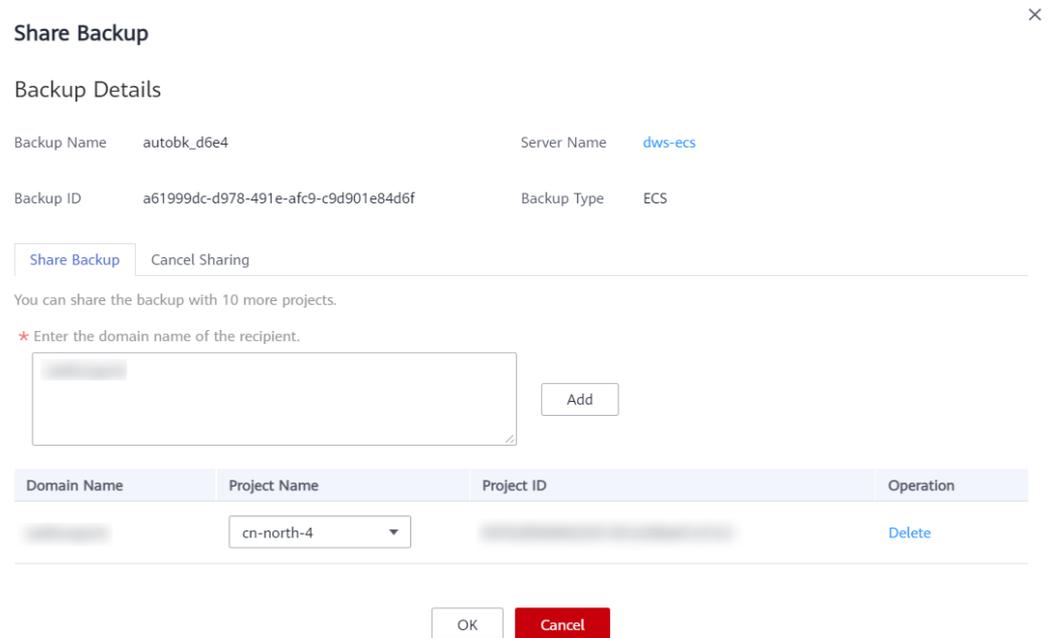
Paso 2 En la página de copia de respaldo del servidor en la nube o del disco en la nube, haga clic en la pestaña **Backups** y establezca criterios de filtro para ver las copias de seguridad.

Paso 3 Localice la copia de respaldo de destino y elija **More > Share Backup** en la columna **Operation**.

Se muestran el nombre de la copia de respaldo, el nombre del servidor, el ID de la copia de respaldo y el tipo de copia de respaldo.

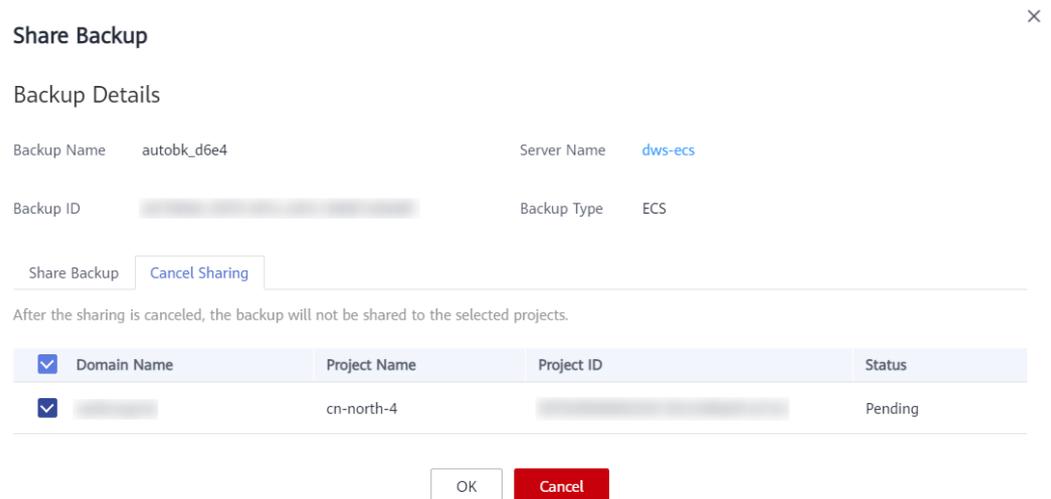
- Compartir una copia de respaldo

Figura 3-1 Compartir una copia de respaldo



1. Haga clic en la pestaña **Share Backup**.
 2. Introduzca el nombre de la cuenta del inquilino con quien se va a compartir la copia de respaldo.
 3. Haga clic en **Add**. El nombre de la cuenta y el proyecto que se van a agregar se muestran en la lista. Puedes seguir agregando nombres de cuenta. Una copia de respaldo se puede compartir con un máximo de diez proyectos.
 4. Haga clic en **OK**.
- Cancelar el uso compartido
 1. Localice la copia de respaldo de destino y elija **More > Share Backup** en la columna **Operation**.
 2. En la página mostrada, haga clic en la pestaña **Cancel Sharing** y seleccione la copia de respaldo que ya no necesita compartirse. A continuación, haga clic en **OK**. Consulte [Figura 3-2](#).

Figura 3-2 Cancelar el uso compartido



----Fin

Procedimiento para el Destinatario

Paso 1 Inicie sesión en la consola de CBR.

1. **Inicie sesión en la consola de gestión.**
2. Haga clic en  en la esquina superior izquierda y seleccione su región y proyecto.
3. Elija **Storage > Cloud Backup and Recovery**. Elija el tipo de copia de respaldo deseado en el panel de navegación izquierdo.

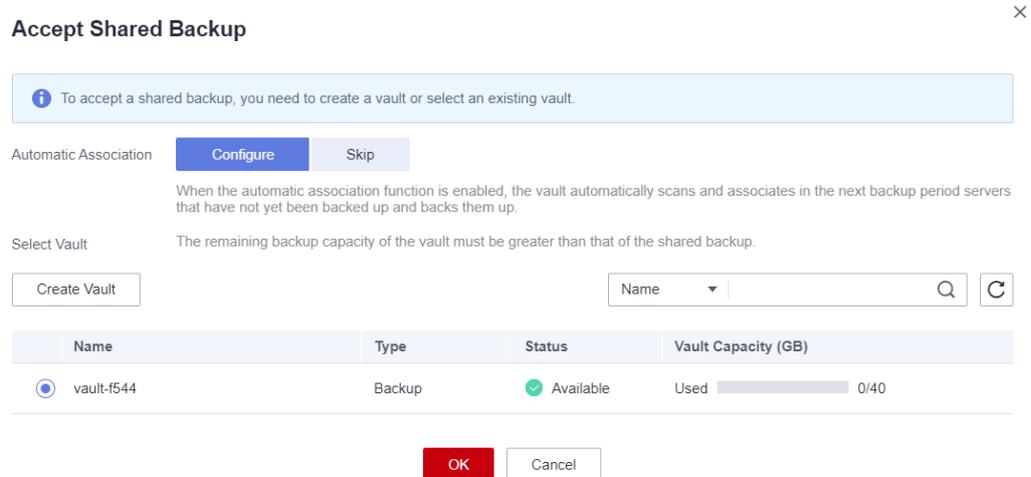
Paso 2 En la página de copia de respaldo del servidor en la nube o del disco en la nube, haga clic en la pestaña **Backups** y, a continuación, haga clic en **Backups Shared with Me**.

Paso 3 Asegúrese de que el destinatario tiene al menos un almacén de copia de respaldo antes de aceptar la copia de respaldo compartida. Para obtener información sobre **Comprar un almacén**.

Paso 4 Haga clic en **Accept**. En la página mostrada, seleccione el almacén utilizado para almacenar la copia de respaldo compartida. Asegúrese de que la capacidad restante del almacén es mayor que el tamaño de la copia de respaldo. Consulte **Figura 3-3**.

Asociación automática: determine si desea habilitar la asociación automática para el almacén. Si selecciona **Configure**, el almacén analiza y asocia automáticamente en el siguiente período de copia de respaldo los servidores que no se han realizado copias de seguridad y realiza copias de seguridad.

Figura 3-3 Aceptar una copia de respaldo compartida



Paso 5 Después de aceptar una copia de respaldo compartida, se mostrará en la lista de copias de seguridad. Consulte [Figura 3-4](#).

Figura 3-4 Copia de respaldo compartida aceptada



----Fin

3.3 Eliminación de una copia de respaldo

Puede eliminar copias de respaldo no deseadas para reducir el uso de espacio y los costos.

La eliminación de una copia de respaldo de una bóveda de copia de respaldo en la nube híbrida no afecta a la copia de respaldo local correspondiente, y viceversa.

Si se ha utilizado una copia de respaldo para crear una imagen, la copia de respaldo no se puede eliminar. En este caso, elimine primero la imagen según las instrucciones en [Eliminación de imágenes](#).

Contexto

CBR admite la eliminación manual de copias de respaldo y la eliminación automática de copias de respaldo caducadas. Este último se implementa en función de la regla de retención de copias de respaldo en la política de copias de respaldo. Para más detalles, consulte [Creación de una política de copia de respaldo](#).

Prerrequisitos

- Existe al menos una copia de respaldo.

- La copia de respaldo que se va a eliminar está en el estado **Available** o **Error**.

Procedimiento

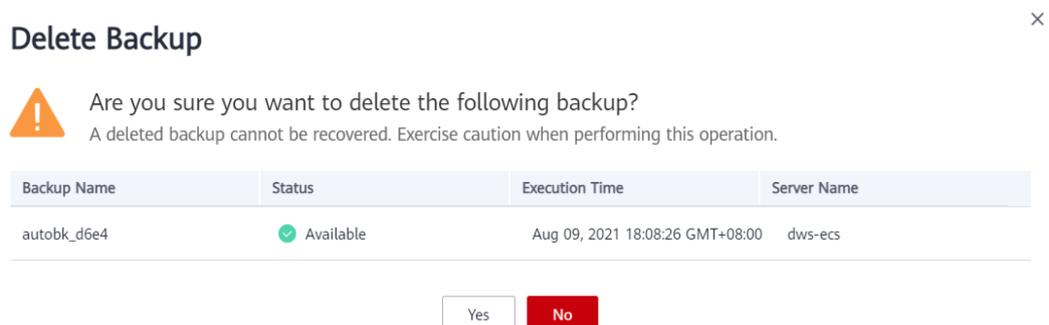
Paso 1 Inicie sesión en la consola de CBR.

1. **Inicie sesión en la consola de gestión.**
2. Haga clic en  en la esquina superior izquierda y seleccione su región y proyecto.
3. Elija **Storage > Cloud Backup and Recovery**. Elija el tipo de copia de respaldo deseado en el panel de navegación izquierdo.

Paso 2 En cualquier página de copia de respaldo, haga clic en la pestaña **Backups** y busque la copia de respaldo deseada. Para más detalles, consulte [Consulta de una copia de respaldo](#).

Paso 3 En la fila de la copia de respaldo, elija **More > Delete**. Consulte [Figura 3-5](#). Alternativamente, seleccione las copias de respaldo que desea eliminar y haga clic en **Delete** en la esquina superior izquierda para eliminarlas en un lote.

Figura 3-5 Eliminación de una copia de respaldo



Paso 4 Haga clic en **Yes**.

----Fin

Procedimiento posterior

Cuando utiliza CBR para realizar una copia de respaldo de un disco, se realizará una copia de respaldo de todos los datos del disco, incluidos los datos invisibles. Si se han realizado operaciones frecuentes de adición, eliminación y modificación en el disco antes de cada tarea de copia de respaldo, se seguirá ocupando una gran cantidad de espacio del almacén incluso después de eliminar algunas copias de respaldo. Para obtener información sobre cómo reducir el espacio ocupado en la bóveda, consulte [¿Cómo puedo reducir el espacio ocupado por las copias de respaldo?](#)

3.4 Uso de una copia de respaldo para crear una imagen

CBR le permite crear imágenes usando copias de respaldo de ECS. Puede utilizar las imágenes para aprovisionar ECS para restaurar rápidamente entornos en ejecución de servicios.

Prerrequisitos

- Confirme que se han realizado las siguientes operaciones antes de utilizar una copia de respaldo de ECS para crear una imagen:
 - Ha optimizado el ECS de Linux (refiriéndose a [Optimizar una imagen privada de Linux](#)) e instalado Cloud-Init (refiriéndose a [Instalar Cloud-Init](#)).
 - Ha optimizado el ECS de Windows (refiriéndose a [Optimizar una imagen privada de Windows](#)) e instalado Cloudbase-Init (refiriéndose a [Instalar y configurar Cloudbase-Init](#)).
- Una copia de respaldo se puede utilizar para crear una imagen en cualquiera de los siguientes escenarios: 1. La copia de respaldo se encuentra en el estado **Available**. 2. La copia de respaldo está en el estado de **Creating** que está marcado con **Image can be created**.

NOTA

Una vez que se inicia la creación de una copia de respaldo, la copia de respaldo entra en el estado **Creating**. Después de un período de tiempo, se muestra un mensaje que indica "Image can be created" en **Creating**. En este caso, la copia de respaldo se puede utilizar para crear una imagen, aunque todavía se está creando y no se puede utilizar para la restauración.

- La copia de respaldo que desea utilizar para crear una imagen contiene los datos del disco del sistema.
- Solo se pueden usar copias de respaldo de ECS para crear imágenes.

Descripción de funciones

- Las imágenes creadas con una copia de respaldo son las mismas, por lo que CBR le permite utilizar una copia de respaldo para crear solo una imagen completa de ECS que contiene todos los datos del disco del sistema y los discos de datos de un ECS, con el fin de guardar la cuota de imagen. Después de crear una imagen, puede utilizar la imagen para aprovisionar varios ECS en un lote.
- Una copia de respaldo con una imagen creada no se puede eliminar directamente. Si desea eliminar una copia de respaldo de este tipo, elimine primero su imagen. Si una copia de respaldo se genera automáticamente según una política de copia de respaldo y la copia de respaldo se ha utilizado para crear una imagen, la copia de respaldo no se contabilizará como una copia de respaldo retenida y no se eliminará automáticamente.
- Una copia de respaldo se comprime cuando se utiliza para crear una imagen. Por lo tanto, el tamaño de la imagen generada es menor que el de la copia de respaldo.

Procedimiento

Paso 1 Inicie sesión en la consola de CBR.

1. [Inicie sesión en la consola de gestión.](#)

2. Haga clic en  en la esquina superior izquierda y seleccione su región y proyecto.
3. Elija **Storage > Cloud Backup and Recovery**. Elija el tipo de copia de respaldo deseado en el panel de navegación izquierdo.

Paso 2 Haga clic en la pestaña **Backups**. Localice la copia de respaldo deseada. Para más detalles, consulte [Consulta de una copia de respaldo](#).

Paso 3 En la fila de la copia de respaldo, elija **More > Create Image**.

Paso 4 Cree una imagen haciendo referencia a [Creación de una imagen de ECS completo a partir de una copia de respaldo de CBR](#) en la *Guía de usuario de Image Management Service*.

Paso 5 Si desea utilizar una imagen para aprovisionar ECS, consulte [Creación de un ECS a partir de una imagen](#) en la *Guía de usuario de Image Management Service*.

---Fin

3.5 Uso de una copia de respaldo para crear un disco

Puede utilizar una copia de respaldo de disco para crear un disco. Después de crear el disco, los datos en el nuevo disco son los mismos que en la copia de respaldo del disco.

Después de crear un nuevo disco usando los datos de copia de respaldo de un disco del sistema, el nuevo disco solo se puede montar en el servidor en la nube como un disco de datos y no se puede montar como un disco del sistema.

Las copias de seguridad de disco solo se pueden usar para crear discos EVS, pero no para servidores.

Procedimiento

Paso 1 Inicie sesión en la consola de CBR.

1. [Inicie sesión en la consola de gestión](#).
2. Haga clic en  en la esquina superior izquierda y seleccione su región y proyecto.
3. Elija **Storage > Cloud Backup and Recovery**. Elija el tipo de copia de respaldo deseado en el panel de navegación izquierdo.

Paso 2 Haga clic en la pestaña **Backups**. Localice la copia de respaldo deseada. Para más detalles, consulte [Consulta de una copia de respaldo](#).

Paso 3 Si el estado de la copia de respaldo de destino es **Available**, haga clic en **Create Disk** en la columna **Operation** de la copia de respaldo.

Paso 4 Establezca los parámetros del disco.

NOTA

Para obtener más información acerca de estos parámetros, consulte la tabla de descripción de parámetros en la sección "Comprar un disco EVS" de la *Guía del usuario de Elastic Volume Service*.

Tenga en cuenta los siguientes elementos al configurar los parámetros del disco:

- Puede elegir la zona de disponibilidad a la que pertenece el disco de origen de copia de respaldo, o puede elegir una zona de disponibilidad diferente.
- El nuevo disco debe ser al menos tan grande como el disco de origen de la copia de respaldo.
Si la capacidad del disco nuevo es mayor que la del disco de origen de copia de respaldo, inicialice el disco siguiendo los pasos proporcionados en la sección "Ampliación de particiones de disco y sistemas de archivos" *Guía del usuario de Elastic Volume Service*.
- Puede crear un disco de cualquier tipo independientemente del tipo de disco de la copia de respaldo.

Paso 5 Haga clic en **Next**.

NOTA

Puedes elegir **Pay-per-use** o **Yearly/Monthly** como **Billing Mode**. Las tarifas que paga dependen del modo de facturación que elija. Los siguientes pasos utilizan el modo de facturación **Yearly/Monthly** como ejemplo.

Paso 6 Confirme la información del disco y haga clic en **Submit**.

Paso 7 Pague las tarifas según se le indique y haga clic en **OK**.

Paso 8 Vuelve a la lista de discos. Compruebe si el disco se ha creado correctamente.

Verá que el estado del disco cambia de la siguiente manera: **Creating**, **Available**, **Restoring**, **Available**. Es posible que no note el estado **Restoring** porque se admite la restauración instantánea y la velocidad de restauración es muy rápida. Una vez que el estado del disco ha cambiado de **Creating** a **Available**, el disco se crea correctamente. Una vez que el estado ha cambiado de **Restoring** a **Available**, los datos de copia de respaldo se han restaurado correctamente en el disco creado.

----Fin

3.6 Uso de una copia de respaldo para crear un sistema de archivos

En caso de un ataque de virus, eliminación accidental o fallo de software o hardware, puede utilizar una copia de respaldo del sistema de archivos SFS Turbo para crear un nuevo sistema de archivos. Después de crearlo, los datos del nuevo sistema de archivos son los mismos que los de la copia de respaldo.

Procedimiento

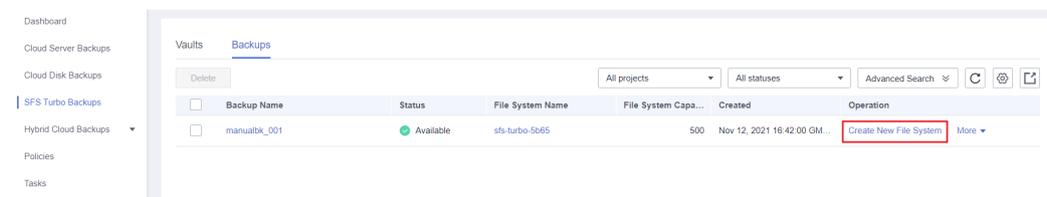
Paso 1 Inicie sesión en la consola de CBR.

1. **Inicie sesión en la consola de gestión.**
2. Haga clic en  en la esquina superior izquierda y seleccione su región y proyecto.
3. Elija **Storage > Cloud Backup and Recovery**. Elija el tipo de copia de respaldo deseado en el panel de navegación izquierdo.

Paso 2 Haga clic en la pestaña **Backups**. Localice la copia de respaldo deseada. Para más detalles, consulte [Consulta de una copia de respaldo](#).

Paso 3 Si el estado de la copia de respaldo de destino es **Available**, haga clic en **Create File System** en la columna **Operation** de la copia de respaldo.

Figura 3-6 Consulta de una copia de respaldo



NOTA

Para obtener información sobre cómo crear copias de seguridad, consulte [Compra de un almacén de copia de respaldo de SFS Turbo](#) y [Creación de una copia de respaldo de SFS Turbo](#).

Paso 4 Establezca los parámetros del sistema de archivos.

NOTA

- Para obtener descripciones detalladas de los parámetros, consulte la tabla "Descripción del parámetro" en [Creación de sistema de archivo de SFS Turbo](#).
- Puede cambiar la clase de almacenamiento del sistema de archivos dentro de un rango determinado. Por ejemplo, puede cambiar un sistema de archivos de Estándar a Rendimiento, pero no de Estándar a Estándar - Mejorado.
- El modo de facturación del nuevo sistema de archivos solo puede ser de pago por uso.

Paso 5 Haga clic en **Next**.

Paso 6 Confirme la información del sistema de archivos y haga clic en **Submit**.

Paso 7 Pague las tarifas según se le indique y haga clic en **OK**.

Paso 8 Vuelva a la lista del sistema de archivos y compruebe si el sistema de archivos se ha creado correctamente.

Verá que el estado del sistema de archivos cambia de la siguiente manera: **Creating**, **Available**, **Restoring**, **Available**. Es posible que no note el estado **Restoring** porque se admite la restauración instantánea y la velocidad de restauración es muy rápida. Una vez que el estado del sistema de archivos ha cambiado de **Creating** a **Available**, el sistema de archivos se crea correctamente. Después de que el estado ha cambiado de **Restoring** a **Available**, los datos de copia de respaldo se han restaurado correctamente en el sistema de archivos creado.

----Fin

3.7 Replicación de una copia de respaldo (en todas las regiones)

CBR le permite replicar copias de respaldo del servidor y copias de respaldo SFS Turbo de una región a otra. Las réplicas de copias de respaldo de servidores en la región de destino se

pueden utilizar para crear imágenes y aprovisionar servidores. Las réplicas de las copias de respaldo de sistemas de archivos SFS Turbo en la región de destino se pueden utilizar para crear sistemas de archivos. Con la replicación de backup, puede implementar rápidamente servicios en una región diferente. El estado del nuevo recurso en la región de destino es el mismo que el del recurso de origen en el punto de tiempo de copia de respaldo en la región de origen.

La consola CBR proporciona los siguientes métodos para la replicación:

- Seleccione una copia de respaldo de la lista de copias de respaldo y realice una replicación única manualmente.
- Seleccione un almacén de copia de respaldo y replíquelo manualmente. También puede configurar una política de replicación para replicar periódicamente copias de respaldo que no se han replicado o que no se han replicado en la región de destino.

Esta sección utiliza la primera forma de describir cómo replicar una copia de respaldo. Para obtener más información sobre el segundo método, consulte [Replicación de un almacén](#).

NOTA

Las siguientes restricciones se aplican a ambos métodos de replicación.

Restricciones

- Las copias de respaldo de disco en la nube no se pueden replicar en otras regiones.
- Esta función solo está disponible en las regiones CN-Hong Kong, AP-Singapore y AP-Bangkok actualmente.
- Una copia de respaldo del servidor sólo se puede replicar si cumple todas las condiciones siguientes:
 - a. Es una copia de respaldo de ECS.
 - b. Contiene datos del disco del sistema.
 - c. Se encuentra en el estado **Available**.
- Sólo se pueden replicar copias de respaldo y depósitos de la región actual. Las réplicas no se pueden replicar de nuevo, pero se pueden utilizar para crear imágenes o sistemas de archivos.
- Una copia de respaldo se puede replicar en varias regiones de destino, pero solo puede tener una réplica en cada región de destino. La regla de replicación varía con el método de replicación:
 - Replicación manual: se puede replicar una copia de respaldo en la región de destino siempre que no tenga réplica en la región de destino. Una copia de respaldo se puede replicar de nuevo si su réplica se ha eliminado en la región de destino.
 - Replicación basada en políticas: una vez que una copia de respaldo se ha replicado correctamente en la región de destino, no se puede replicar de nuevo en esa región, incluso si se ha eliminado su réplica.
- Sólo se pueden seleccionar regiones con capacidades de replicación como regiones de destino.

Procedimiento

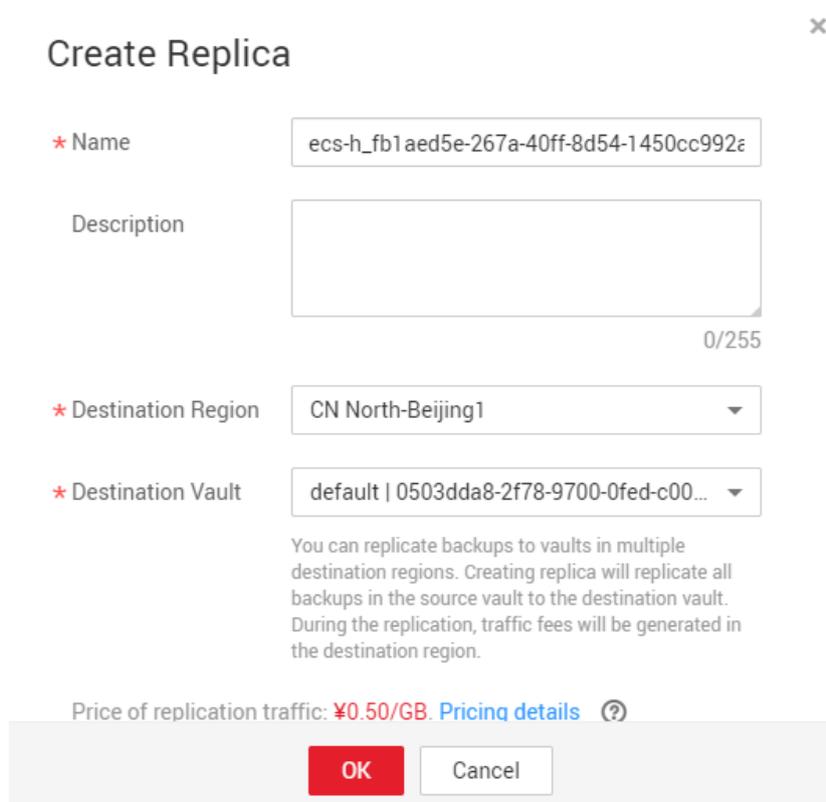
Paso 1 Inicie sesión en la consola de CBR.

1. **Inicie sesión en la consola de gestión.**
2. Haga clic en  en la esquina superior izquierda y seleccione su región y proyecto.
3. Elija **Storage > Cloud Backup and Recovery**. Elija el tipo de copia de respaldo deseado en el panel de navegación izquierdo.

Paso 2 Haga clic en la pestaña **Backups** y busque la copia de respaldo deseada. Para más detalles, consulte [Consulta de una copia de respaldo](#).

Paso 3 Haga clic en **More** y elija **Create Replica** en la columna **Operation** de la copia de respaldo. Consulte [Figura 3-7](#).

Figura 3-7 Creación de una réplica



Paso 4 En el cuadro de diálogo que se muestra, establezca los parámetros como se describe en [Tabla 3-2](#).

Tabla 3-2 Descripción del parámetro

Parámetro	Descripción
Name	Nombre de la réplica Un nombre debe contener de 1 a 64 caracteres, incluidos dígitos, letras, guiones bajos (_) o guiones (-).
Descripción	Descripción de la réplica No puede superar los 255 caracteres.

Parámetro	Descripción
Destination Region	Región en la que se replica el almacén Sólo se mostrarán las regiones que admitan replicación. <ul style="list-style-type: none">● Si la región seleccionada contiene sólo un proyecto, puede seleccionar directamente el nombre de la región.● Si la región seleccionada tiene varios proyectos, el proyecto maestro de la región se selecciona de forma predeterminada. Puede seleccionar otro proyecto si es necesario.
Destination Vault	Un almacén de replicación en la región de destino Las copias de respaldo pueden replicarse en almacenes de múltiples regiones. La creación de la réplica replicará todas las copias de respaldo del almacén de origen en el almacén de destino.

 **NOTA**

El tráfico para la replicación entre regiones es el tamaño del copia de respaldo replicado.

Paso 5 Haga clic en **OK**.

Paso 6 Una vez completada la replicación, puede cambiar a la región de destino para ver las réplicas generadas. Para más detalles, consulte [Consulta de una copia de respaldo](#). A continuación, puede utilizar réplicas para crear imágenes.

---**Fin**

4 Gestión de política

4.1 Creación de una política de copia de respaldo

Una política de copia de respaldo permite que un almacén ejecute automáticamente tareas de copia de respaldo en momentos o intervalos especificados. Las copias de respaldo periódicas se pueden utilizar para restaurar los datos rápidamente contra la corrupción o pérdida de datos.

Para implementar copias de respaldo periódicas, primero debe crear una política de copias de respaldo. A continuación, CBR realizará periódicamente copias de respaldo de acuerdo con el tiempo de ejecución especificado en la política de copia de respaldo. Puede elegir usar la política de copia de respaldo predeterminada proporcionada por CBR o crear una según sea necesario.

Puede aplicar políticas de copia de respaldo a almacenes de copia de respaldo de servidores, almacenes de copia de respaldo de SFS Turbo y almacenes de copia de respaldo de disco.

Contexto

- Después de habilitar una política de copia de respaldo, CBR realiza automáticamente una copia de respaldo de los recursos asociados a los almacenes asociados a la política y elimina periódicamente las copias de respaldo caducadas.
- Cada cuenta puede crear un máximo de 32 políticas de copia de respaldo.
- Al configurar el tiempo de copia de respaldo y el tiempo de replicación, asegúrese de que una tarea de replicación se inicie después de completar una tarea de copia de respaldo. O bien, la replicación puede fallar.
- Cuando las copias de respaldo caducadas se borran según las reglas de retención de una política, solo se eliminarán las copias de respaldo automáticas. La copia de respaldo manual no se eliminará.
- Solo se puede realizar una copia de respaldo de los servidores en el estado **Running** o **Stopped**.
- Solo se puede realizar una copia de respaldo de los discos en el estado **Available** o **In-use**.

Procedimiento

Paso 1 Inicie sesión en la consola de CBR.

1. **Inicie sesión en la consola de gestión.**
2. Haga clic en  en la esquina superior izquierda y seleccione su región y proyecto.
3. Elija **Storage > Cloud Backup and Recovery**. Elija el tipo de copia de respaldo deseado en el panel de navegación izquierdo.

Paso 2 Elija **Policies** y haga clic en la pestaña **Backup Policies**. En la esquina superior derecha, haz clic en **Create Policy**. Consulte [Figura 4-1](#).

Figura 4-1 Creación de una política de copia de respaldo

×

Create Policy

Basic Information

Type Backup policy Replication policy

Name

Status Enabled Disabled

Backup Rule

Current rule:
Automatically perform weekly backups at 22:00 on the following selected days: Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday

Backup Frequency Weekly Day based

Automatically perform backups every Mon Tues Wed Thur Fri Sat Sun

Execution Time Select All Invert Selection

00:00	01:00	02:00	03:00	04:00
05:00	06:00	07:00	08:00	09:00
10:00	11:00	12:00	13:00	14:00
15:00	16:00	17:00	18:00	19:00
20:00	21:00	22:00	23:00	

Create Now Cancel

Paso 3 Establezca los parámetros de política de copia de respaldo. [Tabla 4-1](#) describe los parámetros.

Tabla 4-1 Descripción del parámetro de política de copia de respaldo

Parámetro	Descripción	Valor de ejemplo
Type	Seleccione un tipo de política. En esta sección se utiliza la creación de una política de copia de respaldo como ejemplo.	Backup policy
Name	Nombre de política de copia de respaldo Un nombre debe contener de 1 a 64 caracteres, incluidos dígitos, letras, guiones bajos (_) o guiones (-).	backup_policy
Status	Si se debe habilitar la política de copia de respaldo.	Solo después de habilitar una política de copia de respaldo, CBR realiza automáticamente copias de respaldo de los servidores y discos asociados con los almacenes aplicados a la política y elimina las copias de respaldo caducadas.
Backup Frequency	Fechas para realizar copias de respaldo <ul style="list-style-type: none"> ● Weekly Especifica en qué días de cada semana se ejecutará la tarea de copia de respaldo. Puede seleccionar varios días. ● Day based Especifica el intervalo (cada 1 a 30 días) para ejecutar la tarea de copia de respaldo. 	Todos los días Si selecciona una copia de respaldo basada en días, se supone que la primera hora de copia de respaldo será el día en que se crea la política de copia de respaldo. Si el tiempo de creación de la política de copia de respaldo es posterior al último tiempo de ejecución, la copia de respaldo inicial se realizará en el siguiente ciclo de copia de respaldo. Se recomienda que las copias de respaldo se realicen durante las horas no pico o cuando no hay servicios en ejecución.

Parámetro	Descripción	Valor de ejemplo
Execution Time	<p>Hora de ejecución</p> <p>Las copias de respaldo se pueden programar al principio de cada hora. Se admiten varias selecciones.</p> <p>AVISO</p> <ul style="list-style-type: none"> ● Puede haber una diferencia de tiempo entre el tiempo de copia de respaldo programado y el tiempo de copia de respaldo real. ● Para realizar una copia de respaldo de una gran cantidad de datos, se recomienda establecer un programa de copia de respaldo menos frecuente. Si una tarea de copia de respaldo tarda más que el intervalo de copia de respaldo, el sistema omitirá el siguiente tiempo de ejecución de la copia de respaldo. Por ejemplo, como está programado en una política de copia de respaldo, un disco debe ser respaldado a las 00:00, 01:00 y 02:00. A las 00:00, se inicia la copia de respaldo del disco. Debido a que los datos incrementales de alto volumen necesitan ser respaldados o un montón de tareas de copia de respaldo se ejecutan al mismo tiempo, esta tarea de copia de respaldo tarda 90 minutos y se completa a las 01:30. En este caso, el sistema realiza la siguiente copia de respaldo a las 02:00. Por lo tanto, solo se generarán dos copias de respaldo en total, una a las 00:00 y la otra a las 02:00. 	<p>00:00, 02:00</p> <p>Se recomienda que las copias de respaldo se realicen durante las horas no pico o cuando no hay servicios en ejecución.</p>

Parámetro	Descripción	Valor de ejemplo
Full Backup	<p>Si se deben realizar copias de respaldo completas periódicas.</p> <ul style="list-style-type: none"> ● Habilitar Habilitar la copia de respaldo completa mejora la confiabilidad de sus datos, pero las copias de respaldo completas utilizarán más espacio de almacenamiento. <p>Configure una frecuencia de copia de respaldo completa. El valor varía de 0 a 100. El valor 0 indica que se realizará una copia de respaldo completa en cada tarea de copia de respaldo.</p> ● No habilitar No se realizará una copia de respaldo completa periódica. En su lugar, el sistema siempre realizará copias de respaldo incrementales después de la copia de respaldo inicial. <p>AVISO Una copia de respaldo completa generalmente toma un largo período de tiempo. Si se está ejecutando una copia de respaldo completa de un recurso, no se generarán otras copias de respaldo de este recurso. Por ejemplo, se omitirán las copias de respaldo basadas en políticas que se planeen ejecutar durante la copia de respaldo completa. Puede realizar copias de respaldo de los datos durante las horas no pico.</p> 	7

Parámetro	Descripción	Valor de ejemplo
Retention Rule	<p>Regla que especifica cómo se conservarán las copias de respaldo</p> <ul style="list-style-type: none"> ● Time period Puede optar por conservar las copias de respaldo durante un mes, tres meses, seis meses, un año o por cualquier número deseado (2 a 99999) de días. ● Backup quantity Puede establecer el número máximo de copias de respaldo de servidores en la nube que se conservarán para un servidor en la nube. El valor oscila entre 2 y 99999. ● Advanced Options También puede establecer reglas de retención a largo plazo con opciones avanzadas. Las reglas de retención a largo plazo y las reglas de retención basadas en cantidades no entran en conflicto. Ambos serán aplicados. <ul style="list-style-type: none"> – Day-based: el valor varía de 0 a 100. – Weekly: El valor varía de 0 a 100. – Monthly: El valor varía de 0 a 100. – Yearly: El valor varía de 0 a 100. <p>Por ejemplo, la opción avanzada basada en el día conserva la copia de respaldo más reciente por día. Si se realiza una copia de respaldo de un disco varias veces al día, solo se conserva la copia de respaldo más reciente de ese día. Si establece el valor en 5, el sistema mantiene la copia de respaldo más reciente de cada uno de los últimos cinco días que han generado copias de respaldo. Si hay más de cinco archivos de copia de respaldo, el sistema elimina automáticamente las copias de respaldo más tempranas. Si todas las opciones avanzadas diarias, semanales, mensuales y anuales están configuradas, las copias de respaldo de la unión se seleccionan para la retención. Por ejemplo, si el número de copias de respaldo retenidas basadas en días se establece en 5 y el número de copias de respaldo semanales retenidas se establece en 1, se conservarán cinco copias de respaldo. La regla de retención a largo plazo y la regla</p>	6 meses

Parámetro	Descripción	Valor de ejemplo
	<p>de retención basada en cantidades pueden ser efectivas al mismo tiempo.</p> <ul style="list-style-type: none"> ● Permanent <p>NOTA</p> <ul style="list-style-type: none"> – Cuando el número de copias de respaldo retenidas excede el valor preestablecido, el sistema elimina automáticamente las copias de respaldo más tempranas. Cuando los períodos de retención de las copias de respaldo retenidas exceden el valor preestablecido, el sistema elimina automáticamente todas las copias de respaldo caducadas. De forma predeterminada, el sistema borra automáticamente los datos cada dos días. La copia de respaldo eliminada no afecta a otras copias de respaldo para la restauración. – Las copias de respaldo caducadas no se eliminan justo después de que hayan caducado. Se eliminarán de 12:00 a 0:00 en lotes. – Este parámetro sólo se aplica a las copias de respaldo generadas en función de una política de copia de respaldo programada. Las copias de respaldo manuales no se ven afectadas por este parámetro y no se eliminarán automáticamente. Puede eliminarlos manualmente de la lista de copia de respaldo. – Una vez que se utiliza una copia de respaldo para crear una imagen, la copia de respaldo no se contará como una copia de respaldo conservada y no se eliminará automáticamente. – Se conservan un máximo de 10 copias de respaldo para las tareas de copia de respaldo periódicas fallidas. Se conservan durante un mes y se pueden eliminar manualmente. 	

 **NOTA**

Los intervalos de copia de respaldo más frecuentes crean más copias de respaldo o retienen las copias de respaldo durante más tiempo, protegiendo los datos en mayor medida pero ocupando más espacio de almacenamiento. Establezca un ciclo de respaldo adecuado según sea necesario.

Paso 4 Haga clic en **OK**.

Paso 5 Busque el almacén deseado y elija **More > Apply Backup Policy** para aplicar la política creada al almacén. Puede ver la política aplicada en la página de detalles del almacén.

Una vez aplicada la política, se realizará una copia de respaldo periódica de los datos en el almacén en función de la política.

---Fin

Ejemplo

Un usuario tiene un almacén asociado a un disco. A las 10:00 a.m. el lunes, el usuario establece una política de copia de respaldo para el almacén, es decir, ejecutar una tarea de copia de respaldo a las 02:00 a.m. cada día y conservando un máximo de tres copias de respaldo. A las 11:00 a.m. el sábado, se conservan tres copias de respaldo, que se generan el miércoles, jueves y viernes. La copia de respaldo generada a las 2:00 a.m. el martes se ha eliminado automáticamente.

4.2 Creación de una política de replicación

Después de configurar una política de replicación, CBR replicará periódicamente las copias de respaldo que no se han replicado o que no se han replicado en la región de destino.

Puede aplicar políticas de replicación a almacenes de respaldo de servidores, almacenes de copia de respaldo de nube híbrida, y almacenes de copia de respaldo.

Contexto

Al configurar el tiempo de copia de respaldo y el tiempo de replicación, asegúrese de que una tarea de replicación se inicie después de completar una tarea de copia de respaldo. O bien, la replicación puede fallar.

Procedimiento

Paso 1 Inicie sesión en la consola de CBR.

1. [Inicie sesión en la consola de gestión.](#)
2. Haga clic en  en la esquina superior izquierda y seleccione su región y proyecto.
3. Elija **Storage > Cloud Backup and Recovery**. Elija el tipo de copia de respaldo deseado en el panel de navegación izquierdo.

Paso 2 Haga clic en la pestaña **Replication Policies**. En la esquina superior derecha, haz clic en **Create Policy**. Consulte [Figura 4-2](#).

Figura 4-2 Creación de una política de replicación

The screenshot shows the 'Create Policy' configuration page. At the top, there is a 'Back to CBR Policy List' link. The main configuration area includes:

- Type:** Two radio buttons, 'Backup policy' and 'Replication policy'. 'Replication policy' is selected.
- Name:** A text input field containing 'backup_policy'.
- Status:** A toggle switch that is turned on.
- Execution Time:** A grid of time slots from 00:00 to 23:00. The 00:00 and 02:00 slots are selected.
- Replication Cycle:** Two radio buttons, 'Week-based cycle' and 'Custom cycle'. 'Custom cycle' is selected. Below it, 'Every' is followed by a minus sign, the number '1', and a plus sign, followed by the word 'days'.
- Retention Rule:** Three radio buttons, 'Replica quantity', 'Time period', and 'Permanent'. 'Time period' is selected. Below it, a dropdown menu shows '6 months'.
- Destination Region:** A dropdown menu showing 'CN North-Beijing1'.
- Price of replication traffic:** Displayed as '¥0.50/GB'. There are links for 'Pricing details' and a help icon.
- Buttons:** 'OK' and 'Cancel' buttons at the bottom.

Paso 3 Establezca los parámetros de la política de replicación. [Tabla 4-2](#) describe los parámetros.

Tabla 4-2 Descripción del parámetro de política de replicación

Parámetro	Descripción	Comentarios
Type	Seleccione un tipo de política. En esta sección se utiliza la creación de una política de replicación como ejemplo.	Política de réplicas
Name	Nombre de política de replicación Un nombre debe contener de 1 a 64 caracteres, incluidos dígitos, letras, guiones bajos (_) o guiones (-).	replication_policy

Parámetro	Descripción	Comentarios
Status	Si se debe habilitar la política de replicación	Solo después de habilitar una política de replicación, CBR replicará automáticamente las copias de respaldo en los almacenes asociados a la política y eliminará las copias de respaldo caducadas.
Execution Time	Tiempos de ejecución de la política de replicación en un día Las tareas de replicación se pueden programar al principio de cada hora. Se admiten varias selecciones.	00:00, 02:00 Se recomienda que la replicación se realice durante las horas no pico o cuando no hay servicios en ejecución.
Replication Frequency	Fechas de ejecución de la tarea de replicación <ul style="list-style-type: none"> ● Weekly Especifica en qué días de cada semana se ejecutará la tarea de replicación. Puede seleccionar varios días. ● Day based Especifica el intervalo (cada 1 a 30 días) para ejecutar la tarea de replicación. 	Todos los días Si selecciona replicación basada en días, se supone que la primera hora de replicación será el día en que se crea la política de replicación. Si el tiempo de creación de la política de replicación es posterior al tiempo de ejecución más reciente, la replicación inicial se realizará en el siguiente ciclo de replicación.

Parámetro	Descripción	Comentarios
Retention Rule	<p>Reglas de retención de réplicas generadas en la región de destino</p> <ul style="list-style-type: none"> ● Replica quantity Especifica el número máximo de réplicas permitidas para un único servidor en la nube. El valor oscila entre 2 y 99999. También puede establecer reglas de retención a largo plazo con opciones avanzadas. Las reglas de retención a largo plazo y las reglas de retención basadas en cantidades no entran en conflicto. Ambos serán aplicados. <ul style="list-style-type: none"> – Day-based: el valor varía de 0 a 100. – Weekly: El valor varía de 0 a 100. – Monthly: El valor varía de 0 a 100. – Yearly: El valor varía de 0 a 100. <p>Por ejemplo, la opción avanzada basada en el día conserva la última réplica de copias de respaldo por día. Aunque la copia de respaldo se replica varias veces al día, solo se conserva la última réplica del día actual. Si establece el valor en 5, el sistema conserva la réplica más reciente de cada uno de los últimos cinco días que han generado réplicas de copia de respaldo. Si hay más de cinco réplicas de copia de respaldo, el sistema elimina automáticamente las réplicas de copias de respaldo más tempranas. Si se configuran todas las opciones avanzadas diarias, semanales, mensuales y anuales, se seleccionan las réplicas de copias de respaldo de unión para retención. Por ejemplo, si el número de réplicas de copias de respaldo basadas en días retenidas se establece en 5 y el número de réplicas de copias de respaldo semanales retenidas se establece en 1, se conservarán cinco réplicas de copias de respaldo. La regla de retención a largo plazo y la regla de retención basada en cantidades pueden ser efectivas al mismo tiempo.</p> <ul style="list-style-type: none"> ● Time period Puede optar por conservar las réplicas durante un mes, tres meses, seis meses, un año o por cualquier número deseado (2 a 99999) de días. 	6 meses

Parámetro	Descripción	Comentarios
	<ul style="list-style-type: none"> ● Permanent <p>NOTA</p> <ul style="list-style-type: none"> - Cuando el número de réplicas de copias de respaldo retenidas excede el valor preestablecido, el sistema elimina automáticamente las réplicas más antiguas. Cuando los períodos de retención de las réplicas retenidas exceden el valor preestablecido, el sistema elimina automáticamente todas las réplicas caducadas. De forma predeterminada, el sistema borra automáticamente los datos cada dos días. - Hay un retraso en la eliminación de réplicas de copias de respaldo caducadas, pero normalmente este retraso no será de más de 24 horas. - Este parámetro sólo se aplica a réplicas generadas en función de una política de replicación programada. Estas réplicas creadas manualmente no se verán afectadas por este parámetro y no se eliminarán automáticamente. Puede eliminarlos manualmente de la lista de copia de respaldo. - Una vez que se utiliza una réplica para crear una imagen o un sistema de archivos, la réplica no se contará como una copia de respaldo retenida y no se eliminará automáticamente. 	
Destination Region	<p>Región en la que se replica el copias de respaldo</p> <p>Sólo se mostrarán las regiones que admitan replicación.</p> <ul style="list-style-type: none"> ● Si la región seleccionada contiene sólo un proyecto, puede seleccionar directamente el nombre de la región. ● Si la región seleccionada tiene varios proyectos, el proyecto maestro de la región se selecciona de forma predeterminada. Puede seleccionar otro proyecto si es necesario. 	AP-Bangkok
Enable Acceleration	<p>Si se debe acelerar la replicación</p> <p>La función de aceleración se factura por el tráfico.</p>	-

Paso 4 Haga clic en **Create Now**.

Paso 5 Busque el almacén deseado y elija **More > Apply Replication Policy** para aplicar la política de replicación creada al almacén. Puede ver la política de replicación aplicada en la página de detalles del almacén.

Una vez que la configuración se realiza correctamente, las copias de respaldo se replican periódicamente en el almacén de destino según la política de replicación.

----Fin

Ejemplo

Un usuario aplica una política de replicación a un almacén a las 11:00 a.m. el jueves en una región determinada. De acuerdo con la política, las copias de respaldo se replicarán en la región de destino a las 02:00 a.m. todos los días, y se conservarán dos réplicas de copias de respaldo. Este almacén también tiene una política de copia de respaldo aplicada, que crea automáticamente dos copias de respaldo a las 00:00 todos los días. A las 12:00 p.m. el sábado, el almacén de replicación contendrá dos réplicas de copias de respaldo, que se replican el sábado. Réplicas de copias de respaldo generadas a las 02:00 a.m. el viernes se han eliminado automáticamente de acuerdo con la política de replicación.

4.3 Modificación de una política

En esta sección se describe cómo modificar una política.

Prerrequisitos

Ha creado al menos una política.

Procedimiento

Paso 1 Inicie sesión en la consola de CBR.

1. **Inicie sesión en la consola de gestión.**
2. Haga clic en  en la esquina superior izquierda y seleccione su región y proyecto.
3. Elija **Storage > Cloud Backup and Recovery**. Elija el tipo de copia de respaldo deseado en el panel de navegación izquierdo.

Paso 2 En cualquier página de copia de respaldo, busque el almacén de destino y haga clic en el nombre del almacén para ver los detalles del almacén.

Paso 3 En el área **Políticas**, haga clic en **Edit** en la fila de una política para abrir la página de edición de políticas. Consulte [Figura 4-3](#).

Figura 4-3 Edición de una política de copia de respaldo

×

Edit Policy

Basic Information

Name

Status Enabled Disabled

Backup Rule

Current rule: Automatically perform backups at 00:00,02:00 every 1 days.

Backup Frequency Weekly Day based

Automatically perform backups every days.

Execution Time Select All Invert Selection

<input checked="" type="checkbox"/> 00:00	<input type="checkbox"/> 01:00	<input checked="" type="checkbox"/> 02:00	<input type="checkbox"/> 03:00	<input type="checkbox"/> 04:00
<input type="checkbox"/> 05:00	<input type="checkbox"/> 06:00	<input type="checkbox"/> 07:00	<input type="checkbox"/> 08:00	<input type="checkbox"/> 09:00
<input type="checkbox"/> 10:00	<input type="checkbox"/> 11:00	<input type="checkbox"/> 12:00	<input type="checkbox"/> 13:00	<input type="checkbox"/> 14:00
<input type="checkbox"/> 15:00	<input type="checkbox"/> 16:00	<input type="checkbox"/> 17:00	<input type="checkbox"/> 18:00	<input type="checkbox"/> 19:00
<input type="checkbox"/> 20:00	<input type="checkbox"/> 21:00	<input type="checkbox"/> 22:00	<input type="checkbox"/> 23:00	

Retention Rule

Current rule: Keep backups from the last 6 months.

Type Backup quantity Time period Permanent

Create Now Cancel

Los parámetros relacionados se describen en [Tabla 4-1](#) y [Tabla 4-2](#).

Paso 4 Haga clic en **OK**.

Si se modifica la regla de retención de políticas, la nueva regla entrará en vigor según cómo la haya cambiado. Para obtener más información, consulte [¿Por qué la regla de retención no tiene efecto después de ser modificada?](#)

Paso 5 También puede seleccionar **Policies** en el árbol de navegación de la izquierda y editar la política deseada.

----Fin

4.4 Eliminación de una política

Puede eliminar las políticas de backup y replicación si es necesario.

Prerrequisitos

Ha creado al menos una política.

Procedimiento

Paso 1 Inicie sesión en la consola de CBR.

1. [Inicie sesión en la consola de gestión](#).
2. Haga clic en  en la esquina superior izquierda y seleccione su región y proyecto.
3. Elija **Storage > Cloud Backup and Recovery**. Elija el tipo de copia de respaldo deseado en el panel de navegación izquierdo.

Paso 2 Haga clic en la pestaña **Backup Policies**, localice la fila que contiene la política que desea eliminar y haga clic en **Delete**.

NOTA

La eliminación de una política no eliminará las copias de seguridad generadas en función de la política. Puede eliminar manualmente copias de respaldo no deseadas.

Paso 3 Confirme la información y haga clic en **Yes**.

----Fin

4.5 Aplicación de una política a un almacén

Una política de copia de respaldo o replicación permite que un almacén ejecute automáticamente tareas de copia de respaldo o replicación en momentos o intervalos especificados. Las copias de respaldo periódicas se pueden utilizar para restaurar los datos rápidamente contra la corrupción o pérdida de datos.

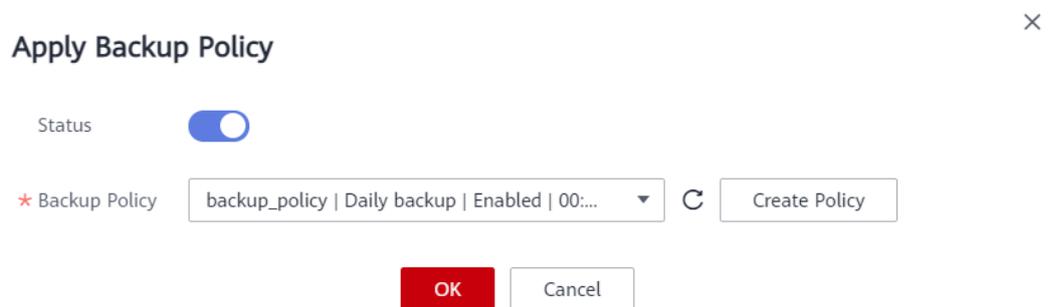
Procedimiento

Paso 1 Inicie sesión en la consola de CBR.

1. [Inicie sesión en la consola de gestión.](#)
2. Haga clic en  en la esquina superior izquierda y seleccione su región y proyecto.
3. Elija **Storage > Cloud Backup and Recovery**. Elija el tipo de copia de respaldo deseado en el panel de navegación izquierdo.

Paso 2 En cualquier página de copia de respaldo, busque el almacén de destino y elija **More > Apply Backup Policy** o **More > Apply Replication Policy**. Consulte [Figura 4-4](#).

Figura 4-4 Configuración de una política de copia de respaldo



Paso 3 Puede seleccionar una política de copia de respaldo existente en la lista desplegable o crear una nueva. Para obtener información sobre cómo crear una política, consulte [Creación de una política de copia de respaldo](#) y [Creación de una política de replicación](#)

Paso 4 Una vez aplicada correctamente la política, puede ver los detalles en el área **Policies** de la página de detalles del almacén.

----Fin

4.6 Eliminación de una política de un almacén

Si ya no necesita copias de seguridad o replicación automáticas para un almacén, elimine la política del almacén.

Prerrequisitos

Se ha aplicado una política al almacén.

Procedimiento

Paso 1 Inicie sesión en la consola de CBR.

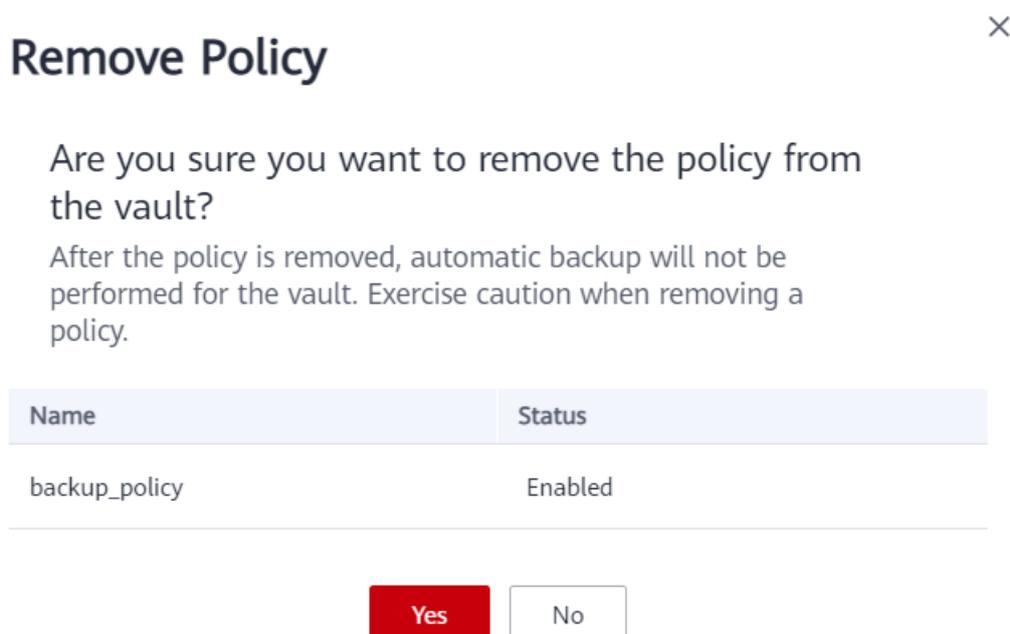
1. [Inicie sesión en la consola de gestión.](#)

2. Haga clic en  en la esquina superior izquierda y seleccione su región y proyecto.
3. Elija **Storage > Cloud Backup and Recovery**. Elija el tipo de copia de respaldo deseado en el panel de navegación izquierdo.

Paso 2 En cualquier página de copia de respaldo, busque el almacén de destino y haga clic en el nombre del almacén para ver los detalles del almacén.

Paso 3 En el área **Policies**, haga clic en **Remove Policy**. Consulte [Figura 4-5](#).

Figura 4-5 Eliminación de una política



 **NOTA**

- Si se está ejecutando una tarea de copia de respaldo para un recurso en el almacén, la política se puede eliminar normalmente. Sin embargo, la tarea de copia de respaldo continuará y se generarán copias de seguridad.
- Después de eliminar una política, las copias de seguridad retenidas por tiempo caducarán según la regla de retención, pero las copias de seguridad retenidas por cantidad no se eliminarán automáticamente. Puede eliminar manualmente las copias de seguridad no deseadas.

Paso 4 Haga clic en **Yes**. El almacén ya no ejecutará las tareas especificadas en esta política.

----Fin

5 Restauración de datos

5.1 Restauración de datos mediante una copia de respaldo de un servidor en la nube

Cuando los discos de un servidor están defectuosos o los datos del servidor se pierden debido a un funcionamiento incorrecto, puede utilizar una copia de respaldo para restaurar el servidor.

Para restaurar datos en otro servidor, consulte [¿Cómo restauro datos en el servidor original a un nuevo servidor?](#)

Contexto

- Los datos de los discos de datos no se pueden restaurar en los discos del sistema.
- Los datos no se pueden restaurar en los servidores en estado **Faulty**.
- No se admite la restauración de datos simultánea.

Prerrequisitos

- Los discos del servidor cuyos datos deben restaurarse se ejecutan correctamente.
- El servidor cuyos datos deben restaurarse tiene al menos una copia de respaldo **Available**.

Procedimiento

Paso 1 Inicie sesión en la consola de CBR.

1. [Inicie sesión en la consola de gestión](#).
2. Haga clic en  en la esquina superior izquierda y seleccione su región y proyecto.
3. Elija **Storage > Cloud Backup and Recovery**. Elija el tipo de copia de respaldo deseado en el panel de navegación izquierdo.

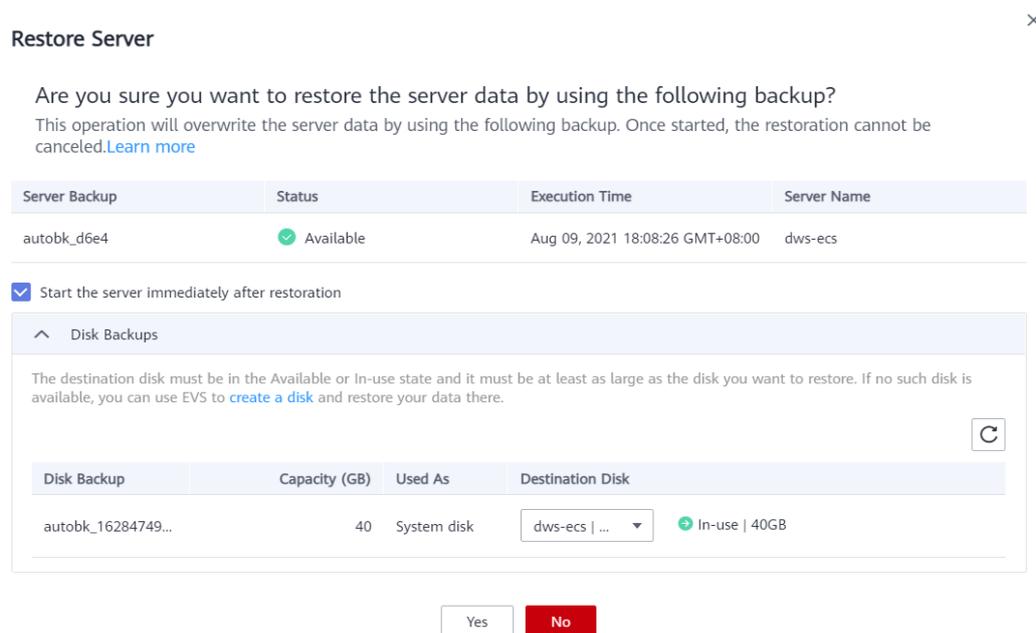
Paso 2 Haga clic en la pestaña **Backups**. Localice la copia de respaldo deseada. Para obtener más información, consulte [Consulta de una copia de respaldo](#).

Paso 3 En la fila de la copia de respaldo, haga clic en **Restore Server**. Consulte **Figura 5-1**.

AVISO

Los datos históricos en el punto de copia de respaldo en el tiempo sobrescribirán los datos actuales del servidor. La restauración no se puede deshacer.

Figura 5-1 Restauración de un servidor



Paso 4 (Opcional) Anule la selección **Start the server immediately after restoration**.

Si anula la selección **Start the server immediately after restoration**, inicie manualmente el servidor una vez completada la restauración.

AVISO

Los servidores se apagan durante la restauración. Por lo tanto, se recomienda que realice operaciones de restauración durante las horas no pico.

Paso 5 En la lista desplegable **Specified Disk**, seleccione el disco de destino en el que se restaurará la copia de respaldo.

 **NOTA**

- Si el servidor solo tiene un disco, la copia de respaldo se restaura en el disco de forma predeterminada.
- Si el servidor tiene varios discos, la copia de respaldo se restaura respectivamente en los discos originales de forma predeterminada. También puede restaurar la copia de respaldo en otro disco en el servidor de copias de seguridad seleccionando el disco en la lista desplegable. Sin embargo, el disco de destino especificado debe ser al menos tan grande como el disco de origen de copia de respaldo.
- Los datos de copia de respaldo de los discos de datos no se pueden restaurar en los discos del sistema.

AVISO

Si el número de discos que se van a restaurar es mayor que el número de discos de los que se realiza una copia de respaldo, la restauración puede provocar incoherencia en los datos.

Por ejemplo, si los datos de Oracle están dispersos en varios discos y sólo algunos de ellos se restauran, la incoherencia de los datos se produce después de la restauración y es posible que la aplicación no pueda iniciarse.

Paso 6 Haga clic en **Yes** y confirme que la restauración se ha realizado correctamente.

En la lista de copia de respaldo, vea el estado de restauración. Cuando la copia de respaldo entra en el estado **Available** y no existen nuevas tareas de restauración con errores en **Tasks**, la restauración se realiza correctamente. El recurso se restaura al estado en el momento en que tomó esa copia de respaldo.

Para obtener más información acerca de cómo ver las tareas de restauración fallidas, consulte [Gestión de tareas](#).

AVISO

Si se restaura un servidor Windows, es posible que los discos de datos no se muestren debido a las limitaciones de Windows.

Después de utilizar una copia de respaldo del servidor en la nube para restaurar un grupo de volúmenes lógicos, el grupo de volúmenes lógicos debe conectarse de nuevo.

Es necesario conectar manualmente estos discos de datos. Para obtener más información, consulte [Los discos de datos no se muestran después de restaurar un servidor de Windows](#).

----Fin

5.2 Restauración de datos mediante una copia de respaldo en disco en la nube

Puede utilizar una copia de respaldo de disco para restaurar un disco a la hora en que se creó la copia de respaldo.

Prerrequisitos

- El estado del disco que se va a restaurar debe ser **Available**.
- Antes de restaurar los datos del disco, detenga el servidor al que está conectado el disco y desconecte el disco del servidor. Después de restaurar los datos del disco, conecte el disco al servidor e inicie el servidor.

Restricciones

- Si se cambia el sistema operativo del servidor después de realizar una copia de respaldo del disco del sistema, la copia de respaldo del disco del sistema no se puede restaurar en el disco del sistema original debido a razones como el cambio del UUID del disco. Puede utilizar la copia de respaldo del disco del sistema para crear un nuevo disco y, a continuación, importar datos al disco original del sistema.
- Las copias de respaldo solo se pueden restaurar en los discos originales. Si desea restaurar una copia de respaldo en un disco distinto al original, utilice directamente la copia de respaldo para crear un nuevo disco.
- Para restaurar la copia de respaldo de un disco de datos en el disco del sistema, consulte [¿Cómo restauro una copia de respaldo de disco de datos en un disco del sistema?](#)
- No se admite la restauración de datos simultánea.

Procedimiento

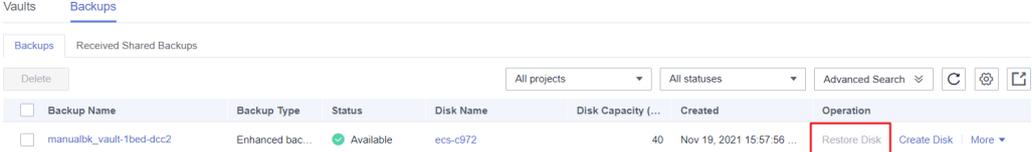
Paso 1 Inicie sesión en la consola de CBR.

1. [Inicie sesión en la consola de gestión](#).
2. Haga clic en  en la esquina superior izquierda y seleccione su región y proyecto.
3. Elija **Storage > Cloud Backup and Recovery**. Elija el tipo de copia de respaldo deseado en el panel de navegación izquierdo.

Paso 2 Haga clic en la pestaña **Backups**. Localice la copia de respaldo deseada. Para más detalles, consulte [Consulta de una copia de respaldo](#).

Paso 3 En la fila de la copia de respaldo, haga clic en **Restore Disk**. Se muestra la página **Restore Disk**. Consulte [Figura 5-3](#).

Figura 5-2 Localización de la copia de respaldo de destino

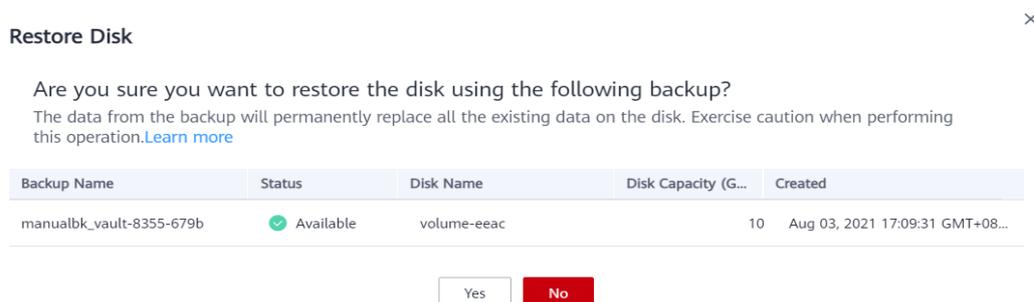


Backup Name	Backup Type	Status	Disk Name	Disk Capacity (...)	Created	Operation
manualbk_vault-1bed-dcc2	Enhanced bac...	Available	ecs-c972	40	Nov 19, 2021 15:57:56 ...	Restore Disk Create Disk More

AVISO

- Los datos de copia de respaldo sobrescribirán los datos actuales del disco y la restauración no se puede deshacer.
- Si el botón de restauración está atenuado, detenga el servidor, desconecte el disco que desea restaurar y, a continuación, restaure los datos. Después de restaurar los datos del disco, conecte el disco al servidor e inicie el servidor.

Figura 5-3 Recuperar Disco



Paso 4 Haga clic en **Yes**. Puede comprobar si los datos se han restaurado correctamente en la página de pestaña **Backups** de **Disk Backups** o en la consola EVS.

Cuando el estado de la copia de respaldo cambia a **Available**, la restauración se realiza correctamente. El recurso se restaura al estado en el momento en que tomó esa copia de respaldo.

Paso 5 Una vez completada la restauración, vuelva a conectar el disco al servidor. Para obtener más información, consulte [Adjuntar un disco no compartido existente](#).

----Fin

5.3 Restauración de datos mediante una copia de respaldo en la nube híbrida

Una vez sincronizadas correctamente las copias de respaldo en un almacén de copia de respaldo en la nube híbrida, puede restaurar los datos de copia de respaldo en servidores en la nube para la recuperación ante desastres, la migración de servicios, el desarrollo y las pruebas.

Restauración de datos mediante una copia de respaldo de VMware

Puede sincronizar las copias de seguridad de las máquinas virtuales de VMware locales en la nube y restaurarlas en servidores en la nube mediante las copias de seguridad. Configure los grupos de seguridad antes de la restauración. De lo contrario, la restauración puede fallar. Para obtener más información, consulte [Restauración en servidores en la nube mediante copias de seguridad de VMware](#).

5.4 Restauración de datos mediante una copia de respaldo de archivos

Puede utilizar una copia de respaldo de archivos para restaurar los datos de un cliente de copia de respaldo al estado en un momento dado cuando se realizó la copia de respaldo de los datos.

Restricciones

- El estado del Agente del cliente de copia de respaldo debe ser **Normal**.
- Se recomienda no restaurar copias de respaldo de archivos en aplicaciones en ejecución. Detenga las aplicaciones y luego restaure los archivos.

Método 1

Paso 1 Inicie sesión en la consola CBR.

1. Inicie sesión en la consola de gestión.
2. Haga clic en  en la esquina superior izquierda y seleccione su región y proyecto.
3. Elija **Storage > Cloud Backup and Recovery > File Backups**.

Paso 2 En la página de la pestaña **File Backup**, haga clic en el nombre del cliente de copia de respaldo de destino.

Paso 3 Encuentre la copia de respaldo deseada y haga clic en **Restore Data**.

Figura 5-4 Restauración de un archivo

Restore Data ×

Restore Time: Apr 11, 2022 15:41:47 GMT+08:00

Restore To: New location Current location

Target Client:

Storage Path:

During the recovery, any file with the same name will be overwritten.

Paso 4 Seleccione una ubicación de restauración.

- **Current location:** Los datos se restaurarán a la ruta original del archivo en el cliente de copia de respaldo actual, y cualquier archivo con el mismo nombre se sobrescribirá. Esta opción solo está disponible para clientes de copia de respaldo de Linux.
- **New location:** Los datos se restaurarán en un servidor diferente. Puede seleccionar un cliente de destino y especificar una ruta.
Solo puede elegir entre los clientes de copia de respaldo cuyo estado de Agente es **Normal**. Si el servidor de destino no está en la lista, vaya a la lista de copia de respaldo de archivos e instale el agente.

Paso 5 Haga clic en **OK**. Puede comprobar si los datos se restauran correctamente en el área **Backup Details** de la página de detalles del cliente o en el host local.

Cuando el estado de la copia de respaldo cambia a **Available**, la restauración se realiza correctamente.

----Fin

Método 2

Paso 1 Inicie sesión en la consola CBR.

1. Inicie sesión en la consola de gestión.
2. Haga clic en  en la esquina superior izquierda y seleccione su región y proyecto.
3. Elija **Storage > Cloud Backup and Recovery > File Backups**.

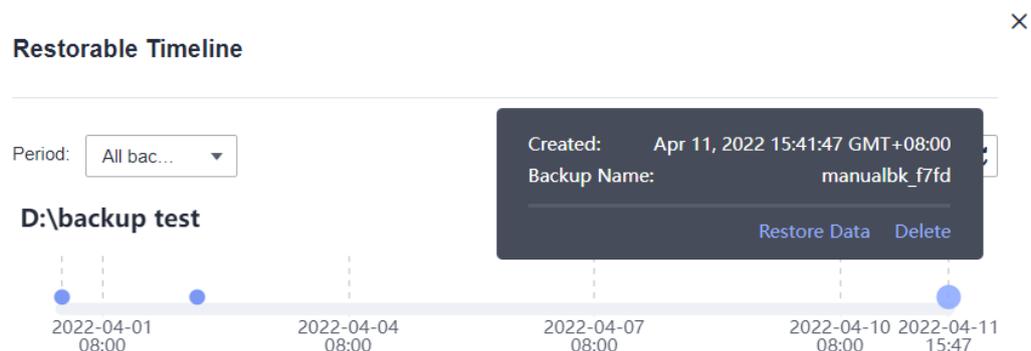
Paso 2 En la página de la pestaña **File Backup**, haga clic en el nombre del cliente de copia de respaldo de destino.

Paso 3 Haga clic en **Restorable Timeline** en la columna **Operation**.

Paso 4 Seleccione un tiempo de restauración y haga clic en **Restore Data**. Consulte [Figura 5-5](#).

El sistema restaurará los datos al estado en el momento seleccionado.

Figura 5-5 Línea de tiempo restaurable



Paso 5 Seleccione una ubicación de restauración.

- **Current location:** Los datos se restaurarán a la ruta original del archivo en el cliente de copia de respaldo actual, y cualquier archivo con el mismo nombre se sobrescribirá.
- **New location:** Los datos se restaurarán en un servidor diferente. Puede seleccionar un cliente de destino y especificar una ruta.

Solo puede elegir entre los clientes de copia de respaldo cuyo estado de Agente es **Normal**. Si el servidor de destino no está en la lista, vaya a la lista de copia de respaldo de archivos e instale el agente.

Paso 6 Haga clic en **OK**. Puede comprobar si los datos se restauran correctamente en el área **Backup Details** de la página de detalles del cliente o en el host local.

Cuando el estado de la copia de respaldo cambia a **Available**, la restauración se realiza correctamente.

---**Fin**

6 Copias de respaldo consistentes con la aplicación

6.1 ¿Qué es la copia de respaldo consistente con las aplicaciones?

Descripción

Hay tres tipos de copia de respaldo en términos de consistencia de copia de respaldo:

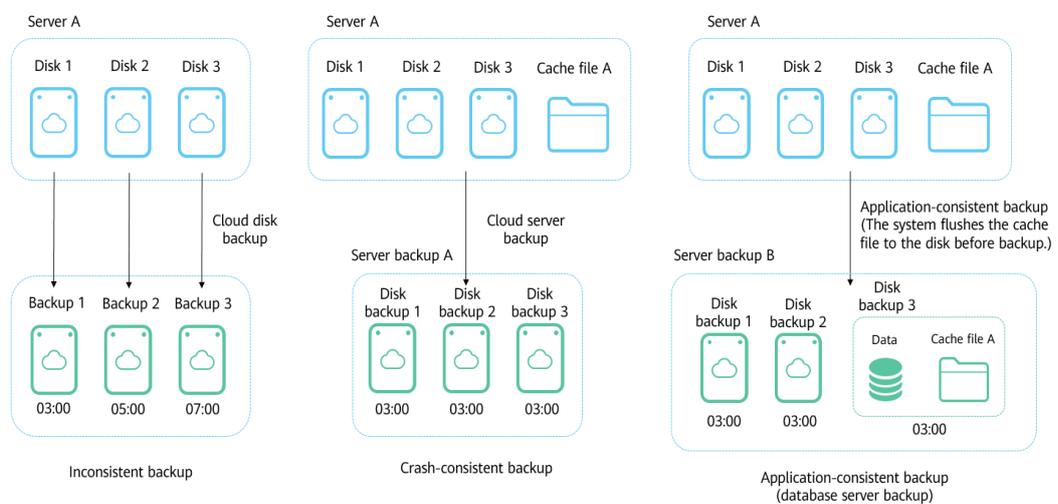
- **Copia de respaldo inconsistente:** Los archivos de una copia de respaldo inconsistente contienen datos tomados de diferentes momentos en el tiempo. Esto ocurre normalmente si se realizan cambios en los archivos o en los datos de los discos mientras se ejecuta la copia de respaldo. La copia de respaldo del servidor en la nube CBR utiliza la tecnología de instantáneas de consistencia para los discos para proteger los datos de ECS y BMS. Si realiza una copia de respaldo de varios discos EVS por separado, los puntos de tiempo de copia de respaldo de los discos EVS son diferentes. Como resultado, los datos de copia de respaldo de los discos EVS son inconsistentes.
- **Copia de respaldo consistente en bloqueos:** Una copia de respaldo consistente en bloqueos captura los datos que existen en los discos a partir del tiempo de copia de respaldo, sin hacer copias de respaldo de los datos de la memoria ni de los sistemas de aplicación inactivos. No se garantiza la consistencia de las copias de respaldo de los sistemas de aplicación. Para completar esto, los discos se comprueban al reiniciar el sistema operativo para restaurar los datos dañados, por ejemplo, mediante el uso de **chkdsk**, y la reversión de registros se realiza en las bases de datos para mantener la coherencia de los datos.
- **Copia de respaldo consistente con las aplicaciones:** Una copia de respaldo consistente con las aplicaciones es una copia de respaldo de los datos de las aplicaciones que permite a las aplicaciones alcanzar un estado inactivo y consistente. Este tipo de copia de respaldo captura el contenido de la memoria y cualquier escritura pendiente que ocurriera durante el proceso de copia de respaldo.

Figura 6-1 compara estos tipos de copia de respaldo en detalle.

CBR admite tanto copias de seguridad consistentes en bloqueos como copias de seguridad consistentes en aplicaciones (también denominadas copias de seguridad del servidor de base de datos).

Si se implementa una base de datos MySQL o SAP HANA en un servidor, puede usar el backup CBR coherente con la aplicación para realizar copias de seguridad de los datos del servidor y la caché de la aplicación. La copia de respaldo consistente en bloqueos solo realiza copias de seguridad de datos y algunas cachés de aplicaciones sin interrumpir los servicios. Si un sistema falla o se produce una pérdida de datos, puede utilizar una copia de respaldo compatible con las aplicaciones para reiniciar rápidamente los servicios. Sin embargo, una copia de respaldo consistente en bloqueos puede fallar al restaurar algunas configuraciones de aplicaciones.

Figura 6-1 Consistencia de copia de respaldo



Diferencias entre copias de seguridad consistentes con las aplicaciones, copias de seguridad de servidores en la nube

Artículo	Copias de respaldo consistentes con la aplicación	Copia de respaldo de servidor en la nube
Copia de respaldo y restauración de objetos	Servidores en la nube con bases de datos MySQL o SAP HANA implementadas	Servidores en la nube excluyendo las aplicaciones de base de datos
Unidad de copia de respaldo	Servidor en la nube	Servidor en la nube
Tipo de almacén	Almacén de respaldo de servidor	Almacén de respaldo de servidor

Artículo	Copias de respaldo consistentes con la aplicación	Copia de respaldo de servidor en la nube
Escenario recomendado	Los datos de los servidores en la nube, así como sus bases de datos implementadas, como MySQL o SAP HANA, necesitan ser respaldados. Todas las configuraciones de datos y aplicaciones necesitan ser restauradas en caso de un error.	Solo es necesario realizar una copia de respaldo de los datos de los servidores en la nube. Todos los datos necesitan ser restaurados en caso de un error. En el caso de que se realice una copia de respaldo del servidor en la nube para un servidor implementado con una base de datos MySQL o SAP HANA, si la copia de respaldo se usa para restaurar datos, algunas configuraciones de base de datos pueden fallar al restaurarse y pueden producirse problemas después de reiniciar la base de datos.

Ámbito de aplicación

Tabla 6-1 enumera los sistemas operativos que admiten la instalación del agente.

Tabla 6-1 Sistemas operativos que admiten la instalación del agente

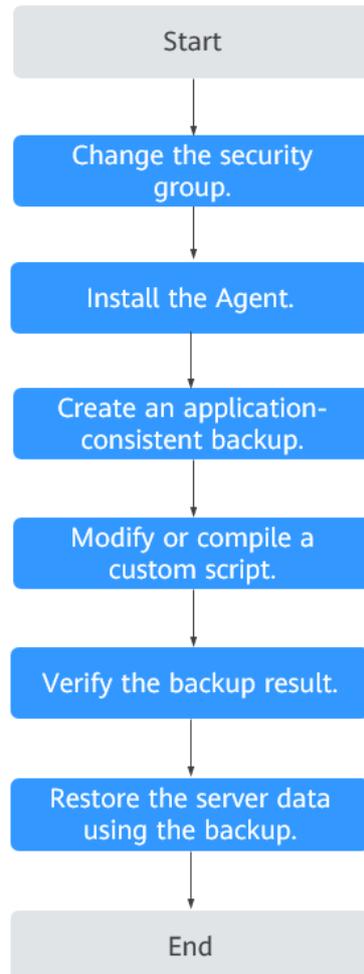
Base de datos	OS	Versión
SQL Server 2008/2012	Windows	Windows Server 2008, 2008 R2, 2012 y 2012 R2 for x86_64
SQL Server 2014/2016/EE	Windows	Windows Server 2014, 2014 R2 y 2016 Datacenter for x86_64
MySQL 5.5/5.6/5.7	Red Hat	Red Hat Enterprise Linux 6 y 7 for x86_64
	SUSE	SUSE Linux Enterprise Server 11, 12, 15 SP1, 15 SP2 for x86_64
	CentOS	CentOS 6 y 7 for x86_64
	EulerOS	EulerOS 2.2 y 2.3 for x86_64
HANA 1.0/2.0	SUSE	SUSE Linux Enterprise Server 12 for x86_64

Para las bases de datos no incluidas en esta lista, puede personalizar un script para realizar copias de seguridad compatibles con las aplicaciones consultando la sección "Uso de un script personalizado para implementar copias de seguridad compatibles con las aplicaciones" en *Prácticas recomendadas de Cloud Backup and Recovery*.

Proceso

Figura 6-2 muestra el proceso de copia de respaldo coherente con la aplicación.

Figura 6-2 Proceso de copia de respaldo consistente con las aplicaciones



- Paso 1** Cambiar el grupo de seguridad: Antes de realizar una tarea de copia de respaldo compatible con la aplicación, cambie el grupo de seguridad del servidor del que desea realizar una copia de respaldo. Para más detalles, consulte [Cambio de un grupo de seguridad](#).
- Paso 2** Instalar el agente: Cambie el grupo de seguridad e instale el agente en cualquier secuencia. Asegúrese de que las dos operaciones se hayan completado antes de realizar una copia de respaldo del servidor deseado. Para más detalles, consulte [Instalación del agente](#).
- Paso 3** Crear una copia de respaldo compatible con la aplicación: Después de crear un almacén de copias de seguridad del servidor para almacenar copias de seguridad compatibles con la aplicación, asócielo con el servidor de base de datos deseado y, a continuación, cree una copia de respaldo compatible con la aplicación. Para más detalles, consulte [Creación de una copia de respaldo consistente con las aplicaciones](#).
- Paso 4** Modificar o compilar un script personalizado: Después de realizar una copia de respaldo de un servidor de base de datos en la consola CBR, modificar o compilar un script personalizado en la base de datos del servidor. Para obtener más información, consulte [Uso de un script personalizado para implementar copias de seguridad consistente con las aplicaciones](#).

- Paso 5** Verificar el resultado de la copia de respaldo: Después de realizar la copia de respaldo, verifique que la copia de respaldo se realice correctamente. Para obtener más información, consulte [Verificación del resultado de copia de respaldo consistente con la aplicación](#).
- Paso 6** Utilice la copia de respaldo para restaurar los datos del servidor: utilice la copia de respaldo compatible con la aplicación para restaurar los datos del servidor. Las aplicaciones y los datos de base de datos restaurados son los mismos que en el momento de la copia de respaldo. Para más detalles, consulte [Restauración de datos mediante una copia de respaldo de un servidor en la nube](#).
- Fin

6.2 Cambio de un grupo de seguridad

Contexto

Un grupo de seguridad es un conjunto de reglas de control de acceso para los ECS que tengan los mismos requisitos de protección de seguridad y que sean de confianza recíproca en una VPC. Después de crear un grupo de seguridad, se pueden crear diferentes reglas de acceso para que el grupo de seguridad proteja los ECS que se agreguen a este grupo de seguridad. La regla predeterminada del grupo de seguridad permite todos los paquetes de datos salientes. Los ECS de un grupo de seguridad tienen acceso recíproco sin necesidad de agregar reglas. El sistema crea un grupo de seguridad para cada cuenta en la nube de forma predeterminada. También puede crear grupos de seguridad personalizados por sí mismo.

Al crear un grupo de seguridad, debe agregar las reglas de acceso entrante y saliente y habilitar los puertos necesarios para la copia de respaldo compatible con las aplicaciones para evitar errores de copia de respaldo compatibles con las aplicaciones.

Instrucciones de operación

Antes de utilizar la función de copia de respaldo compatible con la aplicación, debe cambiar el grupo de seguridad. Para garantizar la seguridad de la red, CBR no ha establecido la dirección de entrada de un grupo de seguridad, por lo que debe configurarlo manualmente.

En la dirección de salida del grupo de seguridad, se deben configurar los puertos 1 a 65535 en el segmento de red 100.125.0.0/16. En la dirección de entrada, se deben configurar los puertos 59526 a 59528 en el segmento de red 100.125.0.0/16. La regla de salida predeterminada es 0.0.0.0/0, es decir, todos los paquetes de datos están permitidos. Si la regla predeterminada en la dirección de salida no se modifica, no es necesario configurar la dirección de salida.

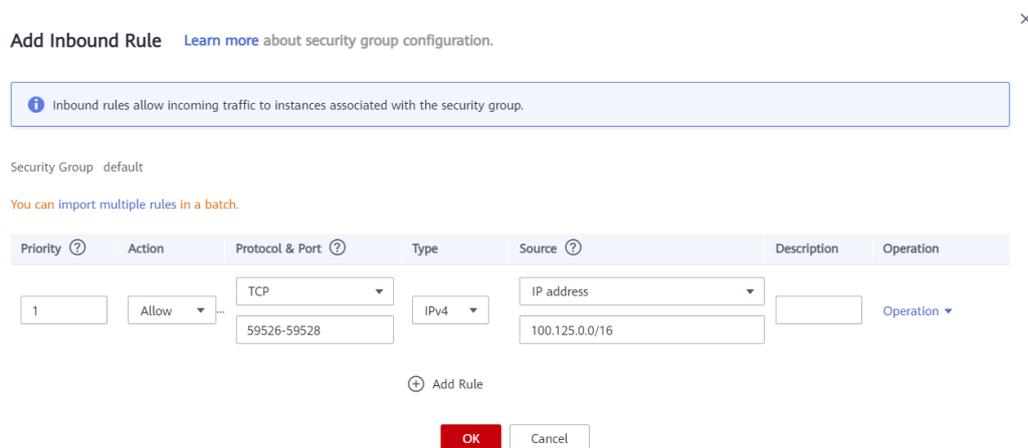
Procedimiento

- Paso 1** Inicie sesión en la consola de ECS.
1. Inicie sesión en la consola de gestión.
 2. Haga clic en  en la esquina superior izquierda y seleccione su región y proyecto.
 3. En **Computing**, haga clic en **Elastic Cloud Server**.
- Paso 2** En el panel de navegación de la izquierda, elija **Elastic Cloud Server** or **Bare Metal Server**. En la página mostrada, seleccione el servidor de destino. Vaya a la página de detalles del servidor.

Paso 3 Haga clic en la pestaña **Security Groups** y seleccione el grupo de seguridad de destino. A la derecha de la página ECS, haga clic en **Modify Security Group Rule** para un ECS. Haga clic en **Change Security Group** para un BMS. En el cuadro de diálogo mostrado, haga clic en **Manage Security Group**.

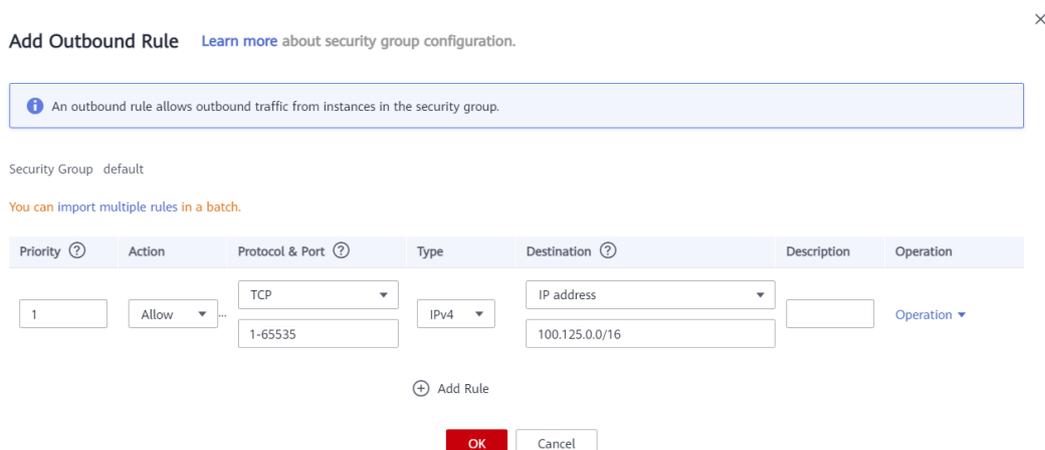
Paso 4 En la página **Security Groups**, haga clic en la pestaña **Inbound Rules** y, a continuación, haga clic en **Add Rule**. Se muestra el cuadro de diálogo **Add Inbound Rule**, como se muestra en **Figura 6-3**. Seleccione **TCP** para **Protocol/Application**, escriba **59526-59528** en **Port & Source**, seleccione **IP address** para **Source** e introduzca **100.125.0.0/16**. Después de completar la descripción, haga clic en **OK** para completar la configuración de la regla de entrada.

Figura 6-3 Adición de una regla de entrada



Paso 5 Haga clic en la pestaña **Outbound Rules** y, a continuación, haga clic en **Add Rule**. Se muestra el cuadro de diálogo **Add Outbound Rule**, como se muestra en **Figura 6-4**. Seleccione **TCP** para **Protocol/Application**, escriba **1-65535** en **Port & Source**, seleccione **IP address** para **Destination** e introduzca **100.125.0.0/16**. Después de completar la descripción, haga clic en **OK** para completar la configuración de la regla de salida.

Figura 6-4 Adición de una regla saliente



----Fin

6.3 Instalación del agente

Antes de habilitar la copia de respaldo compatible con las aplicaciones, cambie el grupo de seguridad e instale correctamente el agente en sus ECS.

Si la copia de respaldo compatible con la aplicación está habilitada pero el Agente no está instalado en los servidores, la copia de respaldo compatible con la aplicación fallará y en su lugar se realizará una copia de respaldo del servidor común. Para asegurarse de que la copia de respaldo consistente con la aplicación se ejecuta correctamente, descargue e instale primero el agente.

Instrucciones de operación

- El backup compatible con las aplicaciones solo admite ECS basados en x86, no ECS basados en Kunpeng.
- Durante la instalación del agente, el sistema requiere los permisos del usuario **rdadmin** para ejecutar el programa de instalación. Para mejorar la seguridad de O&M, cambie la contraseña del usuario **rdadmin** del Agente OS regularmente y deshabilite el permiso de inicio de sesión remoto de este usuario. Para más detalles, consulte [Cambiar la contraseña del usuario rdadmin](#).
- [Tabla 6-2](#) enumera los sistemas operativos que admiten la instalación del agente.

Tabla 6-2 Sistemas operativos que admiten la instalación del agente

Base de datos	OS	Versión
SQL Server 2008/2012	Windows	Windows Server 2008, 2008 R2, 2012 y 2012 R2 for x86_64
SQL Server 2014/2016/EE	Windows	Windows Server 2014, 2014 R2 y 2016 Datacenter for x86_64
MySQL 5.5/5.6/5.7	Red Hat	Red Hat Enterprise Linux 6 y 7 for x86_64
	SUSE	SUSE Linux Enterprise Server 11, 12, 15 SP1, 15 SP2 for x86_64
	CentOS	CentOS 6 y 7 for x86_64
	EulerOS	EulerOS 2.2 y 2.3 for x86_64
HANA 1.0/2.0	SUSE	SUSE Linux Enterprise Server 12 for x86_64

AVISO

Para instalar el Agente, el sistema abrirá el firewall de un puerto de 59526 a 59528 del ECS. Cuando el puerto 59526 está ocupado, el firewall del puerto 59527 está habilitado, y así sucesivamente.

Prerrequisitos

- Ha obtenido un nombre de usuario y su contraseña para iniciar sesión en la consola de gestión.
- Se ha configurado el grupo de seguridad.
- El **Agent Status** del ECS es **Not installed**.
- Si utiliza Internet Explorer, debe agregar los sitios web que utilizará a sitios de confianza.

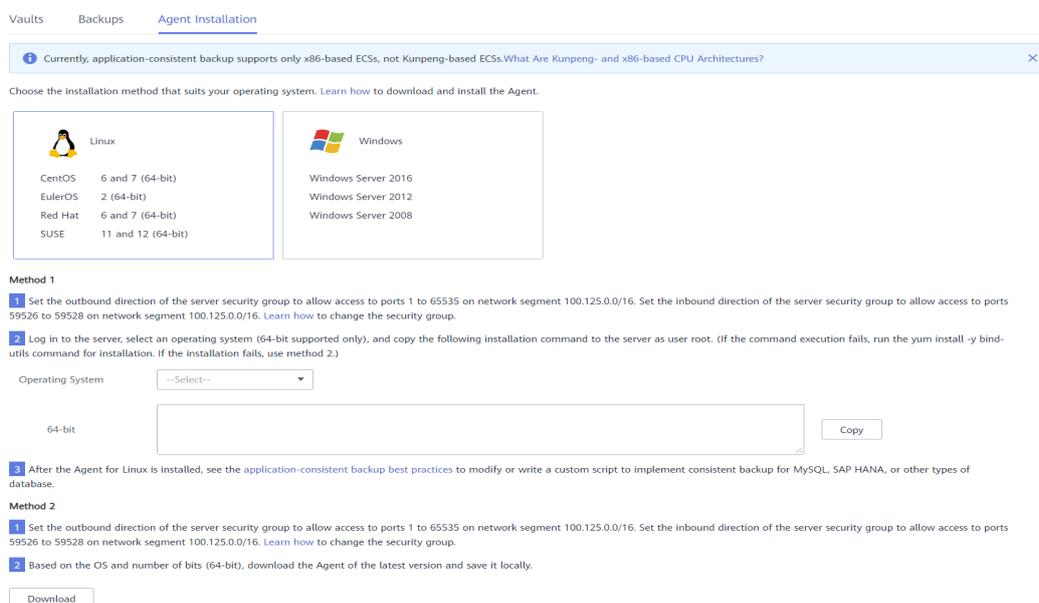
Instalación del agente para un sistema operativo Linux (método 1)

Paso 1 Inicie sesión en la consola de CBR.

1. [Inicie sesión en la consola de gestión.](#)
2. Haga clic en  en la esquina superior izquierda y seleccione su región y proyecto.
3. Elija **Storage > Cloud Backup and Recovery**. Elija el tipo de copia de respaldo deseado en el panel de navegación izquierdo.

Paso 2 Haga clic en la pestaña **Agent Installation**.

Figura 6-5 Página de instalación para Linux



Paso 3 En el método 1, seleccione la versión del agente correspondiente según sea necesario y copie el comando de instalación en el paso 2.

Paso 4 En la página ECS, seleccione el servidor de destino y haga clic en **Remote Login** en la columna **Operation** para iniciar sesión en ECS.

Paso 5 Pegue el comando de instalación en el paso 2 en el servidor y ejecute el comando como usuario **root**. Si la ejecución falla, ejecute el comando **yum install -y bind-utils** para instalar el módulo dig. Si la instalación sigue fallando, utilice el método 2 para instalar el agente para un sistema operativo Linux.

Paso 6 Una vez completada la instalación, el Agente se está ejecutando correctamente. Para implementar copias de seguridad coherentes con las aplicaciones para MySQL, SAP HANA u otros tipos de bases de datos, modifique o compile un script personalizado consultando *Prácticas recomendadas de Cloud Backup and Recovery*.

----Fin

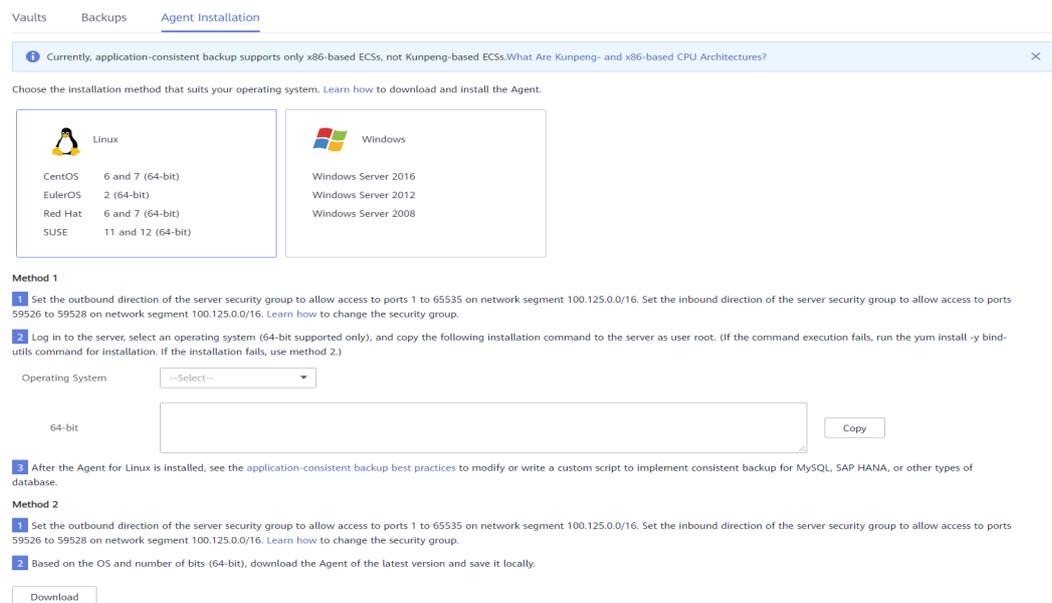
Instalación del agente para un sistema operativo Linux (Método 2)

Paso 1 Inicie sesión en la consola de CBR.

1. [Inicie sesión en la consola de gestión](#).
2. Haga clic en  en la esquina superior izquierda y seleccione su región y proyecto.
3. Elija **Storage > Cloud Backup and Recovery**. Elija el tipo de copia de respaldo deseado en el panel de navegación izquierdo.

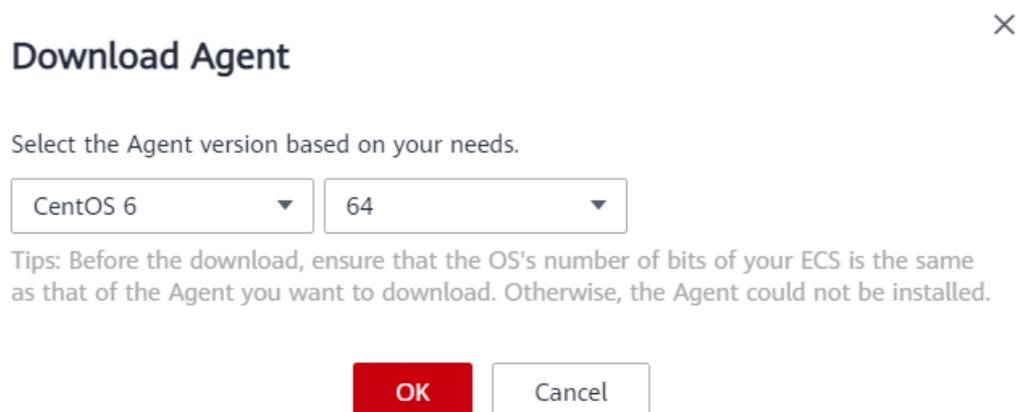
Paso 2 Haga clic en la pestaña **Agent Installation**.

Figura 6-6 Página de instalación para Linux



Paso 3 En el método 2, haga clic en **Download**. En el cuadro de diálogo del cliente de descarga que se muestra, seleccione la versión que se va a descargar en función del tipo de sistema operativo del ECS de destino y haga clic en **OK**. Consulte [Figura 6-7](#).

Figura 6-7 Descarga del agente



- Paso 4** Después de descargar el Agente, utilice una herramienta de transferencia de archivos, como Xftp, SecureFX o WinSCP, para cargar el paquete de instalación del Agente en su ECS.
- Paso 5** Después de la carga, vaya a la página de ECS. Seleccione el servidor de destino y haga clic en **Remote Login** en la columna **Operation** para iniciar sesión en el ECS.
- Paso 6** Ejecute el comando **tar -zxvf** para descomprimir el paquete de instalación del Agente en cualquier directorio y ejecute el siguiente comando para ir al directorio **bin**:

cd bin

- Paso 7** Ejecute el siguiente comando para ejecutar el script de instalación:

sh agent_install_ebk.sh

- Paso 8** El sistema muestra un mensaje que indica que el cliente se ha instalado correctamente. Consulte [Figura 6-8](#).

Figura 6-8 Instalación exitosa del cliente para Linux



- Paso 9** Si la base de datos MySQL o SAP HANA se ha instalado en el ECS, ejecute el siguiente comando para cifrar la contraseña para iniciar sesión en la base de datos MySQL o SAP HANA:

/home/rdadmin/Agent/bin/agentcli encpwd

- Paso 10** Utilice la contraseña cifrada en el [paso anterior](#) para reemplazar la contraseña de inicio de sesión de la base de datos en el script en **/home/rdadmin/Agent/bin/thirdparty/ebk_user/**.
- Paso 11** Una vez completada la instalación, el Agente se está ejecutando correctamente. Para implementar copias de seguridad coherentes con las aplicaciones para MySQL, SAP HANA u

otros tipos de bases de datos, modifique o compile un script personalizado consultando *Prácticas recomendadas de Cloud Backup and Recovery*.

----Fin

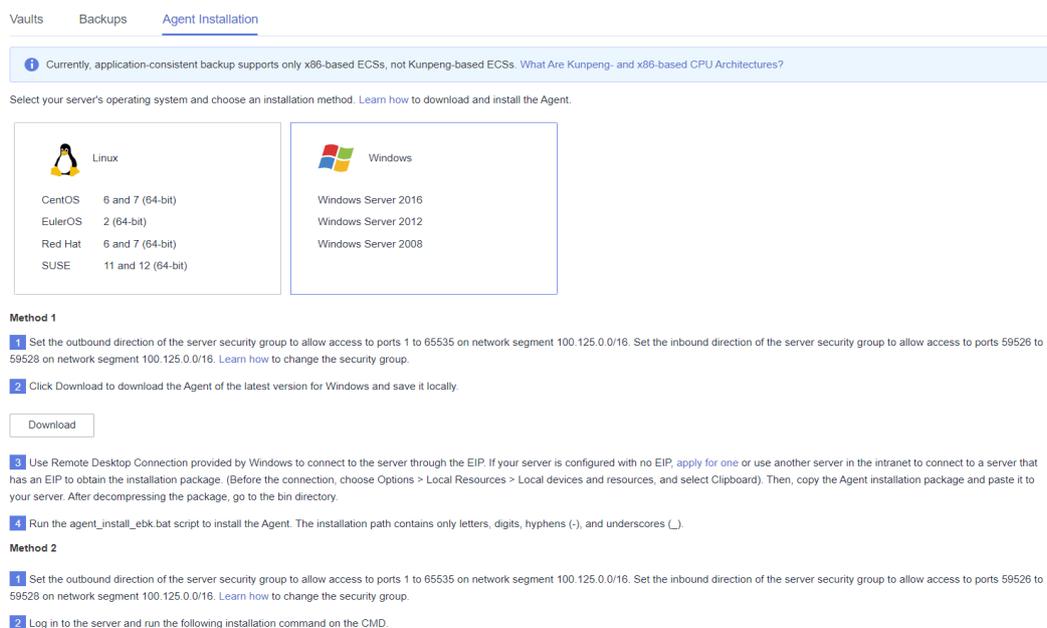
Instalación del agente para un sistema operativo Windows (Método 1)

Paso 1 Inicie sesión en la consola de CBR.

1. **Inicie sesión en la consola de gestión.**
2. Haga clic en  en la esquina superior izquierda y seleccione su región y proyecto.
3. Elija **Storage > Cloud Backup and Recovery**. Elija el tipo de copia de respaldo deseado en el panel de navegación izquierdo.

Paso 2 Haga clic en la pestaña **Agent Installation**.

Figura 6-9 Página de instalación para Windows



Paso 3 En el método 1, haga clic en **Download**. Guarde el paquete de instalación descargado en un directorio local.

Paso 4 Después de descargar el Agente, utilice una herramienta de transferencia de archivos, como Xftp, SecureFX o WinSCP, para cargar el paquete de instalación del Agente en su ECS.

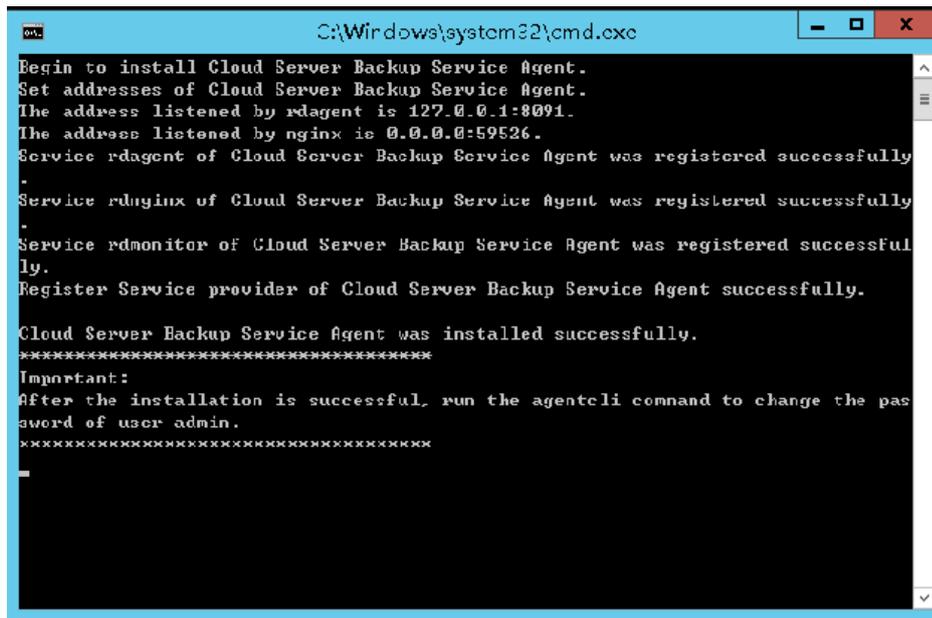
Paso 5 Inicie sesión en la consola y, a continuación, inicie sesión en ECS como administrador.

Paso 6 Descomprima el paquete de instalación en cualquier directorio y vaya al *Installation path\bin*.

Paso 7 Haga doble clic en el script **agent_install_ebk.bat** para iniciar la instalación.

Paso 8 El sistema muestra un mensaje que indica que el cliente se ha instalado correctamente. Consulte **Figura 6-10**.

Figura 6-10 Instalación exitosa del cliente para Windows



```
C:\Windows\system32\cmd.exe
Begin to install Cloud Server Backup Service Agent.
Set addresses of Cloud Server Backup Service Agent.
The address listened by rdagent is 127.0.0.1:8091.
The address listened by nginx is 0.0.0.0:59526.
Service rdagent of Cloud Server Backup Service Agent was registered successfully.
Service rdnginx of Cloud Server Backup Service Agent was registered successfully.
Service rdmonitor of Cloud Server Backup Service Agent was registered successfully.
Register Service provider of Cloud Server Backup Service Agent successfully.
Cloud Server Backup Service Agent was installed successfully.
*****
Important:
After the installation is successful, run the agentcli command to change the password of user admin.
*****
```

----Fin

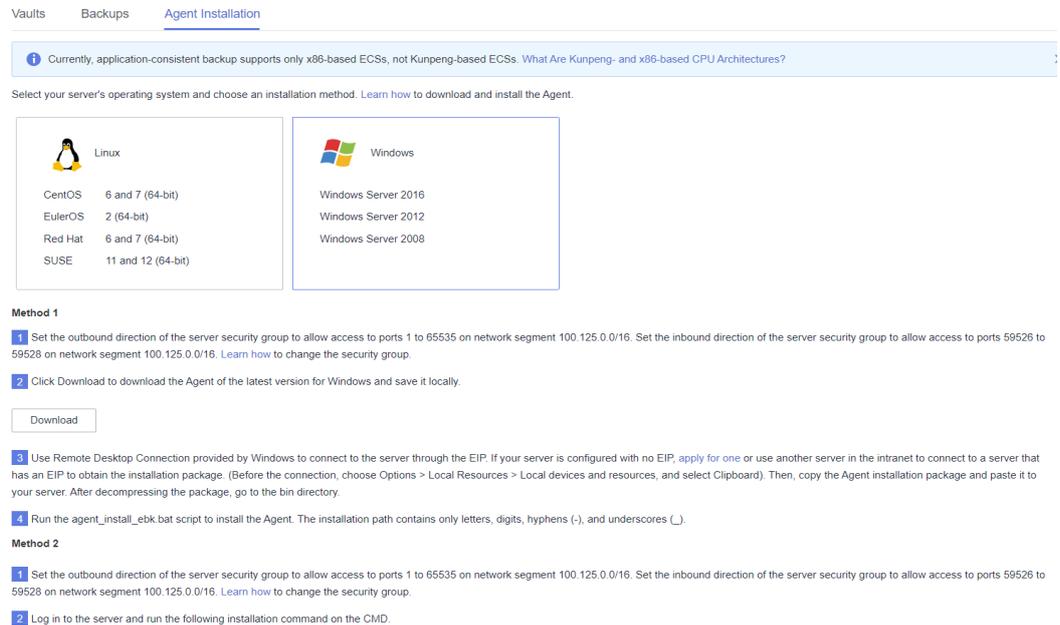
Instalación del agente para un sistema operativo Windows (Método 2)

Paso 1 Inicie sesión en la consola de CBR.

1. **Inicie sesión en la consola de gestión.**
2. Haga clic en  en la esquina superior izquierda y seleccione su región y proyecto.
3. Elija **Storage > Cloud Backup and Recovery**. Elija el tipo de copia de respaldo deseado en el panel de navegación izquierdo.

Paso 2 Haga clic en la pestaña **Agent Installation**.

Figura 6-11 Página de instalación para Windows



Paso 3 En la página ECS, seleccione el servidor de destino y haga clic en **Remote Login** en la columna **Operation** para iniciar sesión en ECS como administrador.

Paso 4 Copie los comandos de instalación del paso 2 del método 2 en el servidor y ejecute el comando en el símbolo del sistema.

Paso 5 Copie cualquier dirección IP en el nombre de la respuesta, péguela en el cuadro de direcciones del navegador y reemplace **0.0.0.0** en la siguiente dirección con la dirección. Reemplace **ap-southeast-1** con la región real. El siguiente comando usa **ap-southeast-1** como ejemplo. A continuación, pulse **Enter** en el navegador para descargar el paquete de instalación.

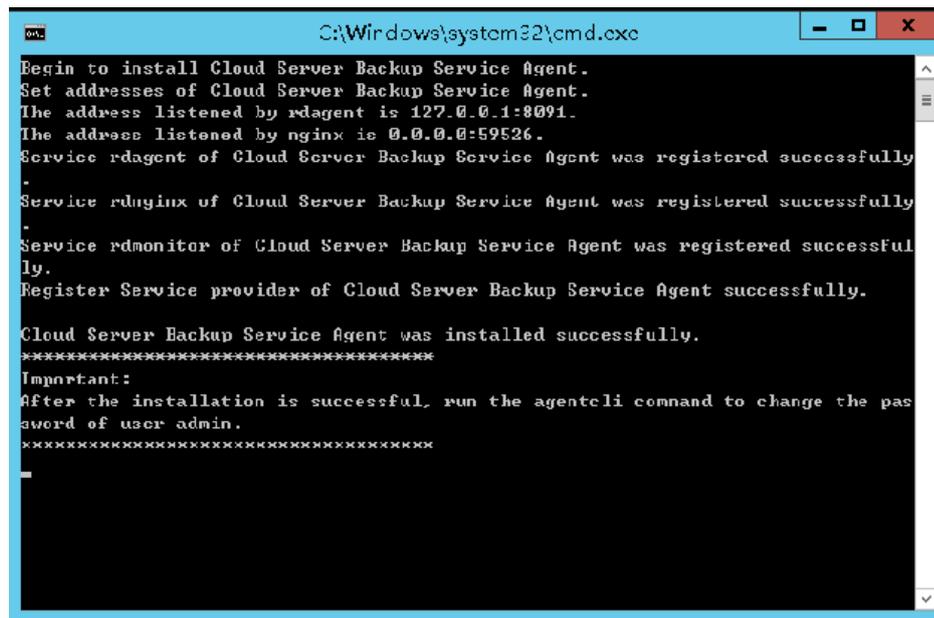
http://0.0.0.0/csbs-agent-ap-southeast-1/Cloud Server Backup Agent-WIN64.zip

Paso 6 Descomprima el archivo para obtener el archivo de instalación. Descomprima el paquete de instalación en cualquier directorio y vaya al **Installation path\bin**.

Paso 7 Haga doble clic en el script **agent_install_ebk.bat** para iniciar la instalación.

Paso 8 El sistema muestra un mensaje que indica que el cliente se ha instalado correctamente. Consulte **Figura 6-12**.

Figura 6-12 Instalación exitosa del cliente para Windows



```
C:\Windows\system32\cmd.exe
Begin to install Cloud Server Backup Service Agent.
Set addresses of Cloud Server Backup Service Agent.
The address listened by rdagent is 127.0.0.1:8091.
The address listened by nginx is 0.0.0.0:59526.
Service rdagent of Cloud Server Backup Service Agent was registered successfully.
Service rdnginx of Cloud Server Backup Service Agent was registered successfully.
Service rdmonitor of Cloud Server Backup Service Agent was registered successfully.
Register Service provider of Cloud Server Backup Service Agent successfully.
Cloud Server Backup Service Agent was installed successfully.
*****
Important:
After the installation is successful, run the agentcli command to change the password of user admin.
*****
```

----Fin

6.4 Creación de una copia de respaldo consistente con las aplicaciones

CBR admite copias de seguridad compatibles con las aplicaciones, además de copias de seguridad compatibles con fallos. La copia de respaldo consistente con las aplicaciones garantiza la consistencia de los datos de las aplicaciones al realizar copias de seguridad de archivos y discos al mismo tiempo. Es adecuado para realizar copias de respaldo de ECS, así como las bases de datos MySQL o SAP HANA que se ejecutan en ellos.

Restricciones

- Actualmente, la copia de respaldo coherente con las aplicaciones no es compatible con las aplicaciones de clúster, como MySQL Cluster. Solo es compatible con aplicaciones en servidores independientes.
- Se le recomienda realizar copias de seguridad coherentes con las aplicaciones en horas fuera de pico.

Procedimiento

Paso 1 Inicie sesión en la consola de CBR.

1. [Inicie sesión en la consola de gestión.](#)
2. Haga clic en  en la esquina superior izquierda y seleccione su región y proyecto.
3. Elija **Storage > Cloud Backup and Recovery**. Elija el tipo de copia de respaldo deseado en el panel de navegación izquierdo.

Paso 2 Cree un almacén para copias de seguridad compatibles con las aplicaciones haciendo referencia a [Compra de un almacén de copia de respaldo de servidor](#). Seleccione **Enable** para **Application-Consistent Backup**.

- Paso 3** Asocie los servidores en la nube con el almacén creado. Asegúrese de que el Agente se haya instalado en los servidores.
- Paso 4** Cree una copia de respaldo de un servidor en la nube haciendo referencia a [Creación de una copia de respaldo de servidor en la nube](#).
- Si se crea correctamente una copia de respaldo compatible con la aplicación, se muestra una letra azul "A" junto al nombre de la copia de respaldo en la lista de copias de seguridad.
 - Si no se puede crear una copia de respaldo compatible con la aplicación, el sistema crea automáticamente una copia de respaldo del servidor en la nube en su lugar y almacena la copia de respaldo en el almacén, y se muestra una letra gris "A" junto al nombre de la copia de respaldo en la lista de copias de seguridad. Puede ver la causa del error en el área **Management Information** de la página de detalles de copia de respaldo. Consulte [Figura 6-13](#).

Figura 6-13 Estado de copia de respaldo consistente con las aplicaciones

<input type="checkbox"/>	Backup Name		Backup Type	Status
<input type="checkbox"/>	autobk_8d1b	Application-consistent backup succeeded.	A Full backup	✓ Available
<input type="checkbox"/>	autobk_ee60	Application-consistent backup failed.	A Incremental b...	✓ Available

- Paso 5** Vuelva a la página de copia de respaldo del servidor en la nube según se le indique. Si la ejecución de la copia de respaldo falla, rectifique el error basándose en los detalles del error mostrados en la página.

---Fin

Procedimiento posterior

Si se pierden datos debido a ataques de virus o fallas en la base de datos, puede restaurar los datos siguiendo las instrucciones en [Restauración de datos mediante una copia de respaldo de servidor en la nube](#).

6.5 Desinstalación del agente

Escenarios

Esta sección describe cómo desinstalar el Agente cuando ya no se necesita una copia de respaldo compatible con la aplicación.

Prerrequisitos

Se han obtenido el nombre de usuario y la contraseña para iniciar sesión en un ECS.

Desinstalación del agente para Linux

- Paso 1** Inicie sesión en ECS y ejecute el comando **su -root** para cambiar a usuario **root**.

Paso 2 En el directorio `home/rdadmin/Agent/bin`, ejecute el siguiente comando para desinstalar el Agente. **Figura 6-14** muestra un ejemplo. Si la palabra aparece **successfully** en verde, el agente se desinstala correctamente.

```
sh agent_uninstall_ebk.sh
```

Figura 6-14 Agente desinstalado correctamente de Linux

```
user@rdadmin:~/bin$ sh agent_uninstall_ebk.sh
You are about to uninstall the Cloud Server Backup Service Agent. This operation stops the Cloud Server Backup Service Agent and deletes the Cloud Server Backup Service Agent and customized configuration data which cannot be recovered. Therefore, applications on the host are no longer protected.
Suggestion: Confirm whether the customized configuration data, such as customized script, has been backed up.
Are you sure you want to uninstall Cloud Server Backup Service Agent? (y/n, default:n):
>>y
Begin to uninstall Cloud Server Backup Service Agent.
Cloud Server Backup Service Agent was uninstalled successfully.
Cloud Server Backup Service Agent has been uninstalled successfully, the applications on the host are no longer protected.
```

----Fin

Desinstalación del agente para Windows

Paso 1 Inicie sesión en el ECS.

Paso 2 En el directorio *Installation path*/`bin`, haga doble clic en `agent_uninstall_ebk.bat`. Se muestra la ventana para desinstalar el Agente.

Después de que la desinstalación se complete y se realice correctamente, la ventana se cerrará automáticamente. Consulte **Figura 6-15**.

Figura 6-15 Agente desinstalado correctamente desde Windows

```
You are about to uninstall the Cloud Server Backup Service Agent. This operation stops the Cloud Server Backup Service Agent service and deletes the Cloud Server Backup Service Agent and customized configuration data which cannot be recovered. Therefore, applications on the host are no longer protected.
Suggestion: Confirm whether the customized configuration data, such as customized script, has been backed up.
Are you sure you want to uninstall Cloud Server Backup Service Agent? (y/n, default:n):
>>y
Begin to uninstall Cloud Server Backup Service Agent...

Service rdmonitor of Cloud Server Backup Service Agent was uninstalled successfully.
Service rdnginx of Cloud Server Backup Service Agent was uninstalled successfully.
Service rdagent of Cloud Server Backup Service Agent was uninstalled successfully.
Service rdprovider of Cloud Server Backup Service Agent was uninstalled successfully.

Delete user rdadmin of Cloud Server Backup Service Agent...
```

----Fin

7 Copia de respaldo de archivos

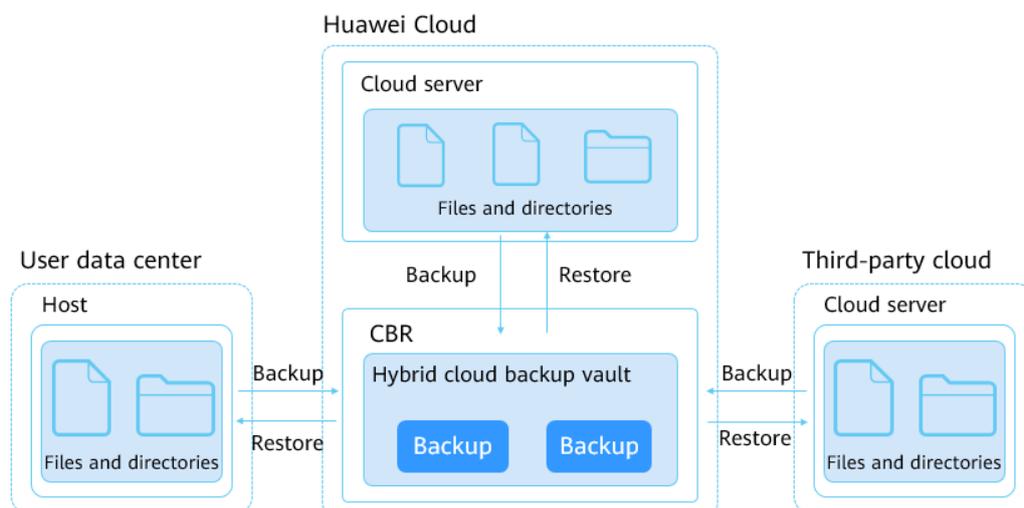
7.1 ¿Qué es la copia de respaldo de archivos?

Descripción general de la copia de respaldo de archivos

CBR proporciona copias de respaldo de archivos que le permite realizar copias de respaldo de archivos y directorios en sus servidores en la nube y hosts locales, por lo que no tiene que realizar copias de respaldo de todos sus servidores o discos. Los servidores en la nube pueden ser servidores de Huawei Cloud o sus homólogos de una nube de terceros. Si se produce una eliminación accidental o un error de software/hardware en sus archivos, puede restaurar los datos en cualquier momento en el pasado cuando se generó una copia de respaldo.

Figura 7-1 muestra la arquitectura de copia de respaldo de archivos.

Figura 7-1 Arquitectura de copia de respaldo de archivos



Ámbito de copia de respaldo de archivos

Tabla 7-1 enumera los sistemas operativos admitidos para hosts locales.

Tabla 7-1 Sistemas operativos que admiten copias de seguridad de archivos

Sistema operativo	Versión admitida
Windows Server	Windows Server 2019 for x86_64 Windows Server 2016 for x86_64 Windows Server 2012 for x86_64
Windows	Windows 10 Windows 7
CentOS	CentOS 7
EulerOS	Euler OS 2.5

 **NOTA**

Si está ejecutando Windows Server 2019, Windows Server 2012 o Windows 7, se devolverá un mensaje que indica que falta MSVCR100.dll durante la instalación del agente. En este caso, corrija el problema haciendo referencia a [actualización de seguridad de MFC](#) y vuelva a instalar el agente.

Diferencias entre Copia de respaldo SFS Turbo y Copia de respaldo de archivos

Artículo	Copia de respaldo SFS Turbo	Copia de respaldo de archivos
Copia de respaldo y restauración de objetos	Sistemas de archivos SFS Turbo	Uno o varios archivos en servidores en la nube y hosts locales
Unidad de copia de respaldo	Sistema de archivos de SFS Turbo	Archivo
Tipo de almacén	Almacén de copia de respaldo SFS Turbo	Almacén de copia de respaldo de nube híbrida
Escenario recomendado	Es necesario proteger los datos de los sistemas de archivos SFS Turbo. Los datos de copia de respaldo no se almacenan en el sistema de archivos y se pueden utilizar para crear nuevos sistemas de archivos cuando sea necesario.	Los datos en uno o varios archivos en servidores en la nube y hosts locales deben protegerse, y los datos pueden respaldarse y restaurarse rápidamente en la nube.

Restricciones de copia de respaldo de archivos

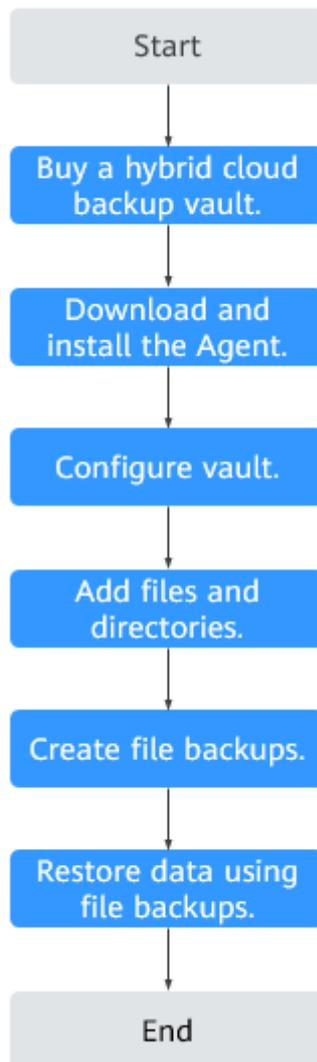
- Durante la copia de respaldo de archivos, si una aplicación está cambiando un archivo y el cliente de copia de respaldo tiene el permiso de lectura en este archivo, los datos de la copia de respaldo estarán incompletos. Se recomienda que primero detenga la aplicación y luego realice una copia de respaldo para garantizar la integridad de los datos.

- Durante la copia de respaldo de archivos, si un proceso está utilizando un archivo o el cliente de copia de respaldo no tiene el permiso de lectura en este archivo, los datos de la copia de respaldo estarán incompletos.
- Se recomienda no restaurar copias de respaldo de archivos en aplicaciones en ejecución. Detenga las aplicaciones y luego restaure los archivos.
- Un cliente de copia de respaldo puede tener un máximo de 8 archivos y directorios añadidos.
- Cada recurso solo puede tener un Agente instalado.
- El número de recursos en los que se puede instalar el Agente no está limitado.
- Se recomienda que un directorio no contenga más de 500,000 archivos.
- Una ruta puede contener un máximo de 200 caracteres.
- El ancho de banda máximo permitido para la transmisión de datos de copia de respaldo de archivos es de 16 Gbit/s. Si se alcanza el ancho de banda máximo, se activará el control de flujo.
- La copia de respaldo de archivos no puede realizar copias de seguridad de los archivos almacenados en los sistemas de archivos SFS que están montados en servidores en la nube.
- La copia de respaldo puede fallar en directorios con escrituras de archivos frecuentes en Windows.

7.2 Proceso de copia de respaldo de archivos

Figura 7-2 muestra el proceso de copia de respaldo de archivos.

Figura 7-2 Proceso de copia de respaldo de archivos



1. Cree un almacén de copia de respaldo en la nube híbrida.
Antes de instalar el agente de copia de respaldo de archivos, cree un almacén haciendo referencia a **Creación de un almacén de copia de respaldo en la nube híbrida**. El almacén creado se utilizará para almacenar copias de respaldo de archivos generadas.
2. Descargue e instale el agente.
Instale el agente en los servidores de destino haciendo referencia a **Descarga e instalación del agente**. Una vez instalado correctamente el Agente, los servidores aparecen automáticamente como clientes de copia de respaldo en la lista de copia de respaldo de archivos.
3. Configurar el almacén.
Configure el almacén para los clientes de copia de respaldo haciendo referencia a **Configuración de almacén**. Las copias de respaldo de archivos generadas se almacenarán en el almacén configurado.
4. Añadir archivos y directorios.

Agregue los archivos y directorios a los que desea hacer una copia de respaldo haciendo referencia a [Adición de directorios](#).

5. Cree copias de respaldo de archivos.

Realice copias de seguridad manualmente haciendo referencia a [Creación de copias de respaldo de archivos](#) o haga que el sistema cree copias de seguridad automáticamente. Las copias de respaldo generadas se almacenarán en el almacén.

6. Restaurar datos mediante copias de respaldo de archivos.

Restaurar datos haciendo referencia a [Restauración de datos mediante una copia de respaldo de archivos](#). Puede restaurar los datos en servidores de origen o en servidores diferentes.

7.3 Creación de un almacén de copia de respaldo en la nube híbrida

Esta sección describe cómo comprar un almacén de copia de respaldo en la nube híbrida para almacenar copias de seguridad de archivos.

Procedimiento

Paso 1 Inicie sesión en la consola CBR.

1. Inicie sesión en la consola de gestión.
2. Haga clic en  en la esquina superior izquierda y seleccione su región y proyecto.
3. Elija **Storage > Cloud Backup and Recovery > File Backups**.

Paso 2 En la esquina superior derecha de la página, haga clic en **Buy Hybrid Cloud Backup Vault**.

Paso 3 Seleccione un modo de facturación.

- **Anual/mensual** es un modo de facturación prepagada. Se le factura en función de la duración de la suscripción que especifique. Este modo proporciona precios más bajos y es ideal cuando la duración del uso de recursos es predecible.
- **El pago por uso** es un modo de facturación pospago. Se le factura en función de su uso de recursos. Con este modo, puede aumentar o eliminar recursos en cualquier momento. Los cargos se deducen del saldo de su cuenta.

Paso 4 Especifique la capacidad del almacén, que oscila entre 1 y 10240 TB.

Debe planificar correctamente la capacidad del almacén, que debe ser al menos el mismo tamaño que el de los archivos de los que desea realizar una copia de respaldo. Compruebe el tamaño del archivo en sus hosts locales. A medida que crece el espacio utilizado del almacén, puede ampliar la capacidad de la bóveda si es insuficiente.

Paso 5 Determine si desea configurar la copia de respaldo automática.

- Si selecciona **Configure**, debe seleccionar una política de copia de respaldo existente o crear una nueva política. Después de crear el almacén, el sistema aplicará la política a este almacén, y todos los archivos asociados a este almacén se copiarán automáticamente según esta política.
- Si selecciona **Skip**, los archivos asociados a este almacén no se copiarán automáticamente hasta que le aplique una política de copia de respaldo.

Paso 6 (Opcional) Agregar etiquetas al almacén.

Una etiqueta se representa en forma de un par clave-valor. Las etiquetas se utilizan para identificar, clasificar y buscar almacenes. Las etiquetas Vault sólo se utilizan para filtrar y gestionar almacenes. Un almacén puede tener un máximo de 10 etiquetas.

Tabla 7-2 describe los parámetros de una etiqueta.

Tabla 7-2 Descripción del parámetro de etiqueta

Parámetro	Descripción	Valor de ejemplo
Key	<p>Cada etiqueta tiene una clave única. Puede personalizar la clave o seleccionar la clave de una etiqueta existente creada en TMS.</p> <p>Una clave de etiqueta:</p> <ul style="list-style-type: none"> ● Puede contener de 1 a 36 caracteres Unicode. ● Puede contener solo letras, dígitos, guiones (-) y guiones bajos (_). 	Key_0001
Value	<p>Un valor de etiqueta puede ser repetitivo o dejarse en blanco.</p> <p>Un valor de etiqueta:</p> <ul style="list-style-type: none"> ● Puede contener de 0 a 43 caracteres Unicode. ● Puede contener solo letras, dígitos, guiones (-) y guiones bajos (_). 	Value_0001

Paso 7 Especifique un nombre para el almacén.

Un nombre debe contener de 1 a 64 caracteres incluyendo dígitos, letras, (_), guiones bajos o (-) guiones, por ejemplo, **vault-f61e**.

 **NOTA**

Puede utilizar el nombre predeterminado, que tiene el formato de **vault_xxxx**.

Paso 8 Especifique la duración requerida si selecciona la facturación anual/mensual. El período de validez oscila entre 1 mes y 5 años.

Determine si desea habilitar la renovación automática. Si selecciona **Auto Renewal**:

- Su suscripción se renovará cada mes para la facturación mensual.
- Su suscripción se renovará cada año para la facturación anual.

Paso 9 Pagar el pedido según se le solicite.

Paso 10 Vuelva a la página **File Backups** y vea el almacén creado en la lista del almacén.

----**Fin**

7.4 Descarga e instalación del agente

Escenarios

Antes de realizar una copia de respaldo de los archivos, debe cambiar el grupo de seguridad de los servidores o máquinas virtuales de destino e instalar el agente en ellos. En esta sección se describe cómo descargar e instalar el Agente.

Actualmente, solo se admiten los hosts que ejecutan sistemas operativos de 64 bits.

Instalación del agente en un servidor Linux

Paso 1 Inicie sesión en la consola CBR.

1. Inicie sesión en la consola de gestión.
2. Haga clic en  en la esquina superior izquierda y seleccione su región y proyecto.
3. Elija **Storage > Cloud Backup and Recovery > File Backups**.

Paso 2 Haga clic en **Add Backup Client**. En la página mostrada, seleccione el sistema operativo Linux.

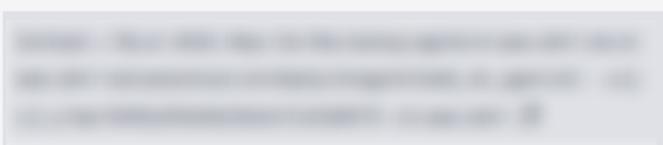
Figura 7-3 Linux

✕

Add Backup Client

i To perform file backups, you must buy a hybrid cloud backup vault first and then install the Agent on target servers.

How to Install the Agent

- Obtain the installation command or package.**
 - Select an operating system.
 -  Linux Supported Versions
 -  Windows Supported Versions
 - Copy the installation command.

After copying the command, proceed with the following steps.
- Install the Agent.**
 - Check the domain connectivity.
Run the `curl -kv obs.myhuaweicloud.com` command. If network latency data is returned, the connectivity is normal.
 - Log in to the client.
Remotely log in to the backup client or VM as user root.
 - Enter AK and SK.
Enter the AK and SK in the brackets of `a{}` and `s{}` in the command. [Learn how to obtain AK and SK.](#)
 - Execute the command.
After the login is successful, paste the command, and press Enter to execute it.
 - Wait for the returned result.
If the following information is displayed, the installation is successful. Wait for 1

Paso 3 Inicie sesión en el host de destino como usuario **root**.

Paso 4 En el host, ejecute el comando **curl -kv obs.myhuaweicloud.com**. Si se devuelven datos de latencia de red, la conectividad es normal.

Paso 5 Complete el comando de instalación proporcionado en la consola CBR introduciendo el AK y el SK entre corchetes de **a {}** y **s {}** en el comando. [¿Cómo obtener un AK/SK?](#)

```
/bin/bash -c '$(curl -kfsSL https://obs.region1.myhuaweicloud.com/cbr/deploy/cbragent/install_cbr_agent.sh)' -- -a {} -s {} -p 0605767aecxxxxxxxxxxxx -r region1
```

NOTA

Elimine los corchetes después de introducir el AK y el SK.

Paso 6 Ejecute el comando obtenido en el host para instalar el Agente.

Paso 7 Si se muestra información similar a la siguiente, el Agente se instala correctamente.

Figura 7-4 Ejecutar el comando de instalación

```
[root@ ~]# /bin/bash -c "$(curl -kfsSL https://mirrors.huaweicloud.com/cbr/deplo/cbragent/install_cbr_agent.sh)" -- -a -s -p -r
Installing CBR agent ...
Begin to config agent
Agent was started successfully.
Start cbr agent success.
The agent is installed successfully.
```

Paso 8 Espere aproximadamente 1 minuto y vea el cliente de copia de respaldo en la lista de copia de respaldo de archivos. Si el estado del Agente es **Normal**, el sistema detecta correctamente al cliente y el Agente se está ejecutando correctamente.

----Fin

Instalación del agente en un servidor Windows

Paso 1 Inicie sesión en la consola CBR.

1. Inicie sesión en la consola de gestión.
2. Haga clic en  en la esquina superior izquierda y seleccione su región y proyecto.
3. Elija **Storage > Cloud Backup and Recovery > File Backups**.

Paso 2 Haga clic en **Add Backup Client**. En la página mostrada, seleccione el sistema operativo Windows.

Figura 7-5 Windows

Add Backup Client

Info To perform file backups, you must buy a hybrid cloud backup vault first and then install the Agent on target servers.

How to Install the Agent

- Obtain the installation command or package.**
 - Select an operating system.
 - [Linux Supported Versions](#)
 - [Windows Supported Versions](#)
 - Obtain the Agent.
 - [Download](#)

Click the button to download the latest Agent to your local computer.
- Install the Agent.**
 - Prepare for the installation.
 - Check the domain connectivity.

On the local host, choose Start > Run. In the Run dialog box, enter `cmd` and press Enter.

Ping `obs.myhuaweicloud.com`. If network latency data is returned, the connectivity is normal.
 - Collect information required for the installation.

AK/SK: [Learn how](#)

Project ID:

Region ID:
 - Install the Agent.

Decompress the obtained package to the installation directory. Ensure that the directory contains only letters, digits, underscores (`_`), and hyphens (`-`). Then go to the script directory, right-click `agent_install.bat`, and choose **Run as administrator** from the shortcut menu. In the displayed dialog box, enter the information

Paso 3 Haga clic en **Download** para descargar el paquete de instalación del agente más reciente en el equipo local.

Paso 4 En el host local, elija **Start > Run**. En el cuadro de diálogo **Run**, escriba `cmd` y pulse **Enter**.

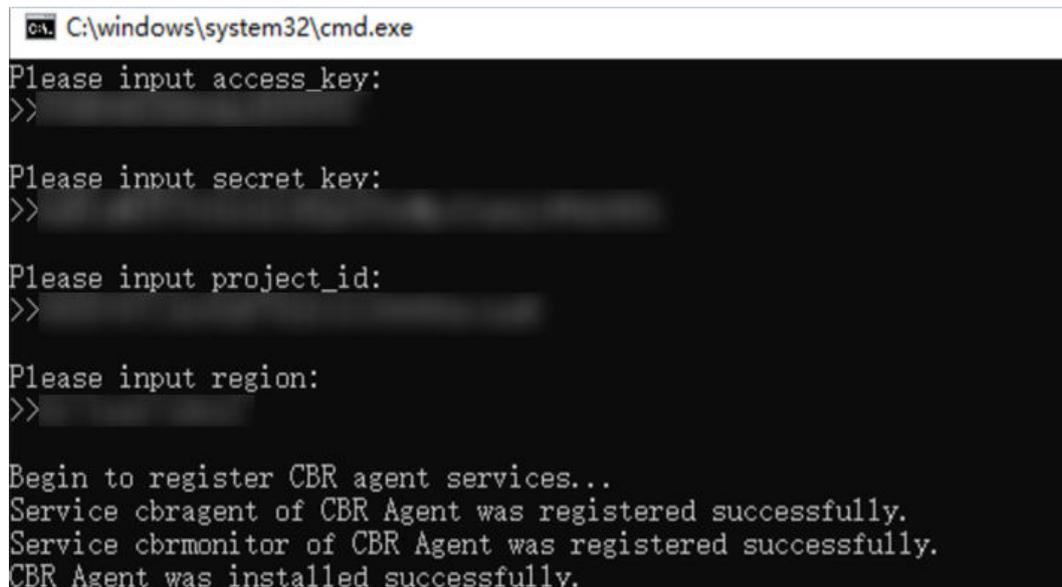
Ejecute el comando **ping obs.myhuaweicloud.com**. Si se devuelven datos de latencia de red, la conectividad es normal.

Paso 5 Descomprima el paquete obtenido en el directorio de instalación. Asegúrese de que el directorio contiene solo letras, dígitos, guiones bajos (`_`), y guiones (`-`). A continuación, vaya al directorio de **script**, haga clic con el botón secundario en `agent_install.bat` y elija **Run as administrator** en el menú contextual. En el cuadro de diálogo que se muestra, introduzca la información según sea necesario.

Paso 6 Asegúrese de que la ruta de instalación contenga solo letras, dígitos, guiones bajos (`_`) o guiones (`-`). Consulte [Figura 7-6](#).

- **access_key**: Ingrese su AK. [¿Cómo obtener un AK/SK?](#)
- **secret_key**: Ingrese su SK. [¿Cómo obtener un AK/SK?](#)
- **project_id**: Copie el ID del proyecto de la página de instalación.
- **region**: copie el ID de región de la página de instalación.

Figura 7-6 Ejecutar el comando de instalación



```
C:\windows\system32\cmd.exe
Please input access_key:
>>
Please input secret key:
>>
Please input project_id:
>>
Please input region:
>>
Begin to register CBR agent services...
Service cbragent of CBR Agent was registered successfully.
Service cbrmonitor of CBR Agent was registered successfully.
CBR Agent was installed successfully.
```

📖 NOTA

Si está ejecutando Windows Server 2019, Windows Server 2012 o Windows 7, se devolverá un mensaje que indica que falta MSVCR100.dll durante la instalación del agente. En este caso, corrija el problema haciendo referencia a [actualización de seguridad de MFC](#) y vuelva a instalar el agente.

Paso 7 Después de que "CBR Agente se instaló correctamente" se devuelve, espere aproximadamente 1 minuto, vuelva a la lista de copia de respaldo de archivos y busque el cliente de copia de respaldo. Si su estado de Agente es **Normal**, el Agente se ha instalado correctamente.

----Fin

Eliminación de un cliente

Si ya no se necesita un cliente de copia de respaldo, puede eliminarlo.

Paso 1 Inicie sesión en la consola CBR.

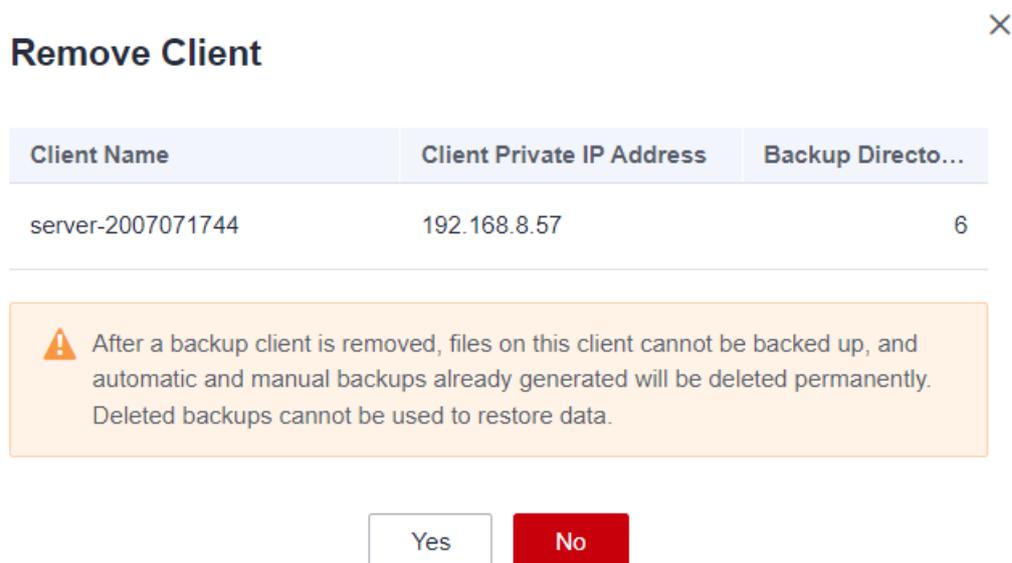
1. Inicie sesión en la consola de gestión.
2. Haga clic en  en la esquina superior izquierda y seleccione su región y proyecto.
3. Elija **Storage > Cloud Backup and Recovery > File Backups**.

Paso 2 Localice la fila que contiene el cliente de copia de respaldo de destino, haga clic en **More** en la columna **Operation** y elija **Remove Client**. Consulte [Figura 7-7](#).

Después de eliminar un cliente de copia de respaldo, los archivos de este cliente no se pueden realizar copias de respaldo, y las copias de respaldo automáticas y manuales ya generadas se

eliminarán permanentemente. Las copias de respaldo eliminadas no se pueden utilizar para restaurar datos.

Figura 7-7 Eliminar cliente



Paso 3 Haga clic en **Yes**.

---Fin

7.5 Configuración de almacén

Escenarios

Una vez que el sistema descubra los clientes de copia de respaldo, configure un almacén para que cada cliente tenga las copias de respaldo generadas automáticamente almacenadas en el almacén.

Procedimiento

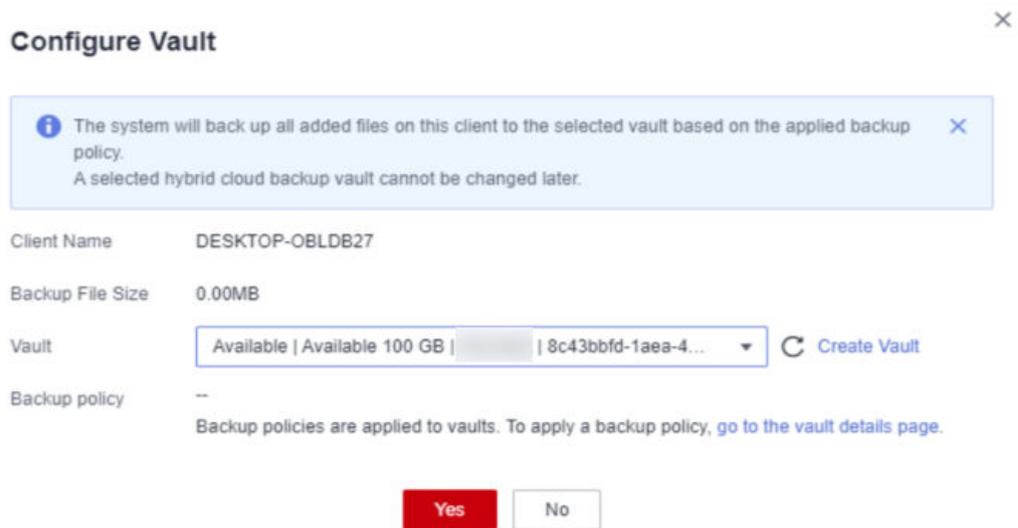
Paso 1 Inicie sesión en la consola CBR.

1. Inicie sesión en la consola de gestión.
2. Haga clic en  en la esquina superior izquierda y seleccione su región y proyecto.
3. Elija **Storage > Cloud Backup and Recovery > File Backups**.

Paso 2 Haga clic en la pestaña **File Backup** y busque el cliente de copia de respaldo de destino. A continuación, haga clic en **Configure Vault** en la columna **Backup Configuration**.

Paso 3 En la página mostrada, seleccione un almacén. Consulte [Figura 7-8](#).

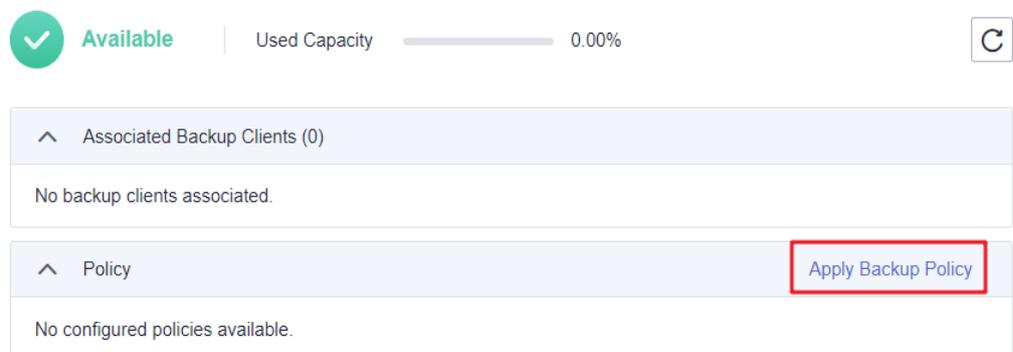
Figura 7-8 Configurar Vault



Paso 4 Haga clic en **OK**. Vea el almacén configurado en la columna **Backup Configuration** de la lista de copia de respaldo de archivos.

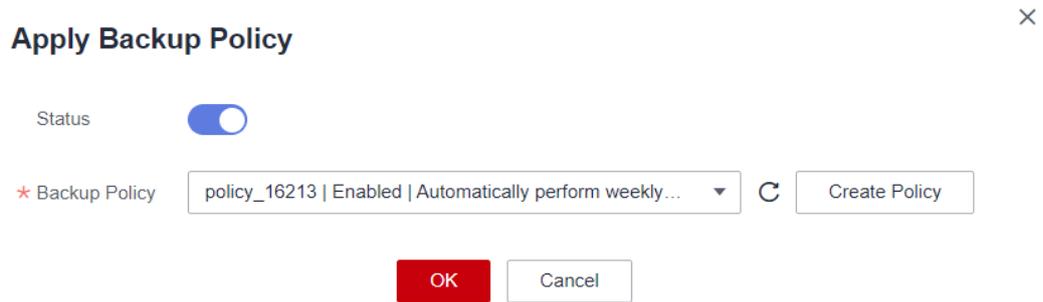
Paso 5 (Opcional) Si no se aplica una política de copia de respaldo al crear la bóveda de copia de respaldo en la nube híbrida y ahora desea configurar la copia de respaldo automática para los clientes de copia de respaldo, haga clic en el nombre de la bóveda en la columna **Backup Configuration** y aplique una política de copia de respaldo al almacén. Consulte [Figura 7-9](#).

Figura 7-9 Aplicar política



Paso 6 (Opcional) Haga clic en **Apply Backup Policy**. Seleccione una política de copia de respaldo existente o cree una nueva. Consulte [Figura 7-10](#).

Figura 7-10 Aplicar política



Paso 7 (Opcional) Haga clic en **OK**. La política se aplica correctamente al almacén de copia de respaldo en la nube híbrida.

----Fin

7.6 Adición de directorios

Escenarios

Después de instalar el agente en los servidores de destino, CBR los detectará y mostrará automáticamente como clientes de copia de respaldo en la lista de copia de respaldo de archivos en **Cloud Backup and Recovery > File Backups > File backup**. Es necesario agregar las rutas de acceso de los archivos y directorios de los que desea realizar una copia de respaldo.

Restricciones

- Un cliente de backup puede tener un máximo de 8 directorios agregados.
- Un directorio soporta hasta archivos 100,000.
- El tamaño de un directorio no puede exceder los 500 GB.
- Una ruta de acceso debe ser una ruta de acceso absoluta, por ejemplo, una ruta de acceso que comience por /, C:\, o D:\.

Adición de directorios

Paso 1 Inicie sesión en la consola CBR.

1. Inicie sesión en la consola de gestión.
2. Haga clic en  en la esquina superior izquierda y seleccione su región y proyecto.
3. Elija **Storage > Cloud Backup and Recovery > File Backups**.

Paso 2 Localice el cliente de copia de respaldo de destino y haga clic en su nombre para ir a la página de detalles.

Paso 3 Haga clic en **Add Backup Directory**. Consulte [Figura 7-11](#).

Figura 7-11 Agregar directorio de copia de respaldo

Paso 4 Pegue las rutas en el cuadro de texto y haga clic en **OK**.

Paso 5 Las rutas de archivo se mostrarán en la parte inferior de la página.

----Fin

Eliminación de directorios

Si ya no se requiere una copia de respaldo para un directorio o se ha alcanzado el número máximo de directorios permitido, puede eliminar los directorios.

Paso 1 Inicie sesión en la consola de ECS.

1. Inicie sesión en la consola de gestión.
2. Haga clic en  en la esquina superior izquierda y seleccione su región y proyecto.
3. Elija **Storage > Cloud Backup and Recovery > File Backups**.

Paso 2 Localice el cliente de copia de respaldo de destino y haga clic en su nombre para ir a la página de detalles.

Paso 3 Localice el directorio de destino y haga clic en **Remove Directory**. Consulte [Figura 7-12](#).

Después de eliminar un directorio, no se puede hacer una copia de respaldo de los archivos de este directorio. Las copias de respaldo ya generadas no se eliminarán y se pueden utilizar para restaurar datos. Un directorio sin copias de respaldo generadas se eliminará permanentemente.

Figura 7-12 Eliminar directorio

Backup Directory	Client Name	Private IP Address
D:\test03	server-2007071744	192.168.8.57

Warning: After a directory is removed, files in this directory cannot be backed up. Backups already generated will not be deleted and can be used to restore data. A directory with no backups generated will be removed permanently.

Paso 4 Haga clic en **Yes**.

---Fin

7.7 Creación de copias de respaldo de archivos

Escenarios

Esta sección describe cómo crear copias de respaldo de archivos manualmente.

Para implementar copias de respaldo automáticas, cree una política y aplíquela a un almacén haciendo referencia a [Creación de una política de copia de respaldo](#). A continuación, el sistema realizará automáticamente copias de respaldo en los puntos de tiempo especificados en la política.

Restricciones

- Sólo se puede hacer una copia de respaldo de los clientes cuyo estado de Agente es **Normal**.

Procedimiento

Paso 1 Inicie sesión en la consola CBR.

1. Inicie sesión en la consola de gestión.
2. Haga clic en  en la esquina superior izquierda y seleccione su región y proyecto.
3. Elija **Storage > Cloud Backup and Recovery > File Backups**.

Paso 2 Haga clic en la pestaña **File Backup** y busque el cliente de copia de respaldo de destino.

Paso 3 Haga clic en **Perform Backup** en la columna **Operation**. El sistema crea automáticamente copias de respaldo de los archivos.

Paso 4 En la página de la pestaña **File Backup**, haga clic en el nombre del cliente de copia de respaldo de destino. En el área **Backup Details** de la página mostrada, si los estados de todas las copias de respaldo generadas están **Available**, la tarea de copia de respaldo se realiza correctamente.

NOTA

Si realiza cambios en un archivo durante la copia de respaldo, la copia de respaldo de ese archivo puede fallar. Para garantizar la integridad de los datos, se recomienda esperar hasta que se complete la tarea de copia de respaldo y, a continuación, cambiar el archivo y realizar una copia de respaldo de nuevo.

Una vez completada la tarea de copia de respaldo, puede restaurar los datos del archivo haciendo referencia a [Restauración de datos mediante una copia de respaldo de archivos](#) según sea necesario.

---Fin

7.8 Restauración de datos mediante una copia de respaldo de archivos

Puede utilizar una copia de respaldo de archivos para restaurar los datos de un cliente de copia de respaldo al estado en un momento dado cuando se realizó la copia de respaldo de los datos.

Restricciones

- El estado del Agente del cliente de copia de respaldo debe ser **Normal**.
- Se recomienda no restaurar copias de respaldo de archivos en aplicaciones en ejecución. Detenga las aplicaciones y luego restaure los archivos.

Método 1

Paso 1 Inicie sesión en la consola CBR.

1. Inicie sesión en la consola de gestión.
2. Haga clic en  en la esquina superior izquierda y seleccione su región y proyecto.
3. Elija **Storage > Cloud Backup and Recovery > File Backups**.

Paso 2 En la página de la pestaña **File Backup**, haga clic en el nombre del cliente de copia de respaldo de destino.

Paso 3 Encuentre la copia de respaldo deseada y haga clic en **Restore Data**.

Figura 7-13 Restauración de un archivo

Restore Data ✕

Restore Time: Apr 11, 2022 15:41:47 GMT+08:00

Restore To: New location Current location

Target Client:

Storage Path:

During the recovery, any file with the same name will be overwritten.

Paso 4 Seleccione una ubicación de restauración.

- **Current location:** Los datos se restaurarán a la ruta original del archivo en el cliente de copia de respaldo actual, y cualquier archivo con el mismo nombre se sobrescribirá. Esta opción solo está disponible para clientes de copia de respaldo de Linux.
- **New location:** Los datos se restaurarán en un servidor diferente. Puede seleccionar un cliente de destino y especificar una ruta.
Solo puede elegir entre los clientes de copia de respaldo cuyo estado de Agente es **Normal**. Si el servidor de destino no está en la lista, vaya a la lista de copia de respaldo de archivos e instale el agente.

Paso 5 Haga clic en **OK**. Puede comprobar si los datos se restauran correctamente en el área **Backup Details** de la página de detalles del cliente o en el host local.

Cuando el estado de la copia de respaldo cambia a **Available**, la restauración se realiza correctamente.

----Fin

Método 2

Paso 1 Inicie sesión en la consola CBR.

1. Inicie sesión en la consola de gestión.
2. Haga clic en  en la esquina superior izquierda y seleccione su región y proyecto.
3. Elija **Storage > Cloud Backup and Recovery > File Backups**.

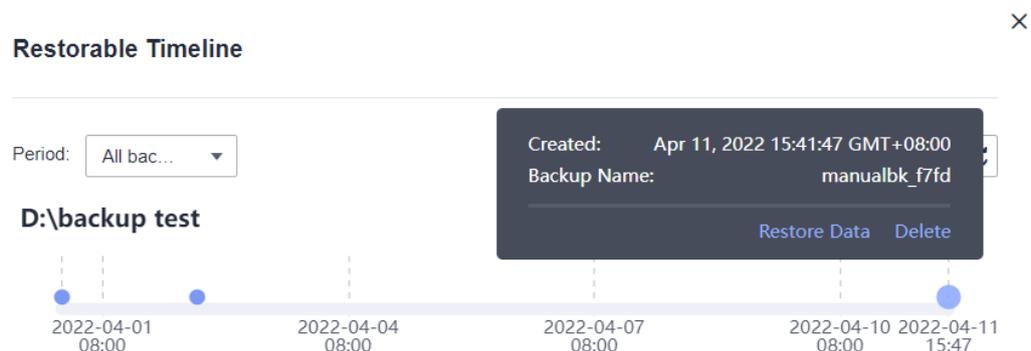
Paso 2 En la página de la pestaña **File Backup**, haga clic en el nombre del cliente de copia de respaldo de destino.

Paso 3 Haga clic en **Restorable Timeline** en la columna **Operation**.

Paso 4 Seleccione un tiempo de restauración y haga clic en **Restore Data**. Consulte [Figura 7-14](#).

El sistema restaurará los datos al estado en el momento seleccionado.

Figura 7-14 Línea de tiempo restaurable



Paso 5 Seleccione una ubicación de restauración.

- **Current location:** Los datos se restaurarán a la ruta original del archivo en el cliente de copia de respaldo actual, y cualquier archivo con el mismo nombre se sobrescribirá.
- **New location:** Los datos se restaurarán en un servidor diferente. Puede seleccionar un cliente de destino y especificar una ruta.

Figura 7-16 Agente desinstalado de Windows

```
C:\windows\system32\cmd.exe
Are you sure you want to uninstall CBR Agent? (y/n, default:n):
>>y
Begin to uninstall CBR Agent...

Service cbrmonitor of CBR Agent was uninstalled successfully.
Service cbragent of CBR Agent was uninstalled successfully.

CBR Agent was uninstalled successfully.

Please remove the installation folders of CBR Agent.
```

----Fin

7.10 Casos de resolución de problemas

Contexto

Cuando instala el Agente para agregar clientes de copia de respaldo, la instalación del Agente puede fallar o puede producirse un error después de instalar el Agente. Esta sección describe algunos síntomas comunes, posibles causas y soluciones para ayudarle a localizar rápidamente el problema.

Estado de agente anormal

Síntoma:

Después de instalar el Agente, el estado del Agente se muestra como Anormal en la lista de clientes.

Posible causa:

El estado del Agente es anormal.

Solución:

1. Compruebe si el proceso del agente se está ejecutando correctamente. Si el proceso ha salido, inicie el proceso de nuevo.
En Windows, haga doble clic en el archivo **agent_start.bat**. En Linux, ejecute el comando **service cbragent start**.
2. Vuelva a instalar el agente.
3. Compruebe la zona horaria y la fecha en el cliente de copia de respaldo. Si la diferencia horaria entre el cliente y el servidor es superior a 15 minutos, ajuste la hora local en función de la hora UTC. Si el estado del agente sigue siendo anormal después de ajustar la hora del cliente, espere aproximadamente media hora hasta que el sistema actualice el estado más reciente del agente.

Error en la instalación del agente con el mensaje "BackupService.7403, Invalid Agent" devuelto

Síntoma:

Error en la instalación del agente y se devolvió el mensaje "BackupService.7403, Invalid Client".

Posible causa:

No hay ningún almacén de copia de respaldo en la nube híbrida disponible antes de instalar el Agente.

Solución:

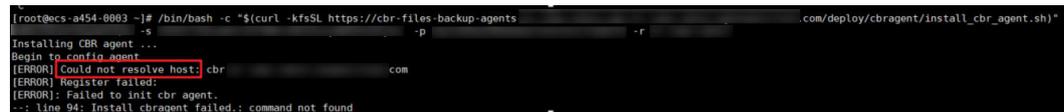
1. Compre un almacén de copia de respaldo en la nube híbrida en la consola CBR.
2. Vuelva a instalar el agente.

Error en la instalación del agente con el mensaje "Could not resolve host" devuelto

Síntoma:

Error en la instalación del agente y se devolvió el mensaje "Could not resolve host".

Figura 7-17 Mensaje "Could not resolve host"



```
[root@ecs-a454-0003 ~]# /bin/bash -c "$(curl -kfsSL https://cbr-files-backup-agents.com/deplo/cbragent/install_cbr_agent.sh)"
Installing CBR agent ...
Begin to config agent.
[ERROR] Could not resolve host: cbr.com
[ERROR] Register failed:
[ERROR] Failed to init cbr agent.
--: line 94: Install cbragent failed.: command not found
```

Posible causa:

El servidor DNS local no puede resolver el nombre de dominio público de Huawei Cloud.

Solución:

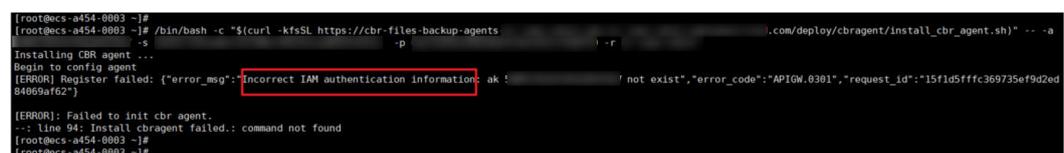
1. Edite el archivo **resolv.conf** en el host local y compruebe si el servidor DNS está configurado. Si accede a Huawei Cloud desde Internet, configure el servidor DNS en **8.8.8.8**.
2. Vuelva a instalar el agente.

Error en la instalación del agente con el mensaje "Incorrect IAM authentication information" devuelto

Síntoma:

Error en la instalación del agente y se devolvió el mensaje "Incorrect IAM authentication information".

Figura 7-18 Mensaje "Incorrect IAM authentication information"



```
[root@ecs-a454-0003 ~]# /bin/bash -c "$(curl -kfsSL https://cbr-files-backup-agents.com/deplo/cbragent/install_cbr_agent.sh)" -- -a
Installing CBR agent ...
Begin to config agent.
[ERROR] Register failed: ("error_msg": "Incorrect IAM authentication information: ak ! not exist", "error_code": "APIGW.0301", "request_id": "15f1d5fffc369735ef9d2ed84669af62")
[ERROR] Failed to init cbr agent.
--: line 94: Install cbragent failed.: command not found
[root@ecs-a454-0003 ~]#
```

Posible causa:

El AK y el SK introducidos durante la instalación son incorrectos.

Solución:

1. Obtener el AK y SK correctos e introdúzcalos de nuevo.
2. Vuelva a instalar el agente.

Error de instalación del agente en Windows con "OpenSCManager failed" registrado en el log

Síntoma:

Error en la instalación del agente en Windows y se registró "OpenSCManager failed" en el log.

Posible causa:

El script de instalación no se ejecuta como administrador.

Solución:

Ejecute el script de instalación como administrador para volver a instalar el Agente.

Error de copia de respaldo después de que se reinstaló el agente de un cliente de Windows y el estado del agente se mostró como anormal en la consola

Síntoma:

Después de desinstalar y reinstalar el Agente de un cliente de copia de respaldo de Windows, las copias de seguridad fallaron y el estado del Agente se mostró como Anormal en la consola.

Posible causa:

- El Agente no puede enviar mensajes de latidos o el nombre de dominio es incorrecto.
- Las escrituras en el archivo de configuración del agente fallan o encuentran un error.

Solución:

Desinstale el agente y vuelva a instalarlo.

El cliente de Windows estaba sin conexión y no se pudo reiniciar

Síntoma:

Error en la instalación del agente en Windows y se registró "OpenSCManager failed" en el log.

Posible causa:

Hay un gran número de archivos .tmp (generados debido a excepciones de compresión de registro) en el directorio de log.

Solución:

1. Elimine todos los archivos de log del directorio de log y desinstale el agente.

2. Vuelva a instalar el agente.

8 (Opcional) Migración de recursos desde CSBS/VBS

Contexto

Huawei Cloud ha lanzado el servicio de copia de respaldo de próxima generación, CBR. Si tiene recursos de copia de respaldo en CSBS o VBS pero desea cambiar a CBR para la gestión de estos recursos de copia de respaldo históricos, puede migrarlos a CBR con unos pocos clics.

Si nunca ha utilizado CSBS o VBS, o si ya no necesita las copias de respaldo históricas, omite esta sección.

Reglas de migración

Durante la migración, el sistema creará automáticamente almacenes basadas en sus recursos históricos.

1. Si los servidores o discos se han asociado a una política de copia de respaldo y se han realizado copias de respaldo, durante la migración, el sistema creará un almacén con el mismo nombre (hasta 64 caracteres) que el nombre de la política, independientemente de si la política está habilitada. Después de crear el almacén, la política se aplicará al almacén.
2. Si los servidores o discos se han asociado a una política de copia de respaldo pero no se ha generado ninguna copia de respaldo, durante la migración, el sistema creará un almacén solo cuando la política esté habilitada. Después de crear el almacén, la política se aplicará al almacén. La regla para nombrar el almacén es la misma que en la regla anterior.
3. Si se han aplicado servidores o discos con una política de copia de respaldo o replicación pero no se ha generado ninguna copia de respaldo o réplica, y la política no está habilitada, entonces sólo se migrará la política.
4. El sistema migrará las políticas de copia de respaldo y replicación independientemente de si están asociadas con servidores o discos.
5. Si la copia de respaldo consistente con la aplicación está habilitada en una política de copia de respaldo, el sistema creará un almacén para almacenar las copias de respaldo consistentes con la aplicación generadas y el nombre del almacén será el mismo que el nombre de la política.

6. Las réplicas de copia de respaldo generadas se almacenarán en un almacén de replicación denominado **default**.
7. Otras copias de respaldo, como las copias de respaldo manuales, se almacenarán en un almacén de copias de respaldo del servidor denominado **default**. Los diferentes almacenes se crearán automáticamente en función de diferentes tipos de recursos. Por ejemplo, el sistema creará un almacén de copias de respaldo de disco durante la migración de copias de respaldo de disco.
8. Después de migrar los recursos, las copias de respaldo creadas con CBR también se mostrarán en la consola de VBS, pero solo se le facturará una vez.

NOTA

Para eliminar copias de respaldo de VBS Console, busque estas copias de respaldo en CBR y elimínelas. Luego, las copias de respaldo también se eliminarán automáticamente de la consola VBS.

9. Si se ha creado una imagen utilizando una copia de respaldo antes de la migración y se ha agregado una etiqueta a la imagen, la migración de copia de respaldo puede fallar. En este caso, vaya a consola de IMS, elimine la etiqueta de la imagen y vuelva a realizar la migración. Una vez completada la migración, vuelva a añadir la etiqueta si es necesario.
10. Si las copias de respaldo se migran desde cualquiera de las siguientes regiones, todas las copias de respaldo en estas regiones se migrarán: CN East-Shanghai1, CN North-Beijing4, CN South-Guangzhou, CN-Hong Kong, AP-Singapore y AP-Bangkok. Para migrar copias de respaldo en otras regiones, vaya a la región correspondiente y proceda con la migración por separado.

Sobre la base de las reglas anteriores, la capacidad de cada almacén creada por el sistema está predefinida como 1.2 veces el tamaño total de la copia de respaldo.

Por ejemplo, un usuario tiene un ECS de 100 GB y un ECS de 50 GB. La capacidad de almacenamiento utilizada de los dos ECS es de 20 GB y 10 GB, respectivamente. El usuario ha realizado una copia de respaldo manual de los dos ECS completos mediante la copia de respaldo del servidor en la nube. Durante la migración, la capacidad del almacén creado automáticamente será 1.2 veces el tamaño total de la copia de respaldo. En este ejemplo, el tamaño total de la copia de respaldo multiplicado por 1.2 es 36 GB. Por lo tanto, el sistema creará automáticamente un almacén de 36 GB.

Restricciones

- De forma predeterminada, un almacén creado por el sistema se factura sobre la base de pago por uso. Si desea cambiar a la facturación anual/mensual, consulte las instrucciones en [Cambio del modo de facturación de pago por uso a anual/mensual](#).
- Después de migrar los recursos, VBS y CSBS no estarán disponibles. CBR utiliza nuevos estándares de facturación. Para obtener más información, consulte [Detalles de precio de CBR](#).
- Los almacenes que ha comprado no se pueden utilizar para la migración. El sistema migrará automáticamente los recursos a los almacenes creados por el sistema.
- Los recursos de copia de respaldo de una cuenta solo deben migrarse una vez.
- Después de migrar los recursos, las copias de respaldo en disco y las copias de respaldo del servidor se almacenarán automáticamente en los almacenes CBR. No se requieren más operaciones.

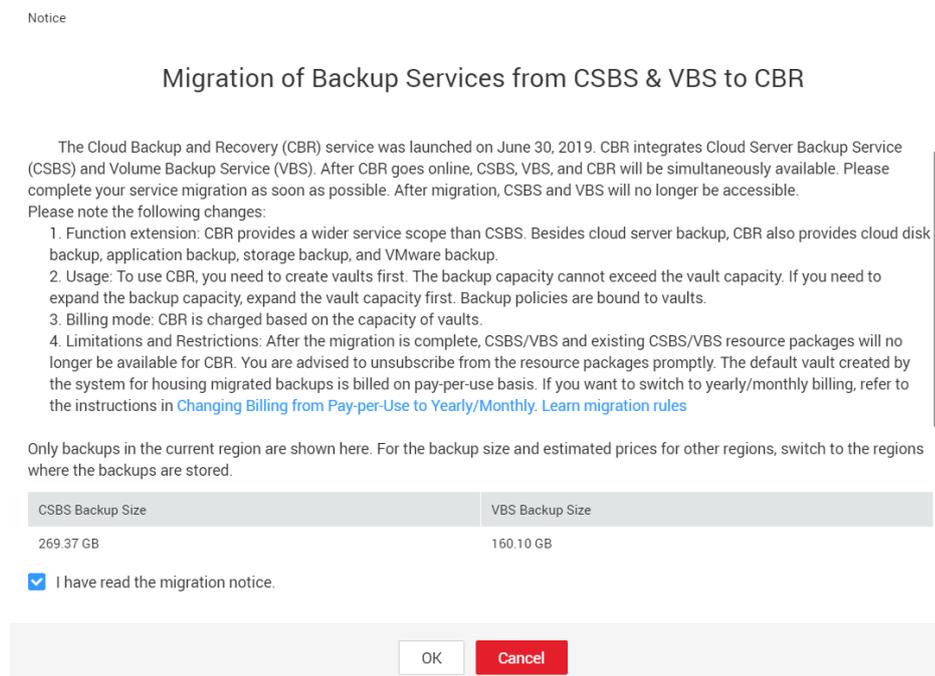
Procedimiento

Paso 1 Inicie sesión en la consola de CBR.

1. **Inicie sesión en la consola de gestión.**
2. Haga clic en  en la esquina superior izquierda y seleccione su región y proyecto.
3. Elija **Storage > Cloud Backup and Recovery**. Elija el tipo de copia de respaldo deseado en el panel de navegación izquierdo.

Paso 2 Haga clic en **Migrate to CBR** en la esquina superior derecha. Lea el contenido del cuadro de diálogo mostrado y haga clic en **OK**. Consulte **Figura 8-1**.

Figura 8-1 Migración de recursos a CBR



Paso 3 El sistema migrará automáticamente los recursos. Después de la migración, se creará un almacén denominado **default** y se mostrará un mensaje en la parte superior de la página indicando que la migración se ha realizado correctamente.

----Fin

Preguntas frecuentes

1. ¿Por qué se muestran las copias de respaldo de CBR en la consola VBS?
Si ha migrado datos de CSBS y VBS a CBR y ha creado una copia de respaldo en la consola CBR, se generará el mismo registro de copia de respaldo en la consola VBS. Esto se debe a un mecanismo subyacente. La consola VBS muestra todas las copias de respaldo generadas por CBR, CSBS y VBS. Estas copias de respaldo no se facturarán repetidamente.
2. ¿Cómo elimino copias de respaldo de la consola VBS?

Después de migrar los datos de CSBS y VBS a CBR, las copias de respaldo mostradas en la Consola VBS no se pueden eliminar solas. Encuentre estas copias de respaldo en CBR y elimínelas. A continuación, las copias de respaldo también se eliminarán de la consola VBS.

3. ¿Cuáles son las diferencias entre CBR, CSBS y VBS?

CBR integra CSBS y VBS. Además, CBR soporta copia de respaldo de SFS Turbo y copia de respaldo en la nube híbrida. El uso y la facturación de CBR también son diferentes de CSBS y VBS.

4. ¿Qué puedo hacer si se muestra un mensaje que indica que un recurso ha sido vinculado con CSBS o VBS?

Elija **Cloud Server Backup Service** o **Volume Backup Service** en la lista de servicios. En la consola de servicio correspondiente, compruebe si hay recursos vinculados a directivas en la pestaña **Policies**. Si es así, desvincule los recursos de la política y vaya a Consola de CBR para asociar los recursos a un almacén.

9 Gestión de tareas

En esta sección se describe cómo ver las tareas. La lista de tareas muestra las tareas de copia de respaldo basadas en políticas que se han ejecutado en los últimos 30 días.

Prerrequisitos

Existe al menos una tarea fallida.

Procedimiento

Paso 1 Inicie sesión en la consola CBR.

1. Inicie sesión en la consola de gestión.
2. Haga clic en  en la esquina superior izquierda y seleccione su región y proyecto.
3. Elija **Storage > Cloud Backup and Recovery > Tasks**.

Paso 2 Puede filtrar tareas por proyecto de empresa, tipo de tarea, estado de tarea, identificador de tarea, identificador de recurso, nombre de recurso, identificador de almacén, nombre de almacén y hora.

Paso 3 Haga clic en  delante de la tarea para ver los detalles de la tarea.

Si una tarea falla, puede ver la causa del error en los detalles de la tarea.

----Fin

10 Monitoreo

10.1 Métricas de CBR

Escenarios

Esta sección describe las métricas reportadas por CBR, así como sus espacios de nombres y dimensiones. Puede usar la consola o [APIs](#) que proporciona Cloud Eye para consultar las métricas generadas para CBR.

Espacio de nombres

SYS.CBR

Métricas

Tabla 10-1 Métricas de CBR

ID de métrica	Nombre de la métrica	Descripción	Rango de valores	Objeto monitoreado	Período de monitoreo (datos brutos)
used_vault_size	Used Vault Size	Capacidad utilizada del almacén Unidad: GB	≥ 0	Vault	15 min
vault_util	Vault Usage	Uso de la capacidad del almacén	0~100%	Vault	15 min

Dimensiones

Clave	Valor
instance_id	Vault name/ID

Consulta de estadísticas de monitoreo

Paso 1 Inicie sesión en la consola de gestión.

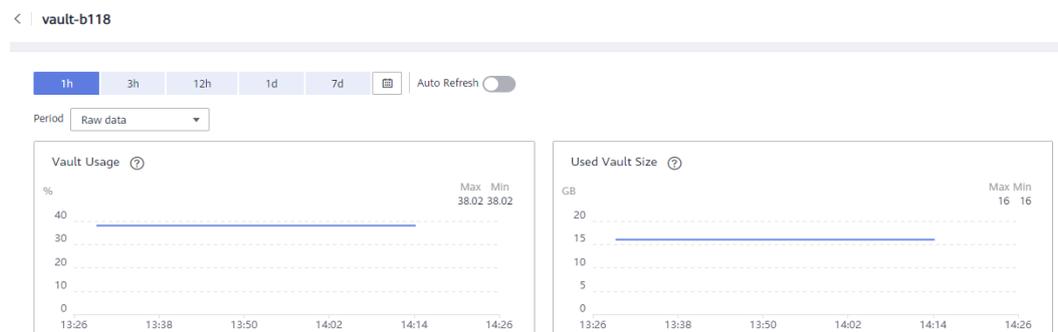
Paso 2 Vea los gráficos de supervisión utilizando cualquiera de los siguientes métodos.

- Método 1: Elija **Storage > Cloud Backup and Recovery**. En la lista de almacén, busque el almacén cuyos datos de supervisión desea ver y elija **More > View Monitoring Data** en la columna **Operation**.
- Método 2: Elija **Management & Governance > Cloud Eye > Cloud Service Monitoring > Cloud Backup and Recovery**. En la lista del almacén, haga clic en **View Metric** en la columna **Operation** del almacén cuyos datos de supervisión desea ver.

Paso 3 Puede ver los datos de supervisión del almacén por métrica o duración supervisada.

Figura 10-1 muestra los gráficos de monitorización. Para obtener más información, consulte la *Guía de usuario de Cloud Eye*.

Figura 10-1 Gráficos de supervisión de almacén



---Fin

10.2 Creación de una regla de alarma

Esta sección describe cómo crear una regla de alarma para CBR.

La copia de respaldo en la nube híbrida solo permite supervisar la capacidad del almacén. No se pueden supervisar las operaciones y los eventos locales.

Procedimiento

1. Inicie sesión en la consola de gestión.
2. En **Management & Governance**, seleccione **Cloud Eye**. En el panel de navegación de la izquierda, elija **Alarm Management > Alarm Rules**.
3. En la página mostrada, haga clic en **Create Alarm Rule** en la esquina superior derecha.

4. En el cuadro de diálogo **Create Alarm Rule**, establezca los parámetros.
 - a. Establecer **Name** y **Description**.

Tabla 10-2 Parámetros para configurar el nombre y la descripción de la regla

Parámetro	Descripción	Valor de ejemplo
Name	Nombre de la regla de alarma. El sistema genera un nombre aleatorio, que puede modificar.	alarm-cgnw
Descripción	Descripción de la regla de alarma. Este parámetro es opcional.	-

- b. Establezca los parámetros de contenido de alarma.
- c. Configure la notificación de alarma.

Tabla 10-3 Parámetros para configurar la notificación de alarma

Parámetro	Descripción	Valor de ejemplo
Alarm Notification	Especifica si se debe notificar a los usuarios cuando se activan las alarmas. Las notificaciones se pueden enviar por correo electrónico o mensaje de texto, o mediante solicitud HTTP/HTTPS a los servidores. Puede activar (recomendado) o desactivar Alarm Notification .	-
Validity Period	Cloud Eye envía notificaciones solo dentro del período de validez especificado en la regla de alarma. Por ejemplo, si Validity Period se establece en 00:00-8:00 , Cloud Eye envía notificaciones solo entre las 00:00-8:00.	-
Notification Object	Especifica el nombre del tema al que se va a enviar la notificación de alarma. Si habilita la notificación de alarma, debe seleccionar un tema. Si no hay temas deseables disponibles, primero debe crear uno, después de lo cual se invoca el servicio SMN. Para obtener más información sobre cómo crear un tema, consulte la <i>Guía de usuario de Simple Message Notification</i> .	-
Trigger Condition	Especifica la condición para activar la notificación de alarma. Puede seleccionar Generated alarm , Cleared alarm , o ambas.	-

- d. Haga clic en **Create**.

Una vez creada la regla de alarma, si los datos de métrica alcanzan el umbral especificado o ocurre un evento CBR, Cloud Eye le informa inmediatamente de que se ha producido una excepción. Para obtener más información, consulte la *Guía de usuario de Cloud Eye*.

11 Auditoría

Puede usar Cloud Trace Service (CTS) para rastrear operaciones en CBR.

Prerrequisitos

Se ha habilitado el CTS.

Operaciones clave registradas por CTS

Tabla 11-1 Operaciones de CBR que pueden ser registradas por CTS

Operación	Tipo de recurso	Nombre de seguimiento
Creación de una política	política	createPolicy
Actualización de una política	política	updatePolicy
Eliminación de una política	política	deletePolicy
Configuración de una política de almacén	almacén	associatePolicy
Eliminación de una política de una almacén	almacén	dissociatePolicy
Creación de un almacén	almacén	createVault
Modificación de un almacén	almacén	updateVault
Eliminación de una almacén	almacén	deleteVault
Eliminación de recursos	almacén	removeResources
Adición de recursos	almacén	addResources
Realización de una replicación	almacén	replicateVaultBackup
Realizar una copia de respaldo	almacén	createVaultBackup

Operación	Tipo de recurso	Nombre de seguimiento
Creación de una copia de respaldo	Copia de respaldo	createBackup
Eliminación de una copia de respaldo	Copia de respaldo	deleteBackup
Sincronización de una copia de respaldo	Copia de respaldo	syncBackup
Restauración de una copia de respaldo	Copia de respaldo	restoreBackup
Replicación de respaldo	Copia de respaldo	replicateBackup

Consulta de registros de auditoría

Para ver los registros de auditoría, consulte la sección "Consultar seguimientos en tiempo real" en la *Guía de usuario de Cloud Trace Service*.

Desactivación o habilitación de un rastreador

El siguiente procedimiento ilustra cómo deshabilitar un rastreador existente en la consola CTS. Después de deshabilitar el rastreador, el sistema detendrá las operaciones de grabación, pero aún puede ver los registros de operaciones existentes.

- Paso 1** Inicie sesión en la consola de gestión.
- Paso 2** En la esquina superior izquierda de la página, haga clic  y seleccione la región y el proyecto deseados.
- Paso 3** Haga clic en **Service List** y elija **Management & Governance > Cloud Trace Service**.
- Paso 4** Haga clic en **Trackers** en el panel de navegación izquierdo.
- Paso 5** En la lista de rastreadores, haga clic en **Disable** en la columna **Operation**.
- Paso 6** Haga clic en **Yes**.
- Paso 7** Después de deshabilitar el rastreador, la operación disponible cambia de **Disable** a **Enable**. Para volver a habilitar el rastreador, haga clic en **Enable** y, a continuación, haga clic en **Yes**. El sistema comenzará de nuevo las operaciones de grabación.

----Fin

12 Cuotas

¿Qué es una cuota?

Las cuotas pueden limitar el número o la cantidad de recursos disponibles para los usuarios, como el número máximo de ECS o discos EVS que se pueden crear.

Si la cuota de recursos existente no puede cumplir con los requisitos de servicio, puede solicitar una cuota más alta.

¿Cómo puedo ver mis cuotas?

1. Inicie sesión en la consola de gestión.
2. Haga clic  en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. En la esquina superior derecha de la página, seleccione **Resources > My Quotas**. Se muestra la página **Service Quota**.

Figura 12-1 Mis cuotas



4. Vea la cuota usada y total de cada tipo de recursos en la página mostrada. Si una cuota no puede cumplir con los requisitos de servicio, solicite una cuota más alta.

¿Cómo solicito una cuota más alta?

1. Inicie sesión en la consola de gestión.

2. En la esquina superior derecha de la página, seleccione **Resources > My Quotas**.
Se muestra la página **Service Quota**.

Figura 12-2 Mis cuotas



3. Haga clic en **Increase Quota**.
4. En la página **Create Service Ticket**, configure los parámetros según sea necesario.
En el área **Problem Description**, rellene el contenido y el motivo del ajuste.
5. Después de configurar todos los parámetros necesarios, seleccione **I have read and agree to the Tenant Authorization Letter and Privacy Statement** y haga clic en **Submit**.

A Apéndice

A.1 Mantenimiento de la seguridad del agente

A.1.1 Cambiar la contraseña del usuario rdadmin

Escenarios

- Para fines de seguridad de O&M, se recomienda cambiar la contraseña del usuario **rdadmin** del sistema operativo del agente regularmente y desactivar el permiso de inicio de sesión remoto de este usuario.
- En Linux, el usuario **rdadmin** no tiene contraseña.
- Esta sección describe cómo cambiar la contraseña del usuario **rdadmin** en Windows 2012. Para otras versiones, cambie la contraseña de acuerdo con la situación real.

Prerrequisitos

- Ha obtenido un nombre de usuario y su contraseña para iniciar sesión en la consola de gestión.
- Se han obtenido el nombre de usuario y la contraseña para iniciar sesión en un ECS de Windows.

Procedimiento

- Paso 1** Vaya a la consola de ECS e inicie sesión en Windows ECS.
- Paso 2** Haga clic en **Start > Control Panel**. En la ventana **Control Panel**, haga clic en **User Accounts**.
- Paso 3** Haga clic en **User Accounts**. Aparece el cuadro de diálogo **User Account Control**. Seleccione **rdadmin** y haga clic en **Reset Password**.
- Paso 4** Ingrese la nueva contraseña y haga clic en **OK**.
- Paso 5** En **Task Manager**, haga clic en la pestaña **Services** y, a continuación, haga clic en **Open Service**.

Paso 6 Seleccione RdMonitor y RdNginx respectivamente. En el cuadro de diálogo que aparece, seleccione **Login**, cambie la contraseña a la introducida en el [paso 4](#) y haga clic en **OK**.

---Fin

A.1.2 Cambio de la Contraseña de la Cuenta para Reportar Alarmas (SNMP v3)

Para mejorar la seguridad del sistema O&M, se recomienda cambiar la contraseña de la cuenta para informar de alarmas.

Prerrequisitos

- Ha obtenido un nombre de usuario y su contraseña para iniciar sesión en la consola de gestión.
- Se ha obtenido el nombre de usuario y la contraseña para iniciar sesión en un servidor.

Contexto

Esta sección presenta los procedimientos en Windows y Linux.

AVISO

Si la contraseña de autenticación y la contraseña de encriptación de datos para SNMP v3 del Agente son iguales, existen riesgos de seguridad. Para garantizar la seguridad del sistema, se recomienda establecer diferentes contraseñas para la autenticación y el encriptación de datos.

Obtenga la contraseña de autenticación inicial del soporte técnico.

NOTA

La contraseña debe cumplir los siguientes requisitos de complejidad:

- Debe contener de 8 a 16 caracteres.
- Contiene al menos uno de los siguientes caracteres especiales: `~!@#%&*()_-+=\|[]{};:","<>/?
- Contiene al menos dos de los siguientes tipos de caracteres:
 - Letras en mayúscula
 - Letras en minúscula
 - Caracteres numéricos
- No puede ser el mismo que el nombre de usuario o el nombre de usuario en orden inverso.
- No puede ser lo mismo que las contraseñas antiguas.
- No puede contener espacios.

Procedimiento (Windows)

Paso 1 Inicie sesión en el servidor donde está instalado el Agente.

Paso 2 Abra la CLI y vaya al directorio de *installation path*\bin.

Paso 3 Ejecute el comando **agentcli.exe chgsnmp**. Escriba la contraseña de inicio de sesión del Agente y pulse **Enter**.

```
Please choose operation:
1: Change authentication password
2: Change private password
3: Change authentication protocol
4: Change private protocol
5: Change security name
6: Change security Level
7: Change security model
8: Change context engine ID
9: Change context name
Other: Quit
Please choose:
```

 **NOTA**

admin es el nombre de usuario configurado durante la instalación del Agente.

Paso 4 Seleccione el SN de la contraseña de autorización o la contraseña de encriptación de datos que desea cambiar y pulse **Enter**.

Paso 5 Escriba la contraseña anterior y pulse **Enter**.

Paso 6 Escriba una nueva contraseña y pulse **Enter**.

Paso 7 Vuelva a escribir la nueva contraseña y presione **Enter**. La contraseña fue cambiada.

----Fin

Procedimiento (Linux)

Paso 1 Inicie sesión en el servidor Linux con la contraseña del servidor.

Paso 2 Ejecute el comando **TMOUT=0** para evitar que PuTTY salga debido al tiempo de espera de la sesión.

 **NOTA**

Después de ejecutar el comando anterior, el sistema permanece en ejecución incluso cuando no se realiza ninguna operación, lo que da como resultado riesgos de seguridad. Por motivos de seguridad, ejecute el comando **exit** para salir del sistema después de finalizar las operaciones.

Paso 3 Ejecute el comando **su - rdadmin** para cambiar al usuario **rdadmin**.

Paso 4 Ejecute el comando **/home/rdadmin/Agent/bin/agentcli chgsnmp**. Escriba la contraseña de inicio de sesión del Agente y pulse **Enter**.

 **NOTA**

La ruta de instalación del Agente es **/home/rdadmin/Agent**.

```
Please choose operation:
1: Change authentication password
2: Change private password
3: Change authentication protocol
4: Change private protocol
5: Change security name
6: Change security Level
7: Change security model
8: Change context engine ID
9: Change context name
Other: Quit
Please choose:
```

Paso 5 Seleccione el SN de la contraseña de autorización o la contraseña de encriptación de datos que desea cambiar y pulse **Enter**.

Paso 6 Escriba la contraseña anterior y pulse **Enter**.

Paso 7 Escriba una nueva contraseña y pulse **Enter**.

Paso 8 Vuelva a escribir la nueva contraseña y presione **Enter**. La contraseña fue cambiada.

---Fin

A.1.3 Sustitución del certificado de servidor

Por motivos de seguridad, es posible que desee utilizar un certificado Secure Socket Layer (SSL) emitido por una entidad emisora de certificados de terceros. El Agente le permite reemplazar los certificados de autenticación y los archivos de clave privada siempre que proporcione los certificados de autenticación y los pares de claves privada-pública. La actualización del certificado solo puede surtir efecto después de reiniciar el Agente, por lo que se recomienda actualizar el certificado durante las horas no pico.

Prerrequisitos

- Ha obtenido un nombre de usuario y su contraseña para iniciar sesión en la consola de gestión.
- Se ha obtenido el nombre de usuario y la contraseña para iniciar sesión en un servidor.
- Se han obtenido nuevos certificados en formato X.509v3.

Contexto

- El agente se implementa previamente con el certificado de CA del agente **bcmagentca**, el archivo de clave privada del certificado de CA **server.key**, y el certificado de autenticación **server.crt**. Todos estos archivos se guardan en **/home/rdadmin/Agent/bin/nginx/conf** (si usa Linux) o **\bin\nginx\conf** (si usa Windows).
- Debe reiniciar el Agente después de reemplazar un certificado para que el certificado sea efectivo.

Procedimiento (Linux)

Paso 1 Inicie sesión en el servidor Linux con el Agente instalado.

Paso 2 Ejecute el comando **TMOU=0** para evitar que PuTTY salga debido al tiempo de espera de la sesión.

NOTA

Después de ejecutar el comando anterior, el sistema permanece en ejecución incluso cuando no se realiza ninguna operación, lo que da como resultado riesgos de seguridad. Por motivos de seguridad, ejecute el comando **exit** para salir del sistema después de finalizar las operaciones.

Paso 3 Ejecute el comando **su - rdadmin** para cambiar al usuario **rdadmin**.

Paso 4 Ejecute el comando **cd /home/rdadmin/Agent/bin** para ir a la ruta del script.

NOTA

La ruta de instalación del Agente es **/home/rdadmin/Agent**.

Paso 5 Ejecute el comando **sh agent_stop.sh** para detener la ejecución del agente.

Paso 6 Coloque los nuevos certificados y archivos de clave privada en el directorio especificado.

 **NOTA**

Coloque nuevos certificados en el directorio `/home/rdadmin/Agent/bin/nginx/conf`.

Paso 7 Ejecute el comando `/home/rdadmin/Agent/bin/agentcli chgkey`.

Se muestra la siguiente información:

```
Enter password of admin:
```

 **NOTA**

`admin` es el nombre de usuario configurado durante la instalación del Agente.

Paso 8 Escriba la contraseña de inicio de sesión del Agente y pulse **Enter**.

Se muestra la siguiente información:

```
Change certificate file name:
```

Paso 9 Introduzca un nombre para el nuevo certificado y pulse **Enter**.

 **NOTA**

Si la clave privada y el certificado son el mismo archivo, los nombres de la clave privada y el certificado son idénticos.

Se muestra la siguiente información:

```
Change certificate key file name:
```

Paso 10 Escriba un nombre para el nuevo archivo de clave privada y pulse **Enter**.

Se muestra la siguiente información:

```
Enter new password:
```

```
Enter the new password again:
```

Paso 11 Introduzca dos veces la contraseña de protección del archivo de clave privada. El certificado se sustituye correctamente.

Paso 12 Ejecute el comando `sh agent_start.sh` para iniciar el agente.

---Fin

Procedimiento (Windows)

Paso 1 Inicie sesión en el servidor de Windows con el Agente instalado.

Paso 2 Abra la CLI y vaya al directorio de `installation path\bin`.

Paso 3 Ejecute el comando `agent_stop.bat` para detener la ejecución del agente.

Paso 4 Coloque los nuevos certificados y archivos de clave privada en el directorio especificado.

 **NOTA**

Coloque nuevos certificados en el directorio de `installation path\bin\nginx\conf`.

Paso 5 Ejecute el comando `agentcli.exe chgkey`.

Se muestra la siguiente información:

```
Enter password of admin:
```

 **NOTA**

admin es el nombre de usuario configurado durante la instalación del Agente.

Paso 6 Introduzca un nombre para el nuevo certificado y pulse **Enter**.

 **NOTA**

Si la clave privada y el certificado son el mismo archivo, los nombres de la clave privada y el certificado son idénticos.

Se muestra la siguiente información:

```
Change certificate key file name:
```

Paso 7 Escriba un nombre para el nuevo archivo de clave privada y pulse **Enter**.

Se muestra la siguiente información:

```
Enter new password:
```

```
Enter the new password again:
```

Paso 8 Introduzca dos veces la contraseña de protección del archivo de clave privada. El certificado se sustituye correctamente.

Paso 9 Ejecute el comando **agent_start.bat** para iniciar el agente.

----Fin

A.1.4 Sustitución de certificados de CA

Escenarios

Un certificado de CA es un archivo digital firmado y emitido por una autoridad de autenticación. Contiene la clave pública, información sobre el propietario de la clave pública, información sobre el emisor, período de validez y cierta información de extensión. Se utiliza para configurar un canal de transferencia de información seguro entre el Agente y el servidor.

Si el certificado de CA no cumple con los requisitos de seguridad o ha caducado, reemplácelo por motivos de seguridad.

Prerrequisitos

- Se han obtenido el nombre de usuario y la contraseña para iniciar sesión en un ECS.
- Un nuevo certificado de CA está listo.

Procedimiento (Linux)

Paso 1 Inicie sesión en el servidor Linux con el Agente instalado.

Paso 2 Ejecute el siguiente comando para evitar el cierre de sesión debido al tiempo de espera del sistema:

```
TMOUT=0
```

Paso 3 Ejecute el siguiente comando para cambiar al usuario **rdadmin**:

```
su - rdadmin
```

Paso 4 Ejecute el siguiente comando para ir a la ruta de acceso al script de start/stop del agente:

```
cd /home/rdadmin/Agent/bin
```

Paso 5 Ejecute el siguiente comando para detener la ejecución del agente:

```
sh agent_stop.sh
```

Paso 6 Ejecute el siguiente comando para ir a la ruta de acceso al certificado de CA:

```
cd /home/rdadmin/Agent/bin/nginx/conf
```

Paso 7 Ejecute el siguiente comando para eliminar el certificado de CA existente:

```
rm bcmagentca.crt
```

Paso 8 Copie el nuevo archivo de certificado de CA en el directorio `/home/rdadmin/Agent/bin/nginx/conf` y cambie el nombre del archivo `bcmagentca.crt`.

Paso 9 Ejecute el siguiente comando para cambiar el propietario del certificado de CA:

```
chown rdadmin:rdadmin bcmagentca.crt
```

Paso 10 Ejecute el siguiente comando para modificar los permisos del certificado de CA:

```
chmod 400 bcmagentca.crt
```

Paso 11 Ejecute el siguiente comando para ir a la ruta de acceso al script de start/stop del agente:

```
cd /home/rdadmin/Agent/bin
```

Paso 12 Ejecute el siguiente comando para iniciar el Agente:

```
sh agent_start.sh
```

----Fin

Procedimiento (Windows)

Paso 1 Inicie sesión en el ECS con el Agente instalado.

Paso 2 Vaya al directorio `Installation path\bin`.

Paso 3 Ejecute el script `agent_stop.bat` para detener el agente.

Paso 4 Vaya al directorio `Installation path\nnginx\conf`.

Paso 5 Elimine el archivo de certificado `bcmagentca.crt`.

Paso 6 Copie el nuevo archivo de certificado de CA en el directorio `Installation path\nnginx\conf` y cambie el nombre del archivo `bcmagentca.crt`.

Paso 7 Vaya al directorio `Installation path\bin`.

Paso 8 Ejecute el script `agent_start.bat` para iniciar el agente.

----Fin

A.2 Historial de cambios

Lanzado en	Descripción
2022-11-21	Esta versión es el séptimo lanzamiento oficial, que incorpora el siguiente cambio: Agregó una restricción en la copia de respaldo de archivos.
2022-07-20	Esta versión es el sexto lanzamiento oficial, que incorpora los siguientes cambios: Agregó el contenido de la copia de respaldo de archivos.
2021-10-27	Esta versión es el quinto lanzamiento oficial, que incorpora el siguiente cambio: Agregó el contenido de la gestión de permisos.
2020-04-08	Esta versión es el cuarto lanzamiento oficial, que incorpora el siguiente cambio: Agregó el contenido de la copia de respaldo del sistema de archivos.
2020-02-25	Esta versión es la tercera versión oficial, que incorpora el siguiente cambio: Se trasladó la sección "Hybrid Cloud Backup" a una nueva documentación titulada <i>Hybrid Cloud Backup Feature Guide</i> .
2019-08-27	Esta versión es el segundo lanzamiento oficial, que incorpora el siguiente cambio: <ul style="list-style-type: none">● Se suprimió la descripción sobre la replicación entre regiones y la copia de respaldo de BMS.
2019-07-31	Esta versión es el primer lanzamiento oficial.