

Cloud Container Engine

FAQs

Edición 01
Fecha 2023-08-02



Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2023. 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 HUAWEI y otras marcas registradas de Huawei pertenecen a Huawei Technologies Co., Ltd. Todas las demás marcas registradas y los otros nombres comerciales mencionados en este documento son propiedad de sus respectivos titulares.

Aviso

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

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

Huawei Cloud Computing Technologies Co., Ltd.

Dirección: Huawei Cloud Data Center Jiaoxinggong Road
Avenida Qianzhong
Nuevo distrito de Gui'an
Gui Zhou, 550029
República Popular China

Sitio web: <https://www.huaweicloud.com/intl/es-us/>

Índice

1 Preguntas frecuentes.....	1
2 Facturación.....	2
2.1 ¿Cómo se factura/cobra la CCE?.....	2
2.2 ¿Cómo cambio el modo de facturación de un clúster de CCE de pago por uso a anual/mensual?.....	4
2.3 ¿Puedo cambiar el modo de facturación de los nodos de CCE de pago por uso a anual/mensual?.....	5
2.4 ¿Qué modos de factura son compatibles con Huawei Cloud?.....	6
2.5 ¿Se me notificará cuando mi saldo sea insuficiente?.....	6
2.6 ¿Se me notificará cuando cambie el saldo de mi cuenta?.....	7
2.7 ¿Puedo eliminar un clúster de CCE facturado anual/mensualmente directamente cuando expire?.....	7
2.8 ¿Cómo puedo cancelar mi suscripción a CCE?.....	7
2.9 ¿Se admite el reembolso de CCE?.....	8
3 Clúster.....	9
3.1 Creación de clústeres.....	9
3.1.1 ¿Por qué no puedo crear un clúster de CCE?.....	9
3.1.2 ¿La escala de gestión de un clúster está relacionada con el número de nodos principales?.....	10
3.1.3 ¿Cómo actualizo el certificado raíz al crear un clúster de CCE?.....	10
3.1.4 ¿A qué cuotas de recursos debo prestar atención al usar CCE?.....	11
3.2 Ejecución de clúster.....	12
3.2.1 ¿Cómo puedo rectificar la falla cuando el estado del clúster no está disponible?.....	12
3.2.2 ¿Cómo puedo restablecer o reinstalar un clúster de CCE?.....	13
3.2.3 ¿Cómo puedo comprobar si un clúster está en modo multimaestro?.....	14
3.2.4 ¿Puedo conectarme directamente al nodo maestro de un clúster?.....	14
3.2.5 ¿Cómo puedo recuperar datos después de eliminar un clúster?.....	14
3.2.6 ¿Cómo actualizo un espacio de nombres en estado Terminating?.....	14
3.2.7 ¿Por qué el uso del disco del nodo de visualización de CCE es incompatible con Cloud Eye?.....	16
3.3 Eliminación de clústeres.....	17
3.3.1 Error al eliminar un clúster: ENI residuales.....	17
3.4 Actualización de clúster.....	18
3.4.1 ¿Qué hago si un complemento de clúster no se actualiza durante la actualización del clúster de CCE?.....	19
4 Nodo.....	22
4.1 Creación de nodos.....	22
4.1.1 ¿Cómo soluciono los problemas que se producen al agregar nodos a un clúster de CCE?.....	22

4.1.2	¿Cómo soluciono los problemas que se producen al aceptar nodos en un clúster de CCE?	26
4.1.3	¿Qué debo hacer si un nodo no se acepta porque no se instala?	27
4.2	Ejecución de nodo	27
4.2.1	¿Qué debo hacer si un clúster está disponible pero algunos nodos no están disponibles?	28
4.2.2	¿Cómo soluciono los problemas de la falla al iniciar sesión de forma remota en un nodo en un clúster de CCE?	34
4.2.3	¿Cómo inicio sesión en un nodo usando una contraseña y restablezco la contraseña?	35
4.2.4	¿Cómo puedo recopilar logs de nodos en un clúster de CCE?	35
4.2.5	¿Qué puedo hacer si la red de contenedores no está disponible después de actualizar el sistema operativo?	36
4.2.6	¿Qué debo hacer si el disco vdb de un nodo está dañado y el nodo no se puede recuperar después del restablecimiento?	37
4.2.7	¿Qué puertos se utilizan para instalar kubelet en los nodos del clúster de CCE?	38
4.2.8	¿Cómo configuro un pod para usar la capacidad de aceleración de un nodo de GPU?	38
4.2.9	¿Qué debo hacer si la suspensión de E/S ocurre ocasionalmente cuando se usan discos SCSI de EVS?	39
4.2.10	¿Qué debo hacer si los logs excesivos de auditoría de Docker afectan a la E/S del disco?	40
4.2.11	¿Cómo soluciono un contenedor o nodo anormal debido a que no hay espacio en disco de thin pool?	41
4.2.12	¿En qué puertos escucha un nodo?	42
4.2.13	¿Cómo puedo rectificar fallas cuando se utiliza el controlador de NVIDIA para iniciar contenedores en nodos de GPU?	45
4.3	Cambio de especificaciones	46
4.3.1	¿Cómo cambio las especificaciones de nodo en un clúster de CCE?	46
4.3.2	¿Qué debo hacer si no puedo reiniciar o crear cargas de trabajo en un nodo después de modificar las especificaciones del nodo?	47
4.3.3	¿Puedo cambiar la dirección IP de un nodo en un clúster de CCE?	47
4.4	Núcleo de nodos	48
4.4.1	Cuando las aplicaciones se crean y eliminan repetidamente en un nodo de CentOS con una versión de kernel anterior, se produce una fuga de cgroup Kmem de vez en cuando	49
4.4.2	Problemas causados por la configuración conn_reuse_mode en el modo de reenvío IPVS de clústeres de CCE	49
4.4.3	¿Por qué los pods son desalojados por kubelet debido a estadísticas anormales de cgroup?	51
4.4.4	Cuando se produce OOM del contenedor en el nodo de CentOS con una versión anterior del kernel, el sistema de archivos Ext4 se suspende ocasionalmente	52
5	Grupo de nodos	53
5.1	¿Qué debo hacer si no se muestra ningún registro de creación de nodos cuando se está expandiendo el grupo de nodos?	53
6	Carga de trabajo	54
6.1	Anomalías de la carga de trabajo	54
6.1.1	¿Cómo uso eventos para corregir cargas de trabajo anormales?	54
6.1.2	¿Qué debo hacer si falla la programación de pods?	56
6.1.3	¿Qué debo hacer si un pod no logra extraer la imagen?	62
6.1.4	¿Qué debo hacer si falla el inicio del contenedor?	70
6.1.5	¿Qué debo hacer si un pod no es desalojado?	76
6.1.6	¿Qué debo hacer si no se puede montar un volumen de almacenamiento o si el tiempo de montaje se agota?	80
6.1.7	¿Qué debo hacer si una carga de trabajo permanece en el estado de creación?	82

6.1.8 ¿Qué debo hacer si no se pueden eliminar los pods en el estado de terminación?.....	82
6.1.9 ¿Qué debo hacer si una carga de trabajo se detiene debido a la eliminación de pods?.....	83
6.1.10 ¿Qué debo hacer si se produce un error al desplegar un servicio en el nodo de GPU?.....	84
6.1.11 ¿Qué debo hacer si se notifican los errores relacionados con sandbox cuando el pod permanece en el estado de creación?.....	85
6.1.12 ¿Por qué el pod no escribe datos?.....	85
6.1.13 ¿Por qué se suspende la creación o eliminación de pods en un nodo donde está montado el almacenamiento de archivos?.....	86
6.1.14 Códigos de salida.....	87
6.2 Configuración del contenedor.....	91
6.2.1 ¿Cuándo se utiliza el procesamiento previo a la parada?.....	91
6.2.2 ¿Cómo configuro un FQDN para acceder a un contenedor especificado en el mismo espacio de nombres?.....	91
6.2.3 ¿Qué debo hacer si las sondas de chequeo médico fallan ocasionalmente?.....	92
6.2.4 ¿Cómo configuro el valor umask para un contenedor?.....	92
6.2.5 ¿Qué puedo hacer si se informa de un error cuando se inicia un contenedor desplegado después de que se especifique el parámetro de memoria de pila de inicio de JVM para ENTRYPOINT en Dockerfile?.....	93
6.2.6 ¿Qué es el mecanismo de reintento cuando CCE no puede iniciar un pod?.....	93
6.3 Monitoreo de alarmas.....	94
6.3.1 ¿Durante cuánto tiempo se almacenan los eventos de una carga de trabajo?.....	94
6.4 Políticas de planificación.....	94
6.4.1 ¿Cómo distribuyo uniformemente varios pods a cada nodo?.....	94
6.4.2 ¿Cómo puedo evitar que un contenedor en un nodo sea desalojado?.....	95
6.4.3 ¿Por qué los pods no se distribuyen uniformemente a los nodos?.....	96
6.4.4 ¿Cómo desalojo todos los pods de un nodo?.....	96
6.5 Otros.....	97
6.5.1 ¿Qué debo hacer si no se puede reiniciar una tarea programada después de haber sido detenida durante un período de tiempo?.....	97
6.5.2 ¿Qué es un servicio sin cabeza cuando creo un StatefulSet?.....	98
6.5.3 ¿Qué debo hacer si se muestra un mensaje de error "Auth is empty" cuando se extrae una imagen privada?.....	99
6.5.4 ¿Por qué no se puede programar un pod en un nodo?.....	100
6.5.5 ¿Qué es la política de extracción de imágenes para contenedores en un clúster de CCE?.....	100
6.5.6 ¿Por qué está desinstalado el punto de montaje de un contenedor Docker en el clúster Kunpeng?.....	100
6.5.7 ¿Qué puedo hacer si falta una capa durante la extracción de imágenes?.....	101
6.5.8 ¿Por qué el permiso de archivo y el usuario en el contenedor son signos de interrogación?.....	102
7 Redes.....	105
7.1 Planificación de la red.....	105
7.1.1 ¿Cuál es la relación entre clústeres, VPC y subredes?.....	105
7.1.2 ¿Cómo puedo ver el bloque CIDR de VPC?.....	106
7.1.3 ¿Cómo configuro el bloque CIDR de VPC y el bloque CIDR de subred para un clúster de CCE?.....	106
7.1.4 ¿Cómo configuro un bloque CIDR de contenedores para un clúster de CCE?.....	107
7.1.5 ¿Cuándo debo usar la red nativa en la nube 2.0?.....	108
7.1.6 ¿Qué es la ENI?.....	109
7.1.7 Configuración de reglas de grupo de seguridad de clúster.....	110

7.1.8 ¿Cómo configuro un bloque CIDR de servicio IPv6?.....	116
7.2 Network Fault.....	118
7.2.1 ¿Cómo se localiza una falla de red de carga de trabajo?.....	118
7.2.2 ¿Por qué no se puede utilizar la dirección ELB para acceder a las cargas de trabajo en un clúster?.....	120
7.2.3 ¿Por qué no se puede acceder al ingreso fuera del clúster?.....	123
7.2.4 ¿Por qué el navegador devuelve el código de error 404 cuando accedo a una aplicación desplegada?.....	129
7.2.5 ¿Qué debo hacer si un contenedor no se conecta a Internet?.....	130
7.2.6 ¿Qué puedo hacer si no se puede eliminar una subred de VPC?.....	130
7.2.7 ¿Cómo puedo restaurar una NIC de contenedor defectuosa?.....	131
7.2.8 ¿Qué debo hacer si un nodo no se conecta a Internet (red pública)?.....	131
7.2.9 ¿Cómo resuelvo un conflicto entre el bloque CIDR de VPC y el bloque CIDR de contenedores?.....	132
7.2.10 ¿Qué debo hacer si se reporta el error de Java "Connection reset by peer" durante la comprobación de estado de la capa 4 de ELB?.....	132
7.2.11 ¿Cómo localizo el evento de servicio que indica que ningún nodo está disponible para el enlace?.....	133
7.2.12 ¿Por qué se produce el "Dead loop on virtual device gw_11cbf51a, fix it urgently" cuando inicio sesión en una máquina virtual usando VNC?.....	133
7.2.13 ¿Por qué ocurre un pánico ocasionalmente cuando uso políticas de red en un nodo de clúster?.....	135
7.2.14 ¿Por qué se generan muchos logs de origen ip_type en el VNC?.....	136
7.3 Resguardo de la seguridad.....	137
7.3.1 ¿Cómo puedo evitar que los nodos de clúster se expongan a las redes públicas?.....	137
7.4 Configuración de la red.....	137
7.4.1 ¿Cómo se comunica CCE con otros servicios de Huawei Cloud por una intranet?.....	138
7.4.2 ¿Cómo configuro el puerto al configurar el modo de acceso a la carga de trabajo en CCE?.....	138
7.4.3 ¿Cómo puedo lograr la compatibilidad entre la propiedad de entrada y el client-go de Kubernetes?.....	140
7.5 Otros.....	142
7.5.1 ¿Cómo obtengo un certificado de clave TLS?.....	142
7.5.2 ¿Se pueden vincular varias NIC a un nodo en un clúster de CCE?.....	144
7.5.3 ¿Por qué se elimina automáticamente el grupo de servidores backend de un ELB después de publicar un servicio en el ELB?.....	144
7.5.4 ¿Por qué no se puede crear una entrada después de cambiar el espacio de nombres?.....	145
7.5.5 ¿Cómo obtengo la dirección IP de origen real de un cliente después de agregar un servicio a Istio?.....	145
7.5.6 ¿Cómo cambio el grupo de seguridad de nodos en un clúster por lotes?.....	146
8 Almacenamiento.....	148
8.1 ¿Cuáles son las diferencias entre las clases de almacenamiento de CCE en términos de almacenamiento persistente y montaje multinodo?.....	148
8.2 ¿Puedo agregar un nodo sin un disco de datos de 100 GB?.....	149
8.3 ¿Puedo restaurar un disco de EVS utilizado como volumen persistente en un clúster de CCE después de que el disco se elimine o expire?.....	150
8.4 ¿Qué debo hacer si no se puede encontrar el host cuando se necesitan cargar archivos en OBS durante el acceso al servicio CCE desde una red pública?.....	150
8.5 ¿Cuántos nodos (ECS) se puede montar un sistema de archivos SFS?.....	151
8.6 ¿Cómo puedo lograr la compatibilidad entre ExtendPathMode y Kubernetes client-go?.....	151
8.7 ¿Qué debo hacer si no se crea un volumen de almacenamiento?.....	153
8.8 ¿Pueden los PVC de CCE detectar fallas de almacenamiento subyacentes?.....	154

9 Espacio de nombres.....	155
9.1 ¿Por qué no puedo eliminar un espacio de nombres debido a un error de acceso a objetos ApiService?.....	155
10 Gráfico y complemento.....	157
10.1 ¿Qué debo hacer si el complemento nginx-ingress no se instala en un clúster y permanece en el estado de creación?.....	157
10.2 ¿Qué debo hacer si existen recursos de procesos residuales debido a una versión anterior del complemento npd?.....	158
10.3 ¿Qué debo hacer si no se puede eliminar una versión de gráfico porque el formato del gráfico es incorrecto?.....	159
10.4 ¿CCE soporta nginx-ingress?.....	161
10.5 ¿Por qué falla la instalación del complemento y avisa "The release name is already exist"?.....	161
10.6 ¿Por qué falla la creación o la actualización de la versión y avisa "rendered manifests contain a resource that already exists"?.....	163
11 API y preguntas frecuentes de kubectl.....	165
11.1 ¿Cómo puedo acceder a un clúster de CCE?.....	165
11.2 ¿Se pueden mostrar los recursos creados con las API o kubectl en la consola de CCE?.....	165
11.3 ¿Cómo descargo kubeconfig para conectarme a un clúster usando kubectl?.....	166
11.4 ¿Cómo puedo rectificar el error notificado al ejecutar el comando kubectl top node?.....	167
11.5 ¿Por qué se muestra "Error from server (Forbidden)" cuando utilizo kubectl?.....	167
12 Preguntas frecuentes sobre DNS.....	169
12.1 ¿Qué debo hacer si falla la resolución de nombres de dominio?.....	169
12.2 ¿Por qué un contenedor en un clúster de CCE no puede realizar la resolución de DNS?.....	172
12.3 ¿Por qué no se puede resolver el nombre de dominio de la zona del tenant después de modificar la configuración de DNS de la subred?.....	173
12.4 ¿Cómo puedo optimizar la configuración si la resolución del nombre de dominio externo es lenta o se agota?....	173
12.5 ¿Cómo configuro una política de DNS para un contenedor?.....	174
13 Preguntas frecuentes sobre el repositorio de imágenes.....	176
13.1 ¿Cómo puedo crear una imagen de Docker y resolver el problema de la extracción lenta de imágenes?.....	176
13.2 ¿Cómo subo mis imágenes a CCE?.....	176
14 Permisos.....	178
14.1 ¿Puedo configurar solo los permisos de espacio de nombres sin permisos de gestión de clústeres?.....	178
14.2 ¿Puedo usar las API de CCE si los permisos de gestión de clústeres no están configurados?.....	178
14.3 ¿Puedo usar kubectl si los permisos de gestión de clústeres no están configurados?.....	179
15 Referencia.....	180
15.1 ¿Cómo puedo ampliar la capacidad de almacenamiento de un contenedor?.....	180
15.2 ¿Cómo pueden las direcciones IP de contenedores sobrevivir a un reinicio de contenedores?.....	182
15.3 ¿Cuáles son las diferencias entre CCE y CCI?.....	183
15.4 ¿Cuáles son las diferencias entre CCE y ServiceStage?.....	186

1 Preguntas frecuentes

Gestión de clústeres

- [¿Por qué no puedo crear un clúster de CCE?](#)
- [¿La escala de gestión de un clúster está relacionada con el número de nodos principales?](#)
- [¿Cómo puedo rectificar la falla cuando el estado del clúster no está disponible?](#)

Gestión de nodos/grupos de nodos

- [¿Qué debo hacer si un clúster está disponible pero algunos nodos no están disponibles?](#)
- [¿Qué debo hacer si un nodo no se acepta porque no se instala?](#)
- [¿Qué debo hacer si la suspensión de E/S ocurre ocasionalmente cuando se usan discos SCSI de EVS?](#)

Gestión de la carga de trabajo

- [¿Qué debo hacer si falla la programación de pods?](#)
- [¿Qué debo hacer si un pod no logra extraer la imagen?](#)
- [¿Qué debo hacer si falla el inicio del contenedor?](#)
- [¿Qué debo hacer si no se pueden eliminar los pods en el estado de terminación?](#)
- [¿Qué es la política de extracción de imágenes para contenedores en un clúster de CCE?](#)

Redes

[¿Por qué el navegador devuelve el código de error 404 cuando accedo a una aplicación desplegada?](#)

[¿Qué debo hacer si un nodo no se conecta a Internet \(red pública\)?](#)

[¿Cómo puedo optimizar la configuración si la resolución del nombre de dominio externo es lenta o se agota?](#)

2 Facturación

2.1 ¿Cómo se factura/cobra la CCE?

Conceptos de facturación:

Cloud Container Engine (CCE) es gratuito. Solo paga por los recursos (como los nodos) creados cuando utiliza CCE. Hay dos tipos de artículos de facturación:

1. **Clusters:** La tarifa de clúster es el costo de los recursos utilizados por los nodos principales. La tarifa varía según el tipo de clúster y el tamaño del clúster. Los tipos de clúster incluyen clúster de VM y clúster de BMS (el número de nodos principales determina si un clúster está altamente disponible). El tamaño del clúster (también llamado escala de gestión) indica el número máximo de nodos permitidos en un clúster.

NOTA

La escala de gestión indica el número de ECS o de BMS en un clúster.

Para obtener más información, consulte [Detalles de precios de CCE](#).

2. **IaaS resources:** se factura el costo de los recursos de IaaS creados para ejecutar nodos de trabajo en el clúster. Los recursos de IaaS, que se crean manualmente o automáticamente, incluyen ECS, discos de EVS, EIP, ancho de banda y balanceadores de carga.

Para obtener más información sobre los precios, consulte [Detalles de precios del producto](#).

Modos de facturación

CCE se factura sobre una base de pago por uso o anual/mensual.

- **Pago por uso:** Es un modo de pago después de uso. La facturación se inicia cuando se aprovisiona un recurso y se detiene cuando se elimina el recurso. Puede utilizar los recursos en la nube según sea necesario y dejar de pagarlos cuando ya no los necesite. No hay pago por adelantado por exceso de capacidad.

 **NOTA**

Los siguientes son principios de precios en el caso de la hibernación del clúster de CCE o el apagado del nodo. Tenga en cuenta que hay muchos tipos de nodos de clúster y ECS se utiliza como ejemplo.

- **Cluster hibernation:** después de hibernar un clúster, se detendrá la facturación de los recursos utilizados por los nodos principales.
- **Node shutdown:** la facturación del nodo del trabajador se detiene cuando se detiene el nodo. Tenga en cuenta que la hibernación de un clúster no detendrá los nodos de trabajo en el clúster. Para detener un ECS, inicie sesión en la consola de ECS. Para obtener más información, consulte [Detener un nodo](#).

Los ECS detenidos no se facturan. Para obtener más información, consulte [Facturación de ECS](#).

- **Anual/mensual:** Es un modo de pago antes de usar. La facturación anual/mensual proporciona un descuento más significativo que el pago por uso y se recomienda para el uso a largo plazo de los servicios en la nube. Cuando usted compra un paquete anual/mensual, el sistema deducirá el costo del paquete de su cuenta en la nube según las especificaciones elegidas.
- **Cambio del modo de facturación:** el modo de facturación no se puede cambiar dentro del ciclo de facturación.

AVISO

- Los clústeres siguen un plan de precios por niveles. Los precios de cada nivel varían según el tamaño y el tipo del clúster.
- Una vez que una suscripción mensual/anual ha caducado o un recurso de pago por uso está en mora, Huawei Cloud proporciona un período de tiempo durante el cual puede renovar el recurso o recargar su cuenta. Dentro del período de gracia, todavía puede acceder y utilizar su servicio en la nube. Para obtener más información, consulte [¿Qué es un período de gracia? Cuánto dura el período de gracia de Huawei Cloud. ¿Qué es un período de retención? Cuánto dura el período de retención de Huawei Cloud.](#)

Cambios de configuración

De pago por uso a facturación anual/mensual: puede cambiar el modo de facturación de clúster de pago por uso a facturación anual/mensual. Después del cambio, todos los nodos principales, nodos de trabajo y recursos en la nube (como discos de EVS y EIP) utilizados por su clúster se facturarán anualmente/mensualmente y se generará un nuevo pedido. Los nodos y los recursos en la nube estarán listos para su uso inmediatamente después de pagar el nuevo pedido.

De la facturación anual/mensual al pago por uso: los clústeres que se facturan anualmente/mensualmente no pueden cambiar a pago por uso dentro del ciclo de facturación. Tenga en cuenta que los clústeres de pago por uso se pueden eliminar directamente, pero los clústeres que se facturan anualmente/mensualmente no se pueden eliminar. Para dejar de usar los clústeres que se facturan anualmente/mensualmente, vaya al Centro de facturación y [cancele la suscripción a los mismos](#).

Notas

- Los cupones en efectivo no se devolverán después de degradar las especificaciones de los servidores en la nube que se compran con cupones en efectivo.

- Tendrá que pagar la diferencia de precio entre las especificaciones originales y nuevas después de actualizar las especificaciones del servidor en la nube.
- La reducción de las especificaciones del servidor en la nube (la cantidad de recursos de CPU o memoria) perjudicará el rendimiento del servidor en la nube.
- Si degrada las especificaciones del servidor en la nube y luego las actualiza a las especificaciones originales, todavía tendrá que pagar la diferencia de precio incurrida por la actualización.

2.2 ¿Cómo cambio el modo de facturación de un clúster de CCE de pago por uso a anual/mensual?

Actualmente, los clústeres son compatibles con los modos de facturación **pay-per-use** y **yearly/monthly**. Un clúster de pago por uso se puede convertir en un clúster de facturación anual/mensual.

Restricciones y limitaciones

- Solo los nodos del grupo de nodos predeterminado **DefaultPool** se pueden cambiar al modo de facturación anual/mensual.
- Los nodos cuyo modo de facturación se cambia a anual/mensual no admiten el ajuste automático.

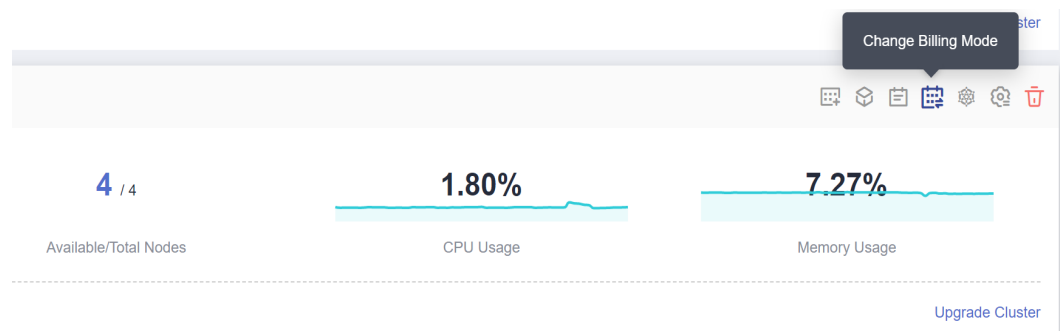
Cambio al modo de facturación anual/mensual

Para cambiar el modo de facturación de los clústeres que ha comprado de pago por uso a anual/mensual, realice los siguientes pasos:

Paso 1 Log in to the CCE console. In the navigation pane, choose **Clusters**.

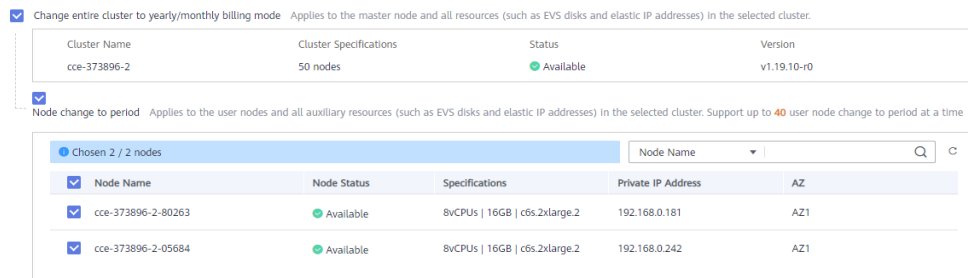
Paso 2 Click  next to the target cluster.

Figura 2-1 Changing to the yearly/monthly billing mode



Paso 3 On the **Change Billing Mode** page, choose the master and worker nodes that will be changed to the yearly/monthly billing mode.

Figura 2-2 Changing billing mode for master and worker nodes



Paso 4 Click **OK**. Wait until the order is processed and the payment is complete.

During payment, if a message is displayed indicating that **you do not have the permission to access the resource API**, go back to the previous page and perform the operation again.

----Fin

2.3 ¿Puedo cambiar el modo de facturación de los nodos de CCE de pago por uso a anual/mensual?

Actualmente, los nodos admiten los modos de facturación **pago por uso** y **anual/mensual**.

Restricciones y limitaciones

- No puede cambiar los nodos de pago por uso a anual/mensual en la consola de ECS.
- Solo los nodos del grupo de nodos predeterminado **DefaultPool** se pueden cambiar al modo de facturación anual/mensual.
- Los nodos cuyo modo de facturación se cambia a anual/mensual no admiten el ajuste automático.

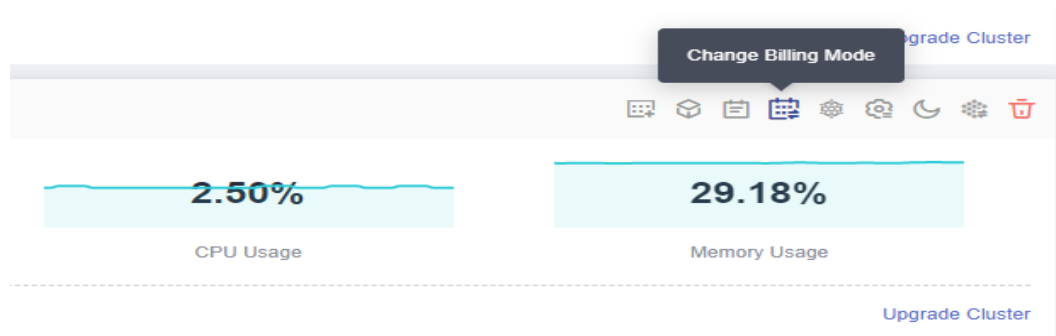
Procedimiento

Para cambiar el modo de facturación de los nodos que ha comprado de pago por uso a anual/mensual, realice los siguientes pasos:

Paso 1 Inicie sesión en la consola de CCE. En el panel de navegación, elija **Clusters**.

Paso 2 Haga clic en  junto al clúster de destino.

Figura 2-3 Cambio al modo de facturación anual/mensual

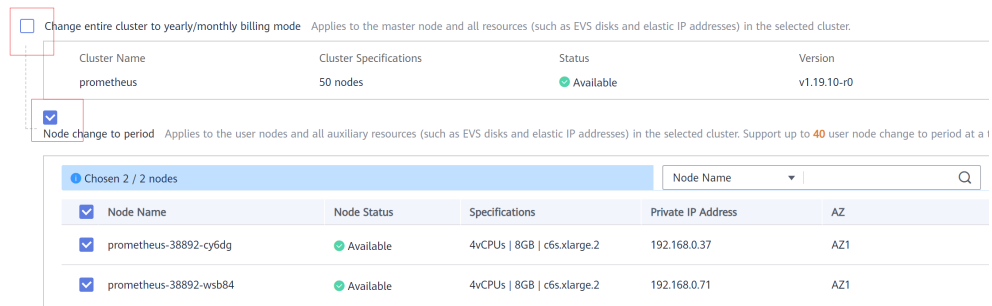


Paso 3 En la página **Change Billing Mode**, elija los nodos que se cambiarán al modo de facturación anual/mensual.

NOTA

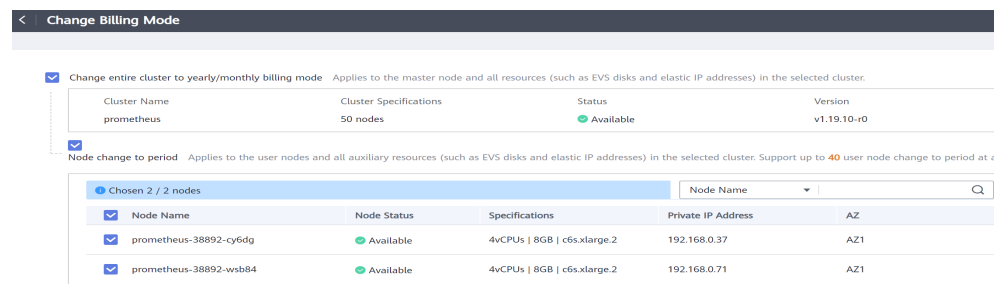
De forma predeterminada, se selecciona **Change entire cluster to yearly/monthly billing mode**. Si desea cambiar ciertos nodos del clúster al modo de facturación anual/mensual, anule la selección de esta opción.

Figura 2-4 Cambiar los nodos al modo de facturación anual/mensual



Si desea cambiar todo el clúster al modo de facturación anual/mensual, seleccione esta opción y los nodos que deben cambiarse al modo de facturación anual/mensual.

Figura 2-5 Cambio del clúster y los nodos del clúster al modo de facturación anual/mensual



Paso 4 Haga clic en **OK**. Espere hasta que se procese el pedido y se complete el pago.

----Fin

2.4 ¿Qué modos de factura son compatibles con Huawei Cloud?

Huawei Cloud admite dos facturas emitidas por ciclo de facturación y por pedido.

Puede seleccionar **Contacts and Invoices > Invoices** en el Centro de facturación para emitir una factura.

2.5 ¿Se me notificará cuando mi saldo sea insuficiente?

Puede establecer un umbral de saldo en la página de recarga. El sistema comprobará su saldo cuando compre un producto y le enviará una notificación si su saldo es inferior o igual al umbral.

2.6 ¿Se me notificará cuando cambie el saldo de mi cuenta?

El sistema le notificará por correo electrónico o mensaje SMS de los cambios en el saldo de su cuenta, incluido si su recarga en línea se realiza correctamente.

2.7 ¿Puedo eliminar un clúster de CCE facturado anual/mensualmente directamente cuando expire?

Después de que caduque un clúster de facturación anual/mensual, puede eliminar el clúster una vez que se haya realizado una copia de respaldo de todos los datos.

Si no renueva ni elimina el clúster después de que caduque, el sistema eliminará el clúster según el tiempo de caducidad del recurso. Se recomienda renovar el clúster y realizar copias de respaldo de los datos de manera oportuna.

2.8 ¿Cómo puedo cancelar mi suscripción a CCE?

Los recursos de CCE facturados anualmente/mensualmente pueden cancelarse, incluida la parte renovada y la parte utilizada actualmente. No puede utilizar estos recursos después de cancelar la suscripción. Se cobrará un gasto de gestión al cancelar la suscripción a un recurso.

Nota

- La cancelación de la suscripción de CCE implica la renovación de los recursos y los recursos que se están utilizando. Después de cancelar la suscripción, estos recursos no estarán disponibles.
- Solo se puede cancelar la suscripción a líneas de productos de soluciones en su totalidad.
- Si un pedido incluye recursos de una relación primaria-secundaria, es necesario cancelar la suscripción a los recursos de forma separada.
- Para obtener más información sobre cómo cancelar la suscripción a los recursos, consulte [Reglas de cancelación de suscripción](#).

Procedimiento

ATENCIÓN

- Antes de solicitar una cancelación de suscripción, asegúrese de haber migrado o realizado una copia de respaldo de los datos guardados en CCE de los que se cancelará la suscripción. Una vez completada la cancelación de la suscripción, CCE y cualquier dato que contenga se eliminarán permanentemente.
- El centro de la página de cancelación de suscripción muestra un mensaje que muestra el número de cancelaciones que ha realizado y el número permitido restante.

-
1. Vaya a la página [Cancelación de la suscripción](#) en el Centro de facturación.
 2. Haga clic en la ficha **Active Resources**.

3. Dese de baja de un solo recurso o de recursos por lotes.
 - Para cancelar la suscripción a un solo recurso, haga clic en **Unsubscribe from Resource** en la fila del nombre del recurso de destino.
 - Para cancelar la suscripción a los recursos de un lote, seleccione los recursos de destino de la lista de recursos y haga clic en **Unsubscribe from Resources** en la esquina superior izquierda de la lista de recursos.
4. En la página **Unsubscribe**, confirme la información de cancelación de suscripción, seleccione una razón para la cancelación de la suscripción y haga clic en **Confirm**.

2.9 ¿Se admite el reembolso de CCE?

Actualmente, no se admite el reembolso automático.

3 Clúster

3.1 Creación de clústeres

3.1.1 ¿Por qué no puedo crear un clúster de CCE?

Descripción

Esta sección describe cómo localizar y rectificar el error si no se puede crear un clúster de CCE.

Detalles

Causas posibles:

1. El Network Time Protocol daemon (ntpd) no está instalado o no se puede instalar, los componentes de Kubernetes no pueden pasar la verificación previa o la partición de disco es incorrecta. La solución actual es crear un clúster de nuevo. Para obtener más información sobre cómo localizar el fallo, consulte [Localización de la causa de la falla](#).
2. Compruebe si tu cuenta está en mora. Si es así, no puede comprar recursos, incluido el uso de cupones en efectivo. Para obtener más información, consulte [¿Cómo recarga una cuenta un cliente común de Huawei Cloud?](#)

Localización de la causa de la falla

Vea los registros del clúster para localizar la causa y rectificar el error.

Paso 1 Inicie sesión en la consola de CCE. En el panel de navegación, haga clic en **Operation Records** encima de la lista de clústeres para ver los registros de operación.

Paso 2 Haga clic en el registro del estado **Failed** para ver información de error.

Figura 3-1 Consulta de los detalles de la operación

Cluster Name	Operation Type	Status	Time
r30027646-new	Create Cluster	Failed	May 07, 2022 11:39:40 GMT+08:00

Project	Start Time	End Time	Status
Create security group rule for cluster communication	May 07, 2022 11:39:41 GMT+08:00	May 07, 2022 11:39:41 GMT+08:00	Completed
Create security group rule for master node	May 07, 2022 11:39:41 GMT+08:00	May 07, 2022 11:39:41 GMT+08:00	Completed
Create security group rules for worker nodes	May 07, 2022 11:39:41 GMT+08:00	May 07, 2022 11:39:46 GMT+08:00	Completed
Create master node network	May 07, 2022 11:39:41 GMT+08:00	May 07, 2022 11:39:41 GMT+08:00	Completed
Create control node subnet	May 07, 2022 11:39:41 GMT+08:00	May 07, 2022 11:39:44 GMT+08:00	Completed
Create master node (5 minutes)[1/3]	May 07, 2022 11:39:44 GMT+08:00	--	Failed

Expected HTTP response code [200 201 202 203 204] when accessing [POST https://ecs-internal.cn-north-7.myhuaweicloud.com/v1/0524ea9c1a00d57e2fddc0190fc7dd97/cloudservers], but got 400 instead {"error":{"message":"The volume type[SSD] cannot be used with the specified flavor in the AZ [cn-north-7b].","code":"Ecs.0044"}}

Paso 3 Rectifique el error basado en la información de error y cree un clúster de nuevo.

----Fin

3.1.2 ¿La escala de gestión de un clúster está relacionada con el número de nodos principales?

La escala de gestión indica el número máximo de nodos que puede gestionar un clúster. Si selecciona **50 nodes**, el clúster puede gestionar un máximo de 50 nodos.

El número de nodos principales varía según la especificación del clúster, pero no se ve afectado por la escala de gestión.

Después de activar el modo de nodo multi-principal, se crearán tres nodos principales. Si un nodo principal está defectuoso, el clúster aún puede estar disponible sin afectar a las funciones de servicio.

3.1.3 ¿Cómo actualizo el certificado raíz al crear un clúster de CCE?

El certificado raíz de los clústeres de CCE es el certificado básico para la autenticación de Kubernetes. Tanto el plano de control del clúster de Kubernetes como el certificado están alojados en Huawei Cloud CCE. CCE actualizará periódicamente el certificado. Este certificado no está abierto a los usuarios, pero no caducará.

El certificado X.509 está habilitado en los clústeres de Kubernetes de forma predeterminada. CCE mantendrá y actualizará automáticamente el certificado X.509.

Obtención de un certificado de clúster

Puede obtener un certificado de clúster en la consola de CCE para acceder a Kubernetes. Para obtener más información, consulte [Obtención de un certificado de clúster](#).

3.1.4 ¿A qué cuotas de recursos debo prestar atención al usar CCE?

CCE restringe **solo el número de clústeres**. Sin embargo, al usar CCE, también puede estar usando otros servicios en la nube, como Elastic Cloud Server (ECS), Elastic Volume Service (EVS), Virtual Private Cloud (VPC), Elastic Load Balance (ELB) y SoftWare Repository for Containers (SWR).

¿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 mi cuota?


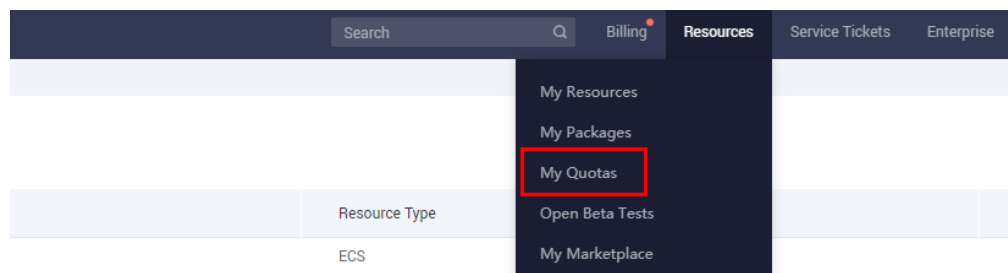
1. Inicie sesión en la consola de gestión.
2. Haga clic en  en la esquina superior izquierda para seleccionar una región y un proyecto.
3. En la esquina superior derecha de la página, seleccione **Resources** > **My Quotas**. Se muestra la página **Service Quota**.

Figura 3-2 Mis cuotas

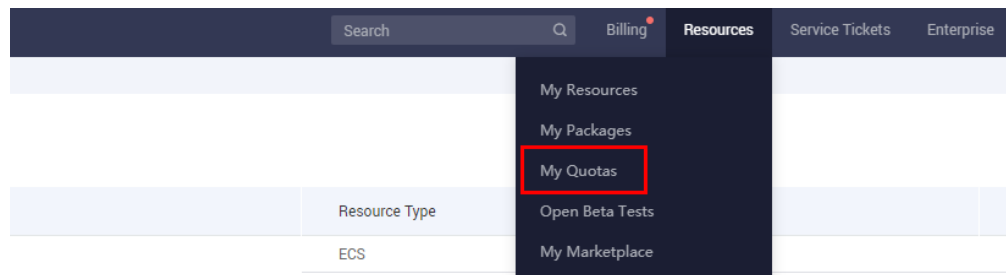


4. En esta página, puede ver la cuota total y la cuota usada de recursos. Si una cuota no puede cumplir con los requisitos de su empresa, haga clic en **Increase Quota**.

¿Cómo puedo aumentar mi cuota?

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 3-3 Mis cuotas



3. Haga clic en **Increase Quota**.
4. En la página **Create Service Ticket**, configure los parámetros según sea necesario y envíe un ticket de servicio.
En el área **Problem Description**, introduzca la cuota requerida y el motivo del ajuste.
5. Seleccione **I have read and agree to the Tenant Authorization Letter** y haga clic en **Submit**.

3.2 Ejecución de clúster

3.2.1 ¿Cómo puedo rectificar la falla cuando el estado del clúster no está disponible?

Si el clúster es **Unavailable**, realice las siguientes operaciones para rectificar el error:

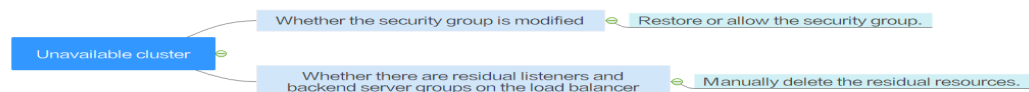
Localización de fallas

Los métodos de resolución de problemas se ordenan en función de la probabilidad de ocurrencia de las posibles causas. Se recomienda comprobar las posibles causas de alta probabilidad a baja probabilidad para localizar rápidamente la causa del problema.

Si la falla persiste después de rectificar una posible causa, compruebe otras posibles causas.

- **Concepto de comprobación 1: Si el grupo de seguridad está modificado**
- **Concepto de comprobación 2: Si hay oyentes residuales y grupos de servidores backend en el balanceador de carga**

Figura 3-4 Localización de fallas



Concepto de comprobación 1: Si el grupo de seguridad está modificado

Paso 1 Inicie sesión en la consola de gestión y elija **Service List > Networking > Virtual Private Cloud**. En el panel de navegación de la izquierda, elija **Access Control > Security Groups** para buscar el grupo de seguridad del nodo principal en el clúster.

El nombre de este grupo de seguridad tiene el formato de *Cluster name-cce-control-ID*.

Paso 2 Haga clic en el grupo de seguridad. En la página de detalles que se muestra, asegúrese de que las reglas de grupo de seguridad del nodo principal son correctas.

Para obtener más información acerca de la seguridad, consulte [Configuración de reglas de grupo de seguridad de clúster](#).

----Fin

Concepto de comprobación 2: Si hay oyentes residuales y grupos de servidores backend en el balanceador de carga

Reproducir el problema

Se produce una excepción de clúster cuando se crea o se elimina un LoadBalancer Service. Después de corregir el error, el Service se elimina correctamente, pero hay escuchas residuales y grupo de servidores backend.

Paso 1 Precree un clúster de CCE. En el clúster, utilice la imagen oficial de Nginx para crear cargas de trabajo, balanceadores de carga preestablecidos, Services y entradas.

Paso 2 Asegúrese de que el clúster se está ejecutando correctamente y que la carga de trabajo de Nginx es estable.

Paso 3 Cree y elimine 10 LoadBalancer Services cada 20 segundos.

Paso 4 Se produce una excepción de inyección en el clúster. Por ejemplo, el pod de etcd no está disponible o el clúster está hibernado.

----Fin

Causa posible

Hay oyentes residuales y grupos de servidores backend en el balanceador de carga.

Solución

Borre manualmente los oyentes residuales y los grupos de servidores back-end.

Paso 1 Inicie sesión en la consola de gestión y seleccione **Network > Elastic Load Balance** en la lista de servicios.

Paso 2 En la lista de balanceadores de carga, haga clic en el nombre del balanceador de carga de destino para ir a la página de detalles. En la página de ficha **Listeners**, localice el oyente de destino y elimínelo.

Paso 3 En la página de ficha **Backend Server Groups**, busque el grupo de servidores backend de destino y elimínelo.

----Fin

3.2.2 ¿Cómo puedo restablecer o reinstalar un clúster de CCE?

Los clústeres de CCE no se pueden restablecer ni reinstalar. Si un clúster no está disponible, [envíe un ticket de servicio](#) o elimine el clúster y luego compre uno nuevo.

CCE admite nodos de restablecimiento. Para obtener más información, consulte [Restablecimiento de un nodo](#).

3.2.3 ¿Cómo puedo comprobar si un clúster está en modo multimaestro?

Inicie sesión en la consola de CCE y haga clic en el clúster. A la derecha de la página de detalles del clúster, vea el número de nodos principales.

- 3: El clúster está en modo multi-principal.
- 1: El clúster está en modo de principal único.

AVISO

El número de nodos maestros no se puede cambiar después de crear el clúster. Si desea ajustar el número, debe crear un nuevo clúster.

3.2.4 ¿Puedo conectarme directamente al nodo maestro de un clúster?

CCE permite utilizar kubectl para conectar un clúster. Para obtener más información, consulte [Conectar a un clúster con kubectl](#).

Sin embargo, no se le permite iniciar sesión en el nodo principal para realizar las operaciones relacionadas.

3.2.5 ¿Cómo puedo recuperar datos después de eliminar un clúster?

Después de eliminar un clúster, la carga de trabajo del clúster también se eliminará y no se podrá restaurar. Por lo tanto, tenga cuidado al eliminar un clúster.

3.2.6 ¿Cómo actualizo un espacio de nombres en estado Terminating?

En Kubernetes, un espacio de nombres tiene dos estados comunes: Active y Terminating. El estado Terminating es raro. Cuando un espacio de nombres tiene recursos en ejecución pero se elimina el espacio de nombres, el espacio de nombres se convierte en Terminating. En este caso, el sistema eliminará automáticamente el espacio de nombres después de que Kubernetes recupere los recursos en el espacio de nombres.

Sin embargo, en algunos casos, incluso si no se está ejecutando ningún recurso en el espacio de nombres, el espacio de nombres en el estado Terminating aún no se puede eliminar.

Para solucionar este problema, realice los siguientes pasos:

Paso 1 Ver los detalles del espacio de nombres.

```
$ kubectl get ns | grep rdb
rdbms                Terminating    6d21h

$ kubectl get ns rdbms -o yaml
apiVersion: v1
kind: Namespace
metadata:
  annotations:
    kubectl.kubernetes.io/last-applied-configuration: |
```

```
{ "apiVersion": "v1", "kind": "Namespace", "metadata": { "annotations":
{} }, "name": "rdbms" }
creationTimestamp: "2020-05-07T15:19:43Z"
deletionTimestamp: "2020-05-07T15:33:23Z"
name: rdbms
resourceVersion: "84553454"
selfLink: /api/v1/namespaces/rdbms
uid: 457788ddf-53d7-4hde-afa3-1fertg21ewel
spec:
  finalizers:
  - kubernetes
status:
  phase: Terminating
```

Paso 2 Ver recursos en el espacio de nombres.

```
# View resources that can be isolated using namespaces in the cluster.
$ kubectl api-resources -o name --verbs=list --namespaced | xargs -n 1 kubectl
get --show-kind --ignore-not-found -n rdbms
```

Después de ejecutar el comando anterior, no se ocupa ningún recurso en el espacio de nombres **rdbms**.

Paso 3 Eliminar el espacio de nombres.

Elimine directamente el **rdbms** del espacio de nombres.

```
$ kubectl delete ns rdbms
Error from server (Conflict): Operation cannot be fulfilled on namespaces
"rdbms": The system is ensuring all content is removed from this namespace. Upon
completion, this namespace will automatically be purged by the system.
```

El sistema muestra un mensaje que indica que la operación de eliminación se completará hasta que el sistema elimine todos los recursos inútiles.

Paso 4 Elimine por la fuerza el espacio de nombres.

```
$ kubectl delete ns rdbms --force --grace-period=0
warning: Immediate deletion does not wait for confirmation that the running
resource has been terminated. The resource may continue to run on the cluster
indefinitely.
Error from server (Conflict): Operation cannot be fulfilled on namespaces
"rdbms": The system is ensuring all content is removed from this namespace. Upon
completion, this namespace will automatically be purged by the system.
```

Después de ejecutar el comando anterior, el espacio de nombres aún no se puede eliminar.

Paso 5 Utilizar la API nativa para eliminar estos recursos.

Obtenga los detalles del espacio de nombres.

```
$ kubectl get ns rdbms -o json > rdbms.json
```

Compruebe la configuración de JSON definida por el espacio de nombres, edite el archivo JSON y elimine la parte **spec**.

```
$ cat rdbms.json
{
  "apiVersion": "v1",
  "kind": "Namespace",
  "metadata": {
    "annotations": {
      "kubectl.kubernetes.io/last-applied-configuration": "{\"apiVersion\":
\\\"v1\\\", \"kind\": \"Namespace\", \"metadata\": { \"annotations\": {}, \"name\": \"rdbms
\\\" } }\\n"
    }
  },
  "creationTimestamp": "2019-10-14T12:17:44Z",
  "deletionTimestamp": "2019-10-14T12:30:27Z",
  "name": "rdbms",
  "resourceVersion": "8844754",
  "selfLink": "/api/v1/namespaces/rdbms",
```

```
    "uid": "29067ddf-56d7-4cce-afa3-1fbdbb221ab1"
  },
  "spec": {
    "finalizers": [
      "kubernetes"
    ]
  },
  "status": {
    "phase": "Terminating"
  }
}
```

Después de ejecutar la solicitud PUT, el espacio de nombres se elimina automáticamente.

```
$ curl --cacert /root/ca.crt --cert /root/client.crt --key /root/client.key -k -H
"Content-Type:application/json" -X PUT --data-binary @rdbms.json https://x.x.x.x:
5443/api/v1/namespaces/rdbms/finalize
{
  "kind": "Namespace",
  "apiVersion": "v1",
  "metadata": {
    "name": "rdbms",
    "selfLink": "/api/v1/namespaces/rdbms/finalize",
    "uid": "29067ddf-56d7-4cce-afa3-1fbdbb221ab1",
    "resourceVersion": "8844754",
    "creationTimestamp": "2019-10-14T12:17:44Z",
    "deletionTimestamp": "2019-10-14T12:30:27Z",
    "annotations": {
      "kubect1.kubernetes.io/last-applied-configuration": "{\"apiVersion\":\"v1\",
\"kind\":\"Namespace\", \"metadata\":{\"annotations\":{}, \"name\":\"rdbms\"}}\n"
    }
  },
  "spec": {
  },
  "status": {
    "phase": "Terminating"
  }
}
```

Si el espacio de nombres aún no se puede eliminar, compruebe si el campo **finalizers** existe en los metadatos. Si el campo existe, ejecute el siguiente comando para acceder al espacio de nombres y eliminar el campo:

```
kubect1 edit ns rdbms
```

NOTA

- Para obtener más información acerca de cómo obtener el certificado de clúster, consulte [Obtención de un certificado de clúster](#).
- **https://x.x.x.x:5443** indica la dirección para conectarse al clúster. Para obtener la dirección, inicie sesión en la consola de CCE, haga clic en el clúster y vea **Private IP** en el panel **Connection Information**.

Paso 6 Compruebe si el espacio de nombres se ha eliminado.

```
$ kubect1 get ns | grep rdb
```

---Fin

3.2.7 ¿Por qué el uso del disco del nodo de visualización de CCE es incompatible con Cloud Eye?

Síntomas

El uso del disco de un nodo en la página de detalles del clúster de CCE es superior al 80%, pero el uso del disco que se muestra en la consola de Cloud Eye es inferior al 40%.

Después de la localización de fallas en el nodo, se encuentra que el uso de un disco de PVC alcanza el 92%. Después de borrar el disco, el uso del disco en CCE es el mismo que en Cloud Eye.

¿CCE muestra solo el uso más alto del disco?

Respuesta

En la información de supervisión del clúster de CCE, se supervisa el disco con el uso más alto del disco en el nodo.

3.3 Eliminación de clústeres

3.3.1 Error al eliminar un clúster: ENI residuales

Para eliminar un clúster, CCE se conecta al kube-apiserver del clúster para consultar información sobre sus recursos, como las interfaces de red elásticas (ENI) o los ENI secundarios conectados a un clúster de CCE Turbo. Si el clúster está en estado no disponible, congelado o hibernado, es posible que no se elimine debido a un error de consulta de recursos.

Síntoma

Error al eliminar un clúster.

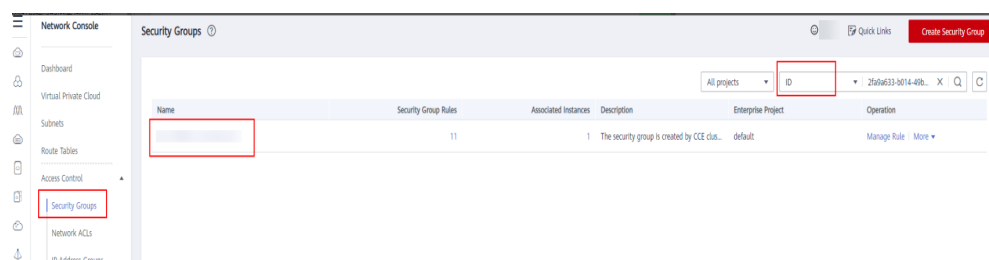
```
Failed Operation:
Resource ID:
Reason: delete failed: {"code": "4967ba194623", "action": "SecGrp.DeleteMasterSecGrp.Skip", "message": "Expected HTTP response code [200 202 204 404] when accessing [DELETE https://1202-52aa-457d-b978-4967ba194623], but got 409 Instead\n{\"NeutronError\": {\"message\": \"Security Group use.\", \"type\": \"SecurityGroupInUse\", \"detail\": {}}\"}"}
:623 in
```

Causa posible

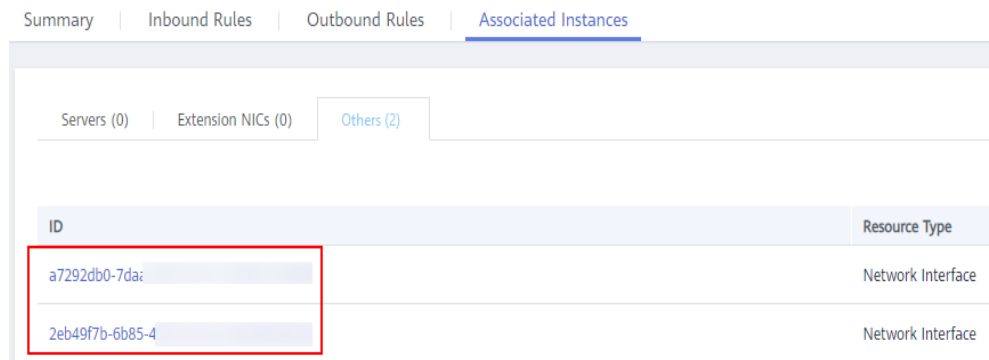
En este ejemplo, el ENI no se puede eliminar porque kube-apiserver del clúster no puede consultar el ENI o el ENI secundario del clúster. El grupo de seguridad creado por el CCE para el ENI o el sub ENI informa del código de error 409. Como resultado, no se puede eliminar el clúster.

Procedimiento

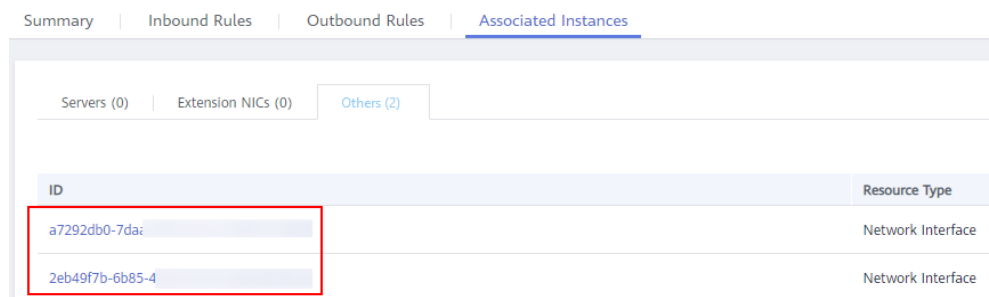
Paso 1 Copie el ID de recurso **f5b0282b-6306-4a4b-a64d-bd32e26c3846** en la información de error, vaya a la página **Security Groups** de la consola de VPC y filtre los grupos de seguridad por ID.



Paso 2 Haga clic en el grupo de seguridad para ver sus detalles y haga clic en la ficha **Associated Instances**.

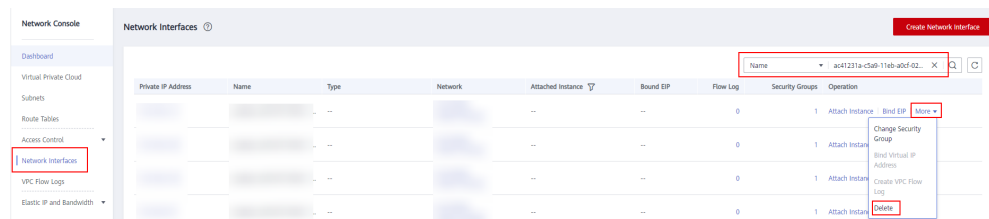


La causa del grupo de seguridad residual es que el grupo de seguridad está asociado con el ENI y el ENI secundario. Haga clic en la ficha **Others** para ver los ENI residuales. Suprima los ENIs residuales y los ENI suplementarios se eliminarán automáticamente.



Paso 3 Elija **Network Interfaces** en el panel de navegación de la consola para eliminar los ENI consultados en el paso anterior.

Puede filtrar los ENI que se van a eliminar por ID o nombre (ID del clúster). En este ejemplo, filtre los ENI por su nombre a través del identificador de clúster **ac41231a-c5a9-11eb-a0cf-a0cf-0255ac100440**.



Paso 4 Después del borrado, vaya a la página **Security Groups** para comprobar que *Cluster name-cce-eni-xxx* no tiene las instancias asociadas. A continuación, puede eliminar el clúster en la consola de CCE.

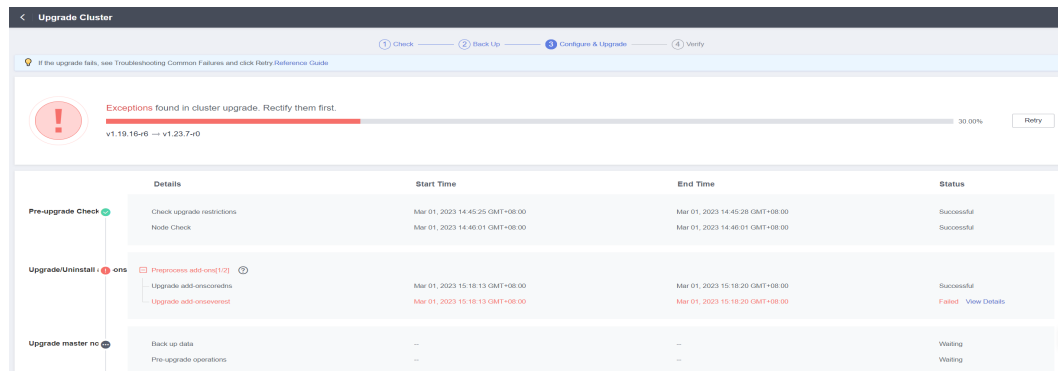
----Fin

3.4 Actualización de clúster

3.4.1 ¿Qué hago si un complemento de clúster no se actualiza durante la actualización del clúster de CCE?

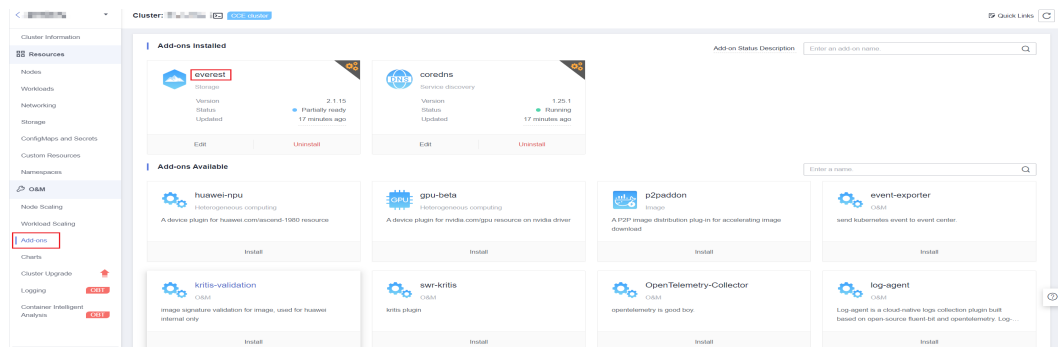
Descripción general

Esta sección describe cómo localizar y rectificar el error si no se puede actualizar un complemento durante la actualización del clúster de CCE.



Procedimiento

- Paso 1** Si el complemento no se actualiza, inténtelo de nuevo primero. Si el reintento falla, realice los siguientes pasos para rectificar la falla.
- Paso 2** Si aparece un mensaje de error en la página de actualización, vaya a la página **Add-ons** para ver el estado del complemento. Para un complemento anormal, haga clic en el nombre del complemento para ver los detalles.



- Paso 3** En la página de detalles de pod, haga clic en **View Events** en la columna **Operation** del pod anormal.

Pods X

Delete Pod Name Search keyword Q C

Pod Name	Status	Names...	Pod IP	Node	Resta...	CPU Request/Limit/Usa	Memory Request/Limit/Usa	Created	Operation
everest-csi-driver- Host network	Running	kube-system	192.168.0.100	192.168.0.100	0	0.1 Cores 0.5 Cores 1.00%	300 MiB 300 MiB 26.25%	3 hours ago	Monitor View Events More
everest-csi-driver- Host network	Running	kube-system	192.168.0.230	192.168.0.230	0	0.1 Cores 0.5 Cores 0.80%	300 MiB 300 MiB 26.03%	3 hours ago	Monitor View Events More
everest-csi-control	Running	kube-system	10.0.0.3	192.168.0.230	0	0.25 Cores 0.25 Cores 0.80%	0.59 GiB 1.46 GiB 5.13%	3 hours ago	Monitor View Events More
everest-csi-control	Abnormal	kube-system	10.0.0.131	192.168.0.100	10	0.25 Cores 0.25 Cores 0.40%	0.59 GiB 1.46 GiB 3.92%	3 hours ago	Monitor View Events More

Paso 4 Rectifique la falla basada en la información de excepción. Por ejemplo, elimine el pod que no se ha iniciado o reinicielo.

Events X



Event data is stored only for one hour and then automatically cleared.

Start Date — End Date Enter a Kubernetes event na Q C

Kubernet...	Event ...	Occurr...	Event Name	Kubernetes Event	First Occurred	Last Occurred
kubelet	Alarm	121	Failed to restar...	the failed container exited with ExitCod...	Mar 01, 2023 15:08:2...	Mar 01, 2023 15:33:1...
kubelet	Alarm	74	Failed to restar...	Back-off restarting failed container	Mar 01, 2023 15:08:2...	Mar 01, 2023 15:23:1...
kubelet	Alarm	4	PodsStart failed	Error: failed to start container "everest-...	Mar 01, 2023 15:08:0...	Mar 01, 2023 15:08:5...
kubelet	Normal	5	Image pulled	Container image "100.79.1.215:20202/...	Mar 01, 2023 11:53:5...	Mar 01, 2023 15:08:5...
kubelet	Normal	5	PodsCreated	Created container everest-csi-controller	Mar 01, 2023 11:53:5...	Mar 01, 2023 15:08:5...
kubelet	Normal	4	PodsVolume ...	Successfully mounted volumes for pod ...	Mar 01, 2023 11:53:5...	Mar 01, 2023 15:08:2...

Paso 5 Una vez que el procesamiento se realiza correctamente, el estado del complemento cambia a **Running**. Asegúrese de que todos los complementos estén en el estado **Running**.

Add-ons Installed

 <p>coredns Service discovery</p> <p>Version: 1.25.1 Status: Running Updated: 8 days ago</p> <p>Edit Uninstall</p>	 <p>everest Storage</p> <p>Version: 2.1.15 Status: Running Updated: 8 days ago</p> <p>Edit Uninstall</p>
---	--

Paso 6 Vaya a la página de actualización del clúster y haga clic en **Retry**.

① Check — ② Back Up — ③ Configure & Upgrade — ④ Verify

If the upgrade fails, see [Troubleshooting Common Failures](#) and click [Retry](#) Reference Guide

Exceptions found in cluster upgrade. Rectify them first. 30.00% Retry

v1.19.16-r6 → v1.23.7-0

	Details	Start Time	End Time	Status
Pre-upgrade Check	Check upgrade restrictions	Mar 01, 2023 14:45:25 GMT+08:00	Mar 01, 2023 14:45:26 GMT+08:00	Successful
	Node Check	Mar 01, 2023 14:46:01 GMT+08:00	Mar 01, 2023 14:46:01 GMT+08:00	Successful
Upgrade/Uninstall	Preprocess add-ons[1/2]			
	Upgrade add-onsccredis	Mar 01, 2023 15:18:13 GMT+08:00	Mar 01, 2023 15:18:20 GMT+08:00	Successful
	Upgrade add-onselasticsearch	Mar 01, 2023 15:18:13 GMT+08:00	Mar 01, 2023 15:18:20 GMT+08:00	Failed View Details
Upgrade master node	Back up data	--	--	Waiting
	Pre-upgrade operations	--	--	Waiting

---Fin

4 Nodo

4.1 Creación de nodos

4.1.1 ¿Cómo soluciono los problemas que se producen al agregar nodos a un clúster de CCE?

Nota

- Las imágenes de nodo en el mismo clúster deben ser las mismas. Preste atención a esto al crear, agregar o aceptar nodos en un clúster.
- Si necesita asignar espacio de usuario desde el disco de datos al crear un nodo, no establezca la ruta de almacenamiento de datos en ningún directorio de claves. Por ejemplo, para almacenar datos en el directorio **/home**, establezca el directorio en **/home/test** en lugar de en **/home**.

NOTA

No establezca **Path inside a node** en el directorio raíz **/**. De lo contrario, el montaje falla. Establezca **Path inside a node** en cualquiera de las siguientes opciones:

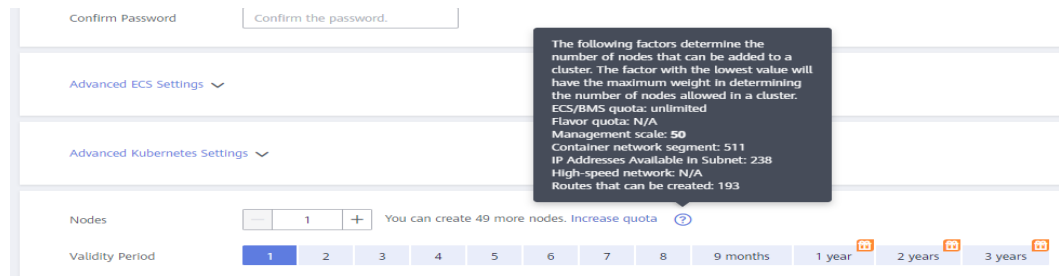
- **/opt/xxxx** (excluido **/opt/cloud**)
- **/mnt/xxxx** (excluido **/mnt/paas**)
- **/tmp/xxx**
- **/var/xxx** (excluidos los directorios clave como **/var/lib**, **/var/script** y **/var/paas**)
- **/xxxx** (No puede entrar en conflicto con el directorio del sistema, como **bin**, **lib**, **home**, **root**, **boot**, **dev**, **etc**, **lost+found**, **mnt**, **proc**, **sbin**, **srv**, **tmp**, **var**, **media**, **opt**, **selinux**, **sys** y **usr**.)

No lo establezca en **/home/paas**, **/var/paas**, **/var/lib**, **/var/script**, **/mnt/paas** ni en **/opt/cloud**. De lo contrario, la instalación del sistema o del nodo fallará.

Concepto de comprobación 1: Cuota de subred

Síntoma

No se pueden agregar nuevos nodos a un clúster de CCE y se muestra un mensaje que indica que la cuota de subred es insuficiente.



Análisis de las causas

Ejemplo:

Bloque CIDR de VPC: 192.168.66.0/24

Bloque CIDR de subred: 192.168.66.0/24

En 192.168.66.0/24, se han utilizado las 251 direcciones IP privadas.

Solución

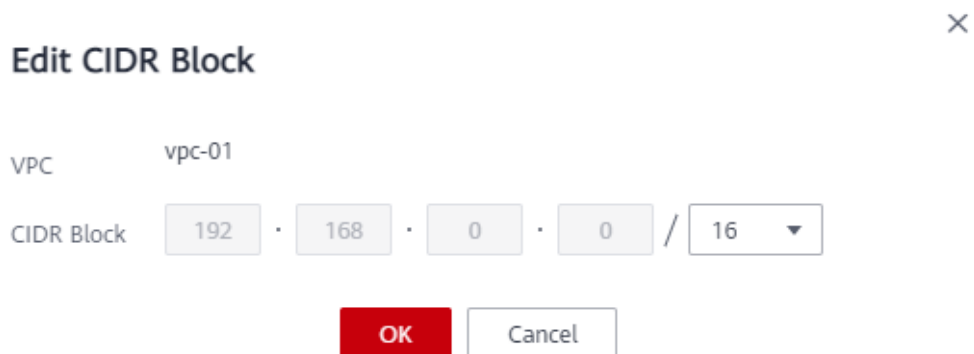
Paso 1 Amplíe la VPC.

Inicie sesión en la consola y elija **Virtual Private Cloud** en la lista de servicios. Haga clic en **Edit CIDR Block** en la columna **Operation** de la VPC de destino.

Consulta la siguiente figura:



Paso 2 Cambie la máscara de subred a 16 y haga clic en **OK**.



Paso 3 Haga clic en el nombre de la VPC. En la página de ficha **Summary**, haga clic en el número junto a **Subnets** a la derecha y haga clic en **Create Subnet** para crear una subred.

✕

Create Subnet

* VPC vpc-cb ↕ 🔄
IPv4 CIDR block: 192.168.0.0/16
 The VPC already contains 1 subnets.

* AZ AZ3 ?

* Name subnet-a430 0-255

* IPv4 CIDR Block 192 · 168 · 0 · 0 / 24 ↕
Available IP Addresses: 251
 The CIDR block cannot be modified after the subnet has been created.

IPv6 CIDR Block Enable ?

Associated Route Table Default ?

Advanced Settings ▾ Gateway | DNS Server Address | Tag

OK
Cancel

Paso 4 Vuelva a la página para agregar un nodo en la consola de CCE y seleccione la subred recién creada.

NOTA

1. La adición de subredes a la VPC no afecta al uso del bloque CIDR 192.168.66.0/24 existente.
 Puede seleccionar una nueva subred al crear un nodo de CCE. La nueva subred tiene un máximo de 251 direcciones IP privadas. Si el número de direcciones IP privadas no puede cumplir con los requisitos de servicio, puede agregar más subredes.
2. Las subredes en la misma VPC pueden comunicarse entre sí.

----Fin

Concepto de comprobación 2: Cuota de la EIP

Síntoma

Cuando se agrega un nodo, el valor **EIP** se establece en **Automatically assign**. No se puede crear el nodo y se muestra un mensaje que indica que las EIP son insuficientes.

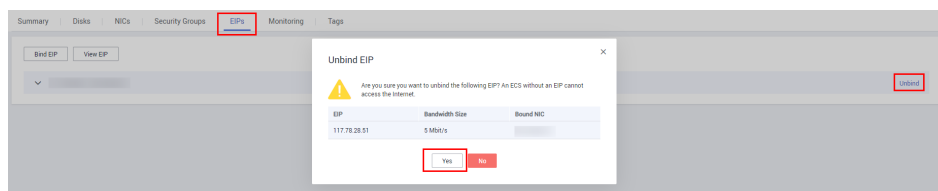
Solución

Hay dos métodos disponibles para resolver el problema.

- **Método 1:** Desvincule las máquinas virtuales enlazadas con las EIP y agregue un nodo de nuevo.
 - a. Inicie sesión en la consola de gestión.

- b. Elija **Computing > Elastic Cloud Server**.
- c. En la lista ECS, busque el ECS de destino y haga clic en su nombre.
- d. En la página de detalles de ECS, haga clic en la ficha **EIPs**. En la lista EIP, haga clic en **Unbind** en la fila del ECS de destino y haga clic en **Yes**.

Figura 4-1 Desvinculación de una EIP



- e. Vuelva a la página para agregar un nodo en la consola de CCE, seleccione **Use existing** para **EIP** y agregue el nodo de nuevo.
- **Método 2:** Aumentar la cuota de la EIP.

Concepto de comprobación 3: Grupo de seguridad

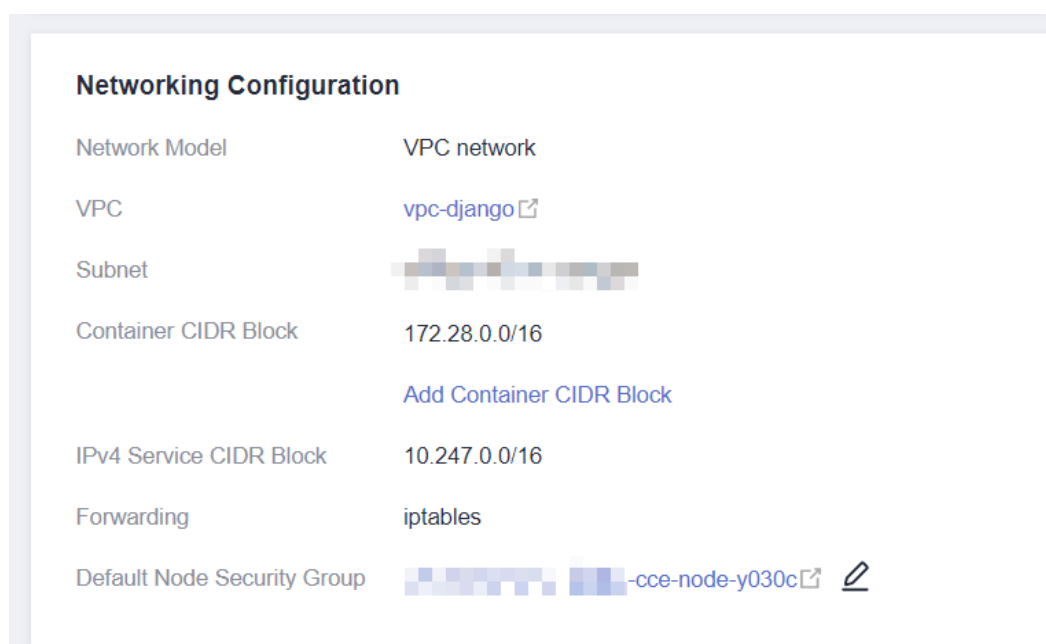
Síntoma

No se puede agregar un nodo a un clúster de CCE.

Solución

Puede hacer clic en el nombre del clúster para ver los detalles del clúster. En el área **Networking Configuration**, haga clic en el icono situado junto a **Default security group of the node** para comprobar si se elimina el grupo de seguridad predeterminado y si las reglas del grupo de seguridad cumplen con [Configuración de reglas de grupo de seguridad de clúster](#).

Si su cuenta tiene varios clústeres y necesita gestionar las políticas de seguridad de red de los nodos de manera unificada, puede especificar grupos de seguridad personalizados. Para obtener más información, consulte [Cambiar el grupo de seguridad predeterminado de un nodo](#).



4.1.2 ¿Cómo soluciono los problemas que se producen al aceptar nodos en un clúster de CCE?

Descripción general

Esta sección describe cómo solucionar los problemas que se produjeron al aceptar o agregar los ECS existentes a un clúster de CCE.

AVISO

- Mientras se acepta un ECS en un clúster, el sistema operativo del ECS se restablecerá a la imagen de sistema operativo estándar proporcionada por CCE para garantizar la estabilidad del nodo. La consola de CCE le pedirá que seleccione el sistema operativo y el modo de inicio de sesión durante el restablecimiento.
- El sistema de ECS y los discos de datos se formatearán mientras el ECS se acepta en un clúster. Asegúrese de que se ha realizado una copia de respaldo de los datos de los discos.
- Mientras se acepta un ECS en un clúster, no realice ninguna operación en el ECS con la consola de ECS.

Notas y restricciones

- La versión del clúster debe ser 1.13 o posterior en la consola anterior y 1.15 o posterior en la consola nueva.
- No se pueden gestionar los nodos de Hyper Elastic Cloud Server (HECS).
- Si IPv6 está habilitado para un clúster, solo se pueden aceptar y gestionar los nodos de una subred con IPv6 habilitado. Si IPv6 no está habilitado para el clúster, solo se pueden aceptar los nodos de una subred sin IPv6 habilitado.
- Si se ha establecido la contraseña o la clave cuando se crea un nodo de máquina virtual, el nodo de máquina virtual se puede aceptar en un clúster 10 minutos después de que esté disponible.
- Los nodos de un clúster de CCE Turbo deben admitir sub-ENI o estar vinculados a al menos 16 ENI. Para obtener más información sobre las especificaciones de nodo, consulte los nodos que se pueden seleccionar en la consola al crear un nodo.

Prerequisites

A cloud server that meets the following conditions can be accepted:

- The node to be accepted must be in the **Running** state and not used by other clusters. In addition, the node to be accepted does not carry the CCE-Dynamic-Provisioning-Node tag.
- The node to be accepted and the cluster must be in the same VPC. (If the cluster version is earlier than v1.13.10, the node to be accepted and the CCE cluster must be in the same subnet.)
- At least one data disk is attached to the node to be accepted. The data disk capacity is greater than or equal to 100 GB. For details about how to attach a data disk, see [Adding a Disk to an ECS](#).

- The node to be accepted has 2-core or higher CPU, 4 GB or larger memory, and only one NIC.
- If an enterprise project is used, the node to be accepted and the cluster must be in the same enterprise project. Otherwise, resources cannot be identified during management. As a result, the node cannot be managed.
- Only cloud servers with the same specifications, AZ, and data disk configuration can be added in batches.

Procedimiento

Vea la información del log del clúster para localizar la causa de la falla y rectificarla.

Paso 1 Inicie sesión en la consola de CCE. En el panel de navegación, haga clic en **Operation Records** encima de la lista de clústeres para ver los registros de operación.

Paso 2 Haga clic en el registro del estado **Failed** para ver información de error.

Paso 3 Rectifique el error basado en la información de error y acepte el nodo en un clúster de nuevo.

----Fin

4.1.3 ¿Qué debo hacer si un nodo no se acepta porque no se instala?

Síntoma

No se puede aceptar un nodo en un clúster.

Causa posible

Inicie sesión en el nodo y compruebe el log de instalación `/var/paas/sys/log/baseagent/baseagent.log`. Se muestra la siguiente información de error:

```
net.core.somaxconn=32768
net.ipv4.tcp_max_syn_backlog=8096
PIBONSmem
failed because of no tenant.conf
10310 10:17:41.075097 6872 baseagent-gs:330] install failed
E8310 10:17:41.076179 6872 install-gs:181] Install failed: Install Version(v1.13.7-r0) failed: Exec component plugins/config-prepare Install failed: exit status 1
, output: [ Tue Mar 10 10:17:35 CST 2020 ] start install plugins/config-prepare
net.ipv4.ip_forward = 1
net.ipv4.neigh.default_gc_thresh1 = 2848
net.ipv4.neigh.default_gc_thresh2 = 4096
net.ipv4.neigh.default_gc_thresh3 = 8192
net.ipv4.ip_forward=1
```

Compruebe la configuración de LVM del nodo. Se encuentra que el volumen lógico de LVM no se crea en el `/dev/vdb`.

Solución

Ejecute el siguiente comando para crear manualmente un volumen lógico:

```
pvcreate /dev/vdb
vgcreate vgpaas /dev/vdb
```

Después de que el nodo se restablezca en la GUI, el nodo se vuelve normal.

4.2 Ejecución de nodo

4.2.1 ¿Qué debo hacer si un clúster está disponible pero algunos nodos no están disponibles?

Si el estado del clúster está disponible pero algunos nodos del clúster no están disponibles, realice las siguientes operaciones para rectificar el error:

Mecanismo para detectar la indisponibilidad de nodos

Kubernetes proporciona el mecanismo de latidos para ayudarlo a determinar la disponibilidad de los nodos. Para obtener detalles sobre el mecanismo y el intervalo, consulte [Latidos cardíacos](#).

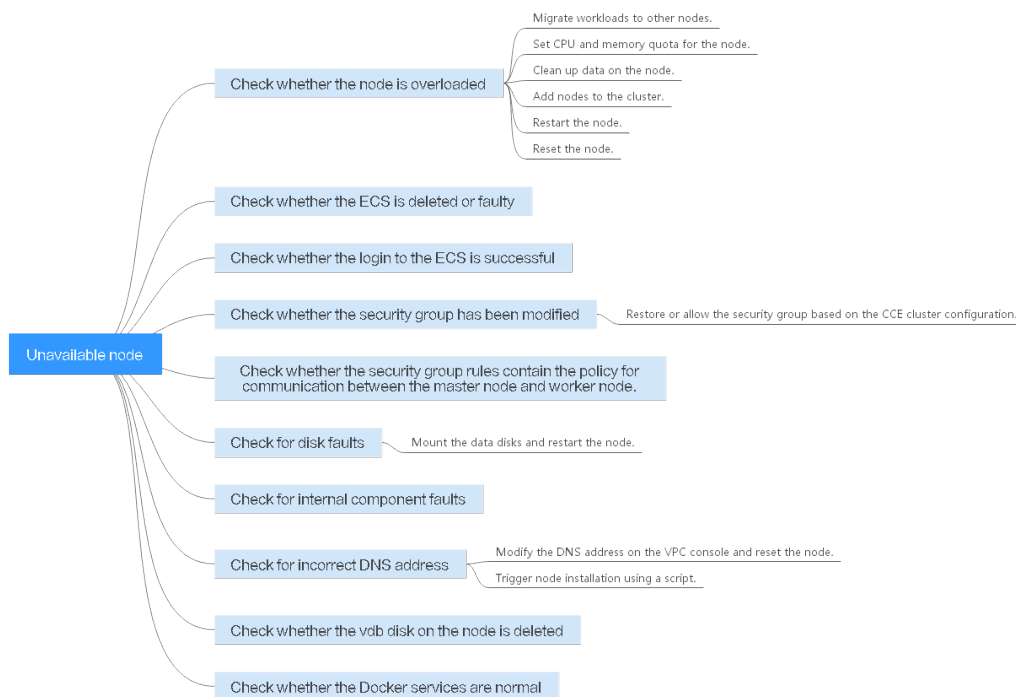
Localización de fallas

Los métodos de resolución de problemas se ordenan en función de la probabilidad de ocurrencia de las posibles causas. Se recomienda comprobar las posibles causas de alta probabilidad a baja probabilidad para localizar rápidamente la causa del problema.

Si la falla persiste después de rectificar una posible causa, compruebe otras posibles causas.

- **Concepto de comprobación 1: Si el nodo está sobrecargado**
- **Concepto de comprobación 2: Si el ECS está eliminado o defectuoso**
- **Concepto de comprobación 3: Si puede iniciar sesión en el ECS**
- **Concepto de comprobación 4: Si el grupo de seguridad está modificado**
- **Concepto de comprobación 5: Si las reglas del grupo de seguridad contienen la política de grupo de seguridad para la comunicación entre el nodo principal y el nodo de trabajo**
- **Concepto de comprobación 6: Si el disco es anormal**
- **Concepto de comprobación 7: Si los componentes internos son normales**
- **Concepto de comprobación 8: Si la dirección DNS es correcta**
- **Concepto de comprobación 9: Si se elimina el disco vdb en el nodo**
- **Concepto de comprobación 10: Si el servicio Docker es normal**

Figura 4-2 Proceso de solución de problemas



Concepto de comprobación 1: Si el nodo está sobrecargado

Síntoma

La conexión de nodo en el clúster es anormal. Varios nodos informan de errores de escritura, pero los servicios no se ven afectados.

Localización de fallas

Paso 1 Inicie sesión en la consola de CCE y haga clic en el clúster. En el panel de navegación, elija **Nodos**. Haga clic en **Monitor** en la fila del nodo no disponible.

Paso 2 En la parte superior de la página mostrada, haga clic en **View More** para ir a la consola de AOM y ver los registros de supervisión históricos.

Un uso demasiado alto de CPU o memoria del nodo dará como resultado una alta latencia de red o sistema de activación OOM. Por lo tanto, el nodo se muestra como no disponible.

---Fin

Solución

1. Se recomienda migrar servicios para reducir las cargas de trabajo en el nodo y establecer el límite superior de recursos para las cargas de trabajo.
2. Borre los datos de los nodos de CCE en el clúster.
3. Limite la CPU y las cuotas de memoria de cada contenedor.
4. Agregue más nodos al clúster.
5. También puede reiniciar el nodo en la consola de ECS.
6. Agregue los nodos para desplegar contenedores con uso intensivo de memoria por separado.

- Restablezca el nodo. Para obtener más información, consulte [Restablecer un nodo](#).
Una vez que el nodo esté disponible, se restaura la carga de trabajo.

Concepto de comprobación 2: Si el ECS está eliminado o defectuoso

Paso 1 Compruebe si el clúster está disponible.

Inicie sesión en la consola de CCE y compruebe si el clúster está disponible.

- Si el clúster no está disponible, por ejemplo, se produce un error, consulte [¿Cómo puedo rectificar la falla cuando el estado del clúster no está disponible?](#).
- Si el clúster se está ejecutando pero algunos nodos del clúster no están disponibles, vaya a [Paso 2](#).

Paso 2 Inicie sesión en la consola de ECS y vea el estado de ECS.

- Si el estado de ECS es **Deleted**, vuelva a la consola de CCE, elimine el nodo correspondiente de la lista de nodos del clúster y, a continuación, cree otro.
- Si el estado de ECS es **Stopped** o **Frozen**, restaure el ECS. Se tarda aproximadamente 3 minutos en restaurar el ECS.
- Si el ECS es **Faulty**, reinicie el ECS para rectificar la falla.
- Si el estado del ECS es **Running**, inicie sesión en el ECS para localizar la falla de acuerdo con [Concepto de comprobación 7: Si los componentes internos son normales](#).

----Fin

Concepto de comprobación 3: Si puede iniciar sesión en el ECS

Paso 1 Inicie sesión en la consola de ECS.

Paso 2 Compruebe si el nombre de nodo que se muestra en la página es el mismo que en la máquina virtual y si la contraseña o la clave se pueden utilizar para iniciar sesión en el nodo.

Figura 4-3 Comprobación del nombre de nodo mostrado en la página

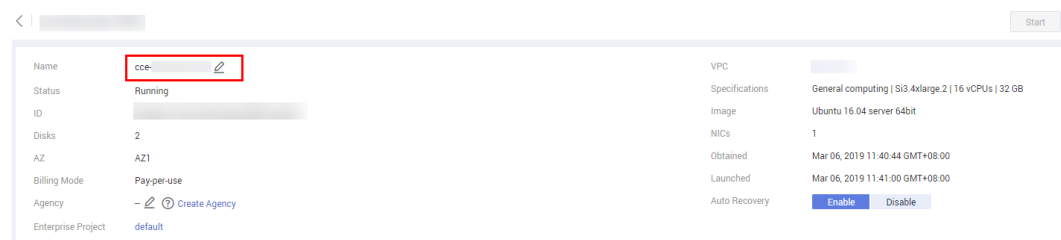


Figura 4-4 Comprobación del nombre del nodo en la máquina virtual y si el nodo puede iniciar sesión en

```
Authorized users only. All activities may be monitored and reported.
cce-iaas-w00401701-03473 login: [ 23.162056] ctnetlink_init: cannot register notifier.
[ 23.166732] ctnetlink_init: cannot register pernet operations
[ 25.059167] cloud-init[6192]: /usr/lib/python2.7/site-packages/Cheetah/Compiler.py:1509: UserWarning:
[ 25.059509] cloud-init[6192]: You don't have the C version of NameMapper installed! I'm disabling Cheetah's useStackFrames op
tion as it is painfully slow with the Python version of NameMapper. You should get a copy of Cheetah with the compiled C version
of NameMapper.
[ 25.060015] cloud-init[6192]: "\nYou don't have the C version of NameMapper installed! "
[ 25.209271] cloud-init[6192]: Cloud-init v. 0.7.9 running 'modules:final' at Fri, 22 Nov 2019 01:30:16 +0000. Up 25.05 second
s.
[ 25.259790] cloud-init[6192]: Cloud-init v. 0.7.9 finished at Fri, 22 Nov 2019 01:30:16 +0000. DataSource DataSourceOpenStack
[net.ver=2]. Up 25.25 seconds
[ 42.868017] ctnetlink_init: cannot register notifier.
[ 42.873117] ctnetlink_init: cannot register pernet operations

Authorized users only. All activities may be monitored and reported.
cce-iaas-w00401701-03473 login:
```

Si los nombres de nodo son inconsistentes y la contraseña y la clave no se pueden usar para iniciar sesión en el nodo, se produjeron problemas de Cloud-Init cuando se creó un ECS. En este caso, reinicie el nodo y envíe un ticket de servicio al personal de ECS para localizar la causa raíz.

----Fin

Concepto de comprobación 4: Si el grupo de seguridad está modificado

Inicie sesión en la consola de VPC. En el panel de navegación, elija **Access Control > Security Groups** y busque el grupo de seguridad del nodo principal del clúster.

El nombre de este grupo de seguridad tiene el formato de *Cluster name-cce-control-ID*. Se puede buscar el grupo de seguridad por **cluster name**.

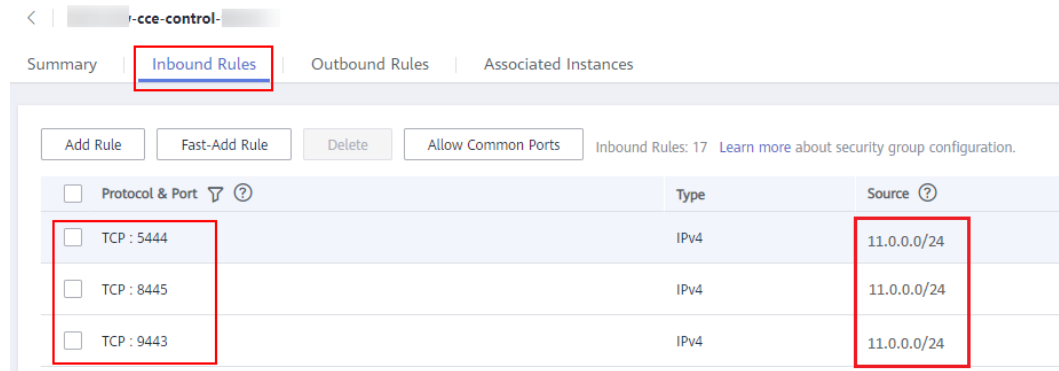
Compruebe si se modifican las reglas del grupo de seguridad. Para obtener más información, véase [Configuración de reglas de grupo de seguridad de clúster](#).

Concepto de comprobación 5: Si las reglas del grupo de seguridad contienen la política de grupo de seguridad para la comunicación entre el nodo principal y el nodo de trabajo

Compruebe si existe una política de grupo de seguridad de este tipo.

Cuando se agrega un nodo a un clúster existente, si se agrega un bloque CIDR extendido a la VPC correspondiente a la subred y la subred es un bloque CIDR extendido, necesita agregar las siguientes tres reglas de grupo de seguridad al grupo de seguridad del nodo principal (el nombre del grupo tiene el formato *Cluster name-cce-control-Random number*). Estas reglas garantizan que los nodos agregados al clúster estén disponibles. (Este paso no es necesario si se ha agregado un bloque CIDR extendido a la VPC durante la creación del clúster.)

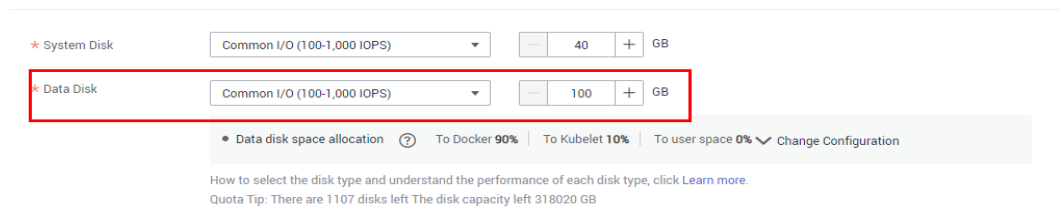
Para obtener más información acerca de la seguridad, consulte [Configuración de reglas de grupo de seguridad de clúster](#).



Concepto de comprobación 6: Si el disco es anormal

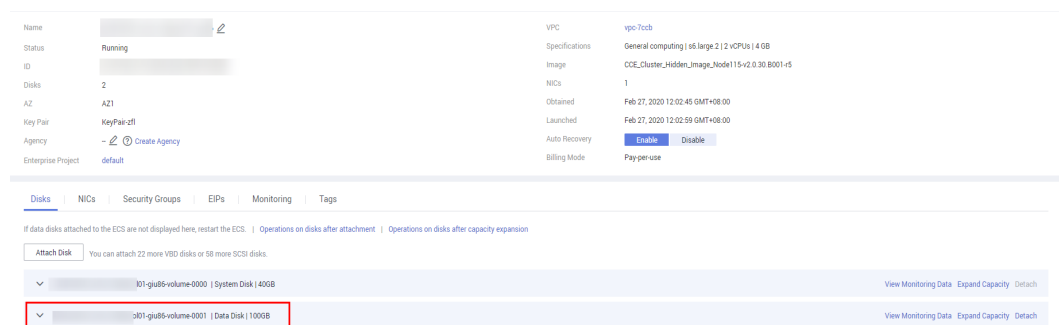
Un disco de datos de 100 GB dedicado a Docker está conectado al nuevo nodo. Si el disco de datos se desinstala o se daña, el servicio Docker se vuelve anormal y el nodo no está disponible.

Figura 4-5 Disco de datos asignado cuando se crea un nodo



Haga clic en el nombre del nodo para comprobar si se desinstala el disco de datos montado en el nodo. Si se desinstala el disco, vuelva a montar un disco de datos en el nodo y reinicie el nodo. Entonces el nodo puede ser recuperado.

Figura 4-6 Comprobación del disco



Concepto de comprobación 7: Si los componentes internos son normales

Paso 1 Inicie sesión en el ECS donde se encuentra el nodo no disponible.

Paso 2 Ejecute el siguiente comando para comprobar si los componentes PaaS son normales:

```
systemctl status kubelet
```

Si el comando se ejecuta correctamente, el estado de cada componente se muestra como **active**, como se muestra en la siguiente figura.

```
root@bms-cc-e-00406059-11044-sh[17029]: ~# systemctl status kubelet
kubelet.service - Cloud Container Engine Kubelet Service
Loaded: loaded (/usr/lib/systemd/system/kubelet.service; enabled; vendor preset: disabled)
Active: active (running) since Mon 2019-08-05 14:38:22 CST; 3 days ago
Main PID: 17029 (sudo)
Memory: 139.6M
CGroup: /system.slice/system-hostos.slice/kubelet.service
├─17029 sudo /var/paas/kubernetes/kubelet/srvkubelet start
├─17030 /bin/sh /var/paas/kubernetes/kubelet/srvkubelet start
└─17422 /usr/local/bin/kubelet --bootstrap-kubeconfig=/var/paas/kubernetes/kubelet/boot.conf --cert-dir=/var/paas/kubernetes/kubelet/pki --rotate-certificates=true ...
Aug 05 14:38:22 bms-cc-e-00406059-11044-sh[17029]: systemd[1]: Started Cloud Container Engine Kubelet Service.
Aug 05 14:38:22 bms-cc-e-00406059-11044-sh[17029]: systemd[1]: Starting Cloud Container Engine Kubelet Service: ...
Aug 05 14:38:22 bms-cc-e-00406059-11044-sh[17029]: sudo[17029]:     paws : TTY=unknown ; PWD=/ ; USER=root ; COMMAND=/var/paas/kubernetes/kubelet/srvkubelet start
Aug 05 14:38:22 bms-cc-e-00406059-11044-sh[17029]: sudo[17051]:     paws : TTY=unknown ; PWD=/ ; USER=root ; COMMAND=/bin/sh -c cat > /etc/resolv.conf <<EOF
Aug 05 14:38:28 bms-cc-e-00406059-11044-sh[17029]: 5 Aug 14:38:28 ntpdate[17054]: adjust time server 100.79.0.250 offset 0.014749 sec
Time: Some lines were ellipsized, use -l to show in full.
```

Si el estado del componente no es **active**, ejecute los siguientes comandos (usando el componente defectuoso **canal** como ejemplo):

Ejecute **systemctl restart canal** para reiniciar el componente.

Después de reiniciar el componente, ejecute **systemctl status canal** para comprobar el estado.

Paso 3 Si el comando de reinicio no se ejecuta, ejecute el siguiente comando para comprobar el estado de ejecución del proceso **monitrc**:

```
ps -ef | grep monitrc
```

Si el proceso **monitrc** existe, ejecute el siguiente comando para eliminar este proceso. El proceso **monitrc** se reiniciará automáticamente después de que se elimine.

```
kill -s 9 `ps -ef | grep monitrc | grep -v grep | awk '{print $2}'`
```

----Fin

Concepto de comprobación 8: Si la dirección DNS es correcta

Paso 1 Después de iniciar sesión en el nodo, compruebe si se registra algún error de resolución de nombres de dominio en el archivo **/var/log/cloud-init-output.log**.

```
cat /var/log/cloud-init-output.log | grep resolv
```

Si el resultado del comando contiene la siguiente información, el nombre de dominio no se puede resolver:

```
Could not resolve host: test.obs.ap-southeast-1.myhuaweicloud.com; Unknown error
```

Paso 2 En el nodo, haga ping al nombre de dominio que no se puede resolver en el paso anterior para comprobar si el nombre de dominio se puede resolver en el nodo.

```
ping test.obs.ap-southeast-1.myhuaweicloud.com
```

- Si no, el DNS no puede resolver la dirección IP. Compruebe si la dirección de DNS del archivo **/etc/resolv.conf** es la misma que la configurada en la subred de VPC. En la mayoría de los casos, la dirección DNS del archivo está configurada incorrectamente. Como resultado, el nombre de dominio no se puede resolver. Corrija la configuración de DNS de la subred de VPC y restablezca el nodo.
- Si es así, la configuración de la dirección de DNS es correcta. Compruebe si hay otras fallas.

----Fin

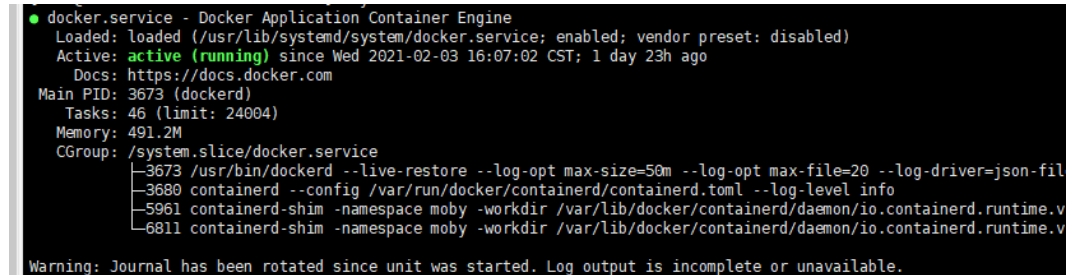
Concepto de comprobación 9: Si se elimina el disco vdb en el nodo

Si se elimina el disco vdb de un nodo, puede consultar [este tema](#) para restaurar el nodo.

Concepto de comprobación 10: Si el servicio Docker es normal

Paso 1 Ejecute el siguiente comando para comprobar si el servicio Docker se está ejecutando:

```
systemctl status docker
```



```
● docker.service - Docker Application Container Engine
   Loaded: loaded (/usr/lib/systemd/system/docker.service; enabled; vendor preset: disabled)
   Active: active (running) since Wed 2021-02-03 16:07:02 CST; 1 day 23h ago
     Docs: https://docs.docker.com
   Main PID: 3673 (dockerd)
    Tasks: 46 (limit: 24004)
   Memory: 491.2M
   CGroup: /system.slice/docker.service
           └─3673 /usr/bin/dockerd --live-restore --log-opt max-size=50m --log-opt max-file=20 --log-driver=json-fil
             └─3680 containerd --config /var/run/docker/containerd/containerd.toml --log-level info
               └─5961 containerd-shim -namespace moby -workdir /var/lib/docker/containerd/daemon/io.containerd.runtime.v
                 └─6811 containerd-shim -namespace moby -workdir /var/lib/docker/containerd/daemon/io.containerd.runtime.v

Warning: Journal has been rotated since unit was started. Log output is incomplete or unavailable.
```

Si el comando falla o el estado del servicio Docker no está activo, localice la causa o póngase en contacto con el soporte técnico si es necesario.

Paso 2 Ejecute el siguiente comando para comprobar el número de contenedores en el nodo:

```
docker ps -a | wc -l
```

Si el comando se suspende, la ejecución del comando tarda mucho tiempo, o hay más de 1000 contenedores anormales, compruebe si las cargas de trabajo se crean y eliminan repetidamente. Si con frecuencia se crean y eliminan un gran número de recipientes, puede ocurrir un gran número de recipientes anormales y no pueden despejarse de manera oportuna.

En este caso, detenga la creación y eliminación repetidas de la carga de trabajo o utilice más nodos para compartir la carga de trabajo. Generalmente, los nodos se restaurarán después de un periodo de tiempo. Si es necesario, ejecute el comando `docker rm {container_id}` para borrar manualmente los contenedores anormales.

----Fin

4.2.2 ¿Cómo soluciono los problemas de la falla al iniciar sesión de forma remota en un nodo en un clúster de CCE?

Después de crear un nodo en CCE, no puede iniciar sesión de forma remota en el nodo mediante SSH. Aparece un mensaje que indica que la clave seleccionada no se ha registrado en el host remoto. En este caso, el usuario raíz no puede iniciar sesión directamente en el nodo.

La causa es que el cloud-init está instalado en el nodo de CCE. Para el cloud-init, ya existe un usuario de Linux predeterminado y la clave del usuario también se usa para el dispositivo que ejecuta Linux.

Solución

Inicie sesión en el dispositivo como usuario **Linux** y ejecute el comando `sudo su` para cambiar al usuario **root**.

4.2.3 ¿Cómo inicio sesión en un nodo usando una contraseña y restablezco la contraseña?

Contexto

Al crear un nodo en CCE, seleccionó un par de claves o especificó una contraseña para iniciar sesión. Si olvida el par de claves o la contraseña, puede iniciar sesión en la consola de ECS para restablecer la contraseña del nodo. Después de restablecer la contraseña, puede iniciar sesión en el nodo con la contraseña.

Procedimiento

- Paso 1** Inicie sesión en la consola de ECS.
- Paso 2** En la lista de ECS, seleccione el tipo de servidor en la nube del nodo. En la misma fila que el nodo, elija **More > Stop**.
- Paso 3** Después de detener el nodo, elija **More > Reset Password** y siga las indicaciones en pantalla para restablecer la contraseña.
- Paso 4** Después de restablecer la contraseña, elija **More > Start** y haga clic en **Remote Login** para iniciar sesión en el nodo con la contraseña.

----Fin

4.2.4 ¿Cómo puedo recopilar logs de nodos en un clúster de CCE?

En las tablas siguientes se enumeran los archivos de log de los nodos de CCE.

Tabla 4-1 Logs de nodos en clústeres de v1.21 y posteriores

Nombre del log	Ruta
kubelet log	/var/log/cce/kubernetes/kubelet.log
kube-proxy log	/var/log/cce/kubernetes/kube-proxy.log
everest log (storage)	/var/log/cce/everest-csi-driver
yangtse log (networking)	/var/log/cce/yangtse
canal log	/var/log/cce/canal
System log	/var/log/messages

Tabla 4-2 Logs of nodes in clusters of v1.19 and earlier

Log Name	Path
kubelet log	/var/paas/sys/log/kubernetes/kubelet.log
kube-proxy log	/var/paas/sys/log/kubernetes/kube-proxy.log
everest log (storage)	/var/log/cce/everest-csi-driver

Log Name	Path
yangtse log (networking)	/var/paas/sys/log/yangtse
canal log	/var/paas/sys/log/canal
System log	/var/log/messages

4.2.5 ¿Qué puedo hacer si la red de contenedores no está disponible después de actualizar el sistema operativo?

La consola de CCE no admite las actualizaciones del sistema operativo en un nodo. Se recomienda no actualizar el sistema operativo mediante el comando **yum update**.

Si actualiza el sistema operativo mediante **yum update** la red del contenedor dejará de estar disponible.

Realice las siguientes operaciones para restaurar la red de contenedores:

AVISO

Este método de restauración es válido solo para EulerOS 2.2.

Paso 1 Ejecute el siguiente script como usuario **root**:

```
#!/bin/bash
function upgrade_kmod()
{
    openvswitch_mod_path=$(rpm -qal openvswitch-kmod)
    rpm_version=$(rpm -qal openvswitch-kmod|grep -w openvswitch|head -1|awk -F
"/" '{print $4}')
    sys_version=`cat /boot/grub2/grub.cfg | grep EulerOS|awk 'NR==1{print $3}' |
sed 's/[()]//g`

    if [[ "${rpm_version}" != "${sys_version}" ]];then
        mkdir -p /lib/modules/"${sys_version}"/extra/openvswitch
        for path in ${openvswitch_mod_path[@]};do
            name=$(echo "$path" | awk -F "/" '{print $NF}')
            rm -f /lib/modules/"${sys_version}"/updates/"${name}"
            rm -f /lib/modules/"${sys_version}"/extra/openvswitch/"${name}"
            ln -s "${path}" /lib/modules/"${sys_version}"/extra/openvswitch/"$
{name}"
        done
    fi
    depmod ${sys_version}
}
upgrade_kmod
```

Paso 2 Reinicie la VM.

----Fin

Enlaces útiles

- [Operaciones de alto riesgo en nodos de clúster](#)

4.2.6 ¿Qué debo hacer si el disco vdb de un nodo está dañado y el nodo no se puede recuperar después del restablecimiento?

Síntoma

El disco vdb de un nodo está dañado y el nodo no se puede recuperar después del reinicio.

Escenarios de errores

- En un nodo normal, elimine el LV y el VG. El nodo no está disponible.
- Restablezca un nodo anormal y se notifica un error de sintaxis. El nodo no está disponible.

La siguiente figura muestra los detalles.

```
vgcreate VG_new PV ...
create volume group error
, skip pause's work in case of failed dependency docker, skip fuxi's work in case of failed dependency docker, sk
work in case of failed dependency kubelet, skip kube-proxy's work in case of failed dependency config-prepare, sk
ork in case of failed dependency config-prepare, skip canal-agent's work in case of failed dependency fuxi, skip c
work in case of failed dependency config-prepare, skip docker's work in case of failed dependency config-prepare,
s work in case of failed dependency config-prepare]
[0525 17:22:55.835605 7116 install.go:361 install failed
Install Failed: [Install config-prepare failed: exit status 1, output: [ Mon May 25 17:22:53 CST 2020 ] start inst
pare
success download the file
success download the file
success download the file
success download the file
success download the file
success download the file
success download the file
success download the file
Checking device: /dev/vda
Raw disk /dev/vda has been partition, will skip this device
Checking device: /dev/vdb
Detected paas disk: /dev/vdb
Use to config lv(eg. docker(direct-lvm),kubelet,user)
No command with matching syntax recognised. Run 'vgcreate --help' for more information.
Correct command syntax is:
vgcreate VG_new PV ...

create volume group error
, skip pause's work in case of failed dependency docker, skip fuxi's work in case of failed dependency docker, sk
work in case of failed dependency kubelet, skip kube-proxy's work in case of failed dependency config-prepare, sk
ork in case of failed dependency config-prepare, skip canal-agent's work in case of failed dependency fuxi, skip c
work in case of failed dependency config-prepare, skip docker's work in case of failed dependency config-prepare,
s work in case of failed dependency config-prepare]
```

Localización de fallas

Si el grupo de volúmenes (VG) del nodo se elimina o se daña y no se puede identificar, primero debe restaurar manualmente el VG para evitar que los discos de datos se formateen por error durante el restablecimiento.

Solución

Paso 1 Inicie sesión en el nodo.

Paso 2 Cree un PV y un VG de nuevo. En este ejemplo, se muestra el siguiente mensaje de error:

```
root@host1:~# pvcreate /dev/vdb
Device /dev/vdb excluded by a filter
```

Esto se debe a que el disco agregado se crea en otra máquina virtual y tiene una tabla de particiones. La VM actual no puede identificar la tabla de particiones del disco. Necesita ejecutar los comandos **parted** tres veces para volver a crear la tabla de particiones.

```
root@host1:~# parted /dev/vdb
GNU Parted 3.2
Using /dev/vdb
Welcome to GNU Parted! Type 'help' to view a list of commands.
(parted) mklabel msdos
```

```
Warning: The existing disk label on /dev/vdb will be destroyed and all data on
this disk will be lost. Do you want to continue?
Yes/No? yes
(parted) quit
Information: You may need to update /etc/fstab.
```

Vuelve a ejecutar a **pvcreate**. Cuando el sistema le pregunte si desea borrar la firma del DOS, escriba **y**. El disco se crea como un PV.

```
root@host1:~# pvcreate /dev/vdb
WARNING: dos signature detected on /dev/vdb at offset 510. Wipe it? [y/n]: y
Wiping dos signature on /dev/vdb.
Physical volume "/dev/vdb" successfully created
```

Paso 3 Cree un VG.

Compruebe los discos Docker del nodo. Si los discos son **/dev/vdb** y **/dev/vdc**, ejecute el siguiente comando:

```
root@host1:~# vgcreate vgpaas /dev/vdb /dev/vdc
```

Si solo existe el disco **/dev/vdb**, ejecute el siguiente comando:

```
root@host1:~# vgcreate vgpaas /dev/vdb
```

Una vez completada la creación, restablezca el nodo.

---Fin

4.2.7 ¿Qué puertos se utilizan para instalar kubelet en los nodos del clúster de CCE?

Se utilizan los siguientes puertos:

- **10250 –port**: solía escuchar en kubelet. La API relacionada se puede usar para comprobar si kubelet se está ejecutando.
- **10248 –healthz-port**: utilizado para la comprobación de estado.
- **10255 –read-only-port**: puerto de solo lectura, al que se puede acceder directamente sin autenticación y autorización.
- **4194 –advisor-port**: utilizado por cAdvisor.

4.2.8 ¿Cómo configuro un pod para usar la capacidad de aceleración de un nodo de GPU?

Descripción del problema

He comprado un nodo de GPU, pero la velocidad de funcionamiento sigue siendo lenta. ¿Cómo configuro el pod para que utilice la capacidad de aceleración del nodo de GPU?

Solución

Solución 1:

Se recomienda quitar las manchas no programadas de los nodos de la GPU en el clúster, para que el controlador de complemento de GPU se pueda instalar correctamente. Además, es necesario instalar el controlador de GPU de una versión posterior.

Si no se despliega un contenedor en un nodo de GPU del clúster, puede configurar políticas de afinidad y antiafinidad para evitar que el contenedor se programe en el nodo de GPU.

Solución 2:

Se recomienda instalar el controlador de GPU de una versión posterior y utilizar kubectl para actualizar la configuración de complemento de GPU. Add the following configuration:

```
tolerations:  
- operator: "Exists"
```

Después de agregar la configuración, el controlador de complemento de GPU se puede instalar correctamente en el nodo de GPU con un taint.

4.2.9 ¿Qué debo hacer si la suspensión de E/S ocurre ocasionalmente cuando se usan discos SCSI de EVS?

Síntoma

Cuando se utilizan los discos SCSI de EVS y se crean y eliminan contenedores en un nodo CentOS, los discos se montan y desmontan con frecuencia. La velocidad de lectura/escritura del disco del sistema puede aumentar instantáneamente. Como resultado, el sistema se suspende, lo que afecta al nodo normal que se ejecuta.

Cuando se produce este problema, se muestra la siguiente información en el log dmesg:

```
Attached SCSI disk  
task jdb2/xxx blocked for more than 120 seconds.
```

Por ejemplo:

```
1128163.173120] sd 2:0:0:0: [sda] Write Protect is off  
1128163.173457] sd 2:0:0:0: [sda] Mode Sense: 69 00 00 08  
1128163.173573] sd 2:0:0:0: [sda] Write cache: disabled, read cache: enabled, doesn't support DPO or FUA  
1128163.176426] sd 2:0:0:0: [sda] Attached SCSI disk  
1128350.437941] INFO: task jbd2/dm-1-8:1604 blocked for more than 120 seconds.  
1128350.438267] "echo 0 > /proc/sys/kernel/hung_task_timeout_secs" disables this message.  
1128350.438564] jbd2/dm-1-8 D ffff9ede7f8420e0 0 1604 2 0x00000000  
1128350.438829] Call Trace:  
1128350.439120] [1128350.439394] [
```

Causa posible

Después de agregar un dispositivo PCI al BUS 0, el núcleo del SO Linux atravesará todos los puentes PCI montados en el BUS 0 varias veces, y estos puentes PCI no pueden funcionar correctamente durante este período. Durante este período, si el puente PCI utilizado por el dispositivo se actualiza, debido a un defecto del núcleo, el dispositivo considera que el puente PCI es anormal, y el dispositivo entra en un modo de falla y no puede funcionar normalmente. Si el front-end está escribiendo datos en el espacio de configuración PCI para que el back-end procese las E/S de disco, la operación de escritura puede eliminarse. Como resultado, el back-end no puede recibir notificaciones para procesar nuevas solicitudes en el anillo de E/S. Finalmente, se produce la suspensión de E/S de front-end.

Este problema es causado por un defecto del kernel de Linux. Para obtener más información, consulte los [defectos en las distribuciones de Linux](#).

Impacto

Los núcleos de CentOS Linux de versiones anteriores a 3.10.0-1127.el7 se ven afectados.

Solución

Actualice el núcleo a una versión posterior **restableciendo el nodo**. Para obtener más información, consulte [Restablecimiento de un nodo](#).

4.2.10 ¿Qué debo hacer si los logs excesivos de auditoría de Docker afectan a la E/S del disco?

Síntoma

Hay un gran número de logs de auditoría de Docker en los nodos existentes de algunos clústeres. Debido a defectos del kernel del sistema operativo, es ligeramente posible que las E/S estén suspendidas. Puede optimizar las reglas del log de auditoría para evitar este problema.

Impacto

Versiones de clúster afectadas:

- v1.15.11-r1
- v1.17.9-r0

AVISO

- Solo tiene que solucionar este problema para los nodos existentes, no para los nodos recién creados.
 - El componente auditado debe reiniciarse durante la actualización.
-

Método de comprobación

Paso 1 Inicie sesión en el nodo de trabajo como usuario **root**.

Paso 2 Ejecute el siguiente comando para comprobar si el problema existe en el nodo actual:

```
auditctl -l | grep "/var/lib/docker -p rwx -k docker"
```

Si se muestra la información similar a la siguiente, el problema existe y debe corregirse. Si no se muestra ningún resultado de comando, el nodo no se ve afectado.

```
[root@k8s-master-0002555 ~]# auditctl -l | grep "/var/lib/docker -p rwx -k docker"
-w /var/lib/docker -p rwx -k docker
```

----Fin

Solución

Paso 1 Inicie sesión en el nodo de trabajo como usuario **root**.

Paso 2 Ejecute los siguientes comandos:

```
sed -i "/var/lib/docker -k docker/d" /etc/audit/rules.d/docker.rules
```

```
service auditd restart
```

```
----Fin
```

Método de verificación

Ejecute el siguiente comando para comprobar si el error está rectificado:

```
auditctl -l | grep "/var/lib/docker -p rwx -k docker"
```

Si no se muestra ningún resultado del comando, el problema se ha resuelto.

4.2.11 ¿Cómo soluciono un contenedor o nodo anormal debido a que no hay espacio en disco de thin pool?

Descripción del problema

Cuando el espacio en disco de un thin pool en un nodo está a punto de agotarse, ocasionalmente se producen las siguientes excepciones:

No se pueden crear archivos o directorios en el contenedor, el sistema de archivos del contenedor es de solo lectura, el nodo está contaminado con la presión del disco o el nodo no está disponible.

Puede ejecutar el comando **docker info** en el nodo para ver el espacio utilizado y restante del thin pool para localizar el error. La siguiente figura es un ejemplo.

```
Storage Driver: devicemapper
Pool Name: vgpaas-thinpool
Pool Blocksize: 524.3kB
Base Device Size: 10.74GB
Backing Filesystem: ext4
Udev Sync Supported: true
Data Space Used: 7.794GB
Data Space Total: 71.94GB
Data Space Available: 64.15GB
Metadata Space Used: 3.076MB
Metadata Space Total: 3.221GB
Metadata Space Available: 3.218GB
Thin Pool Minimum Free Space: 7.194GB
Deferred Removal Enabled: true
Deferred Deletion Enabled: true
Deferred Deleted Device Count: 0
Library Version: 1.02.146-RHEL7 (2018-01-22)
```

Causa posible

Cuando se utiliza el mapeador de dispositivos Docker, aunque puede configurar el parámetro **basesize** para limitar el tamaño del directorio **/home** de un solo contenedor (a 10 GB de forma predeterminada), todos los contenedores del nodo siguen compartiendo el thin pool del nodo para el almacenamiento. No están completamente aislados. Cuando la suma del espacio de thin pool utilizado por ciertos recipientes alcanza el límite superior, otros recipientes no pueden funcionar correctamente.

Además, después de eliminar un archivo en el directorio **/home** del contenedor, el espacio de thin pool ocupado por el archivo no se libera inmediatamente. Por lo tanto, incluso si **basesize**

se establece en 10 GB, el espacio de thin pool ocupado por los archivos sigue aumentando hasta 10 GB cuando se crean archivos en el contenedor. El espacio liberado después de la eliminación del archivo se reutilizará solo después de un tiempo. Si **el número de contenedores de servicio en el nodo multiplicado por tamaño básico** es mayor que el tamaño del espacio de thin pool del nodo, existe la posibilidad de que se haya agotado el espacio de thin pool.

Solución

Cuando se agota el espacio de thin pool de un nodo, algunos servicios pueden migrarse a otros nodos para recuperar servicios rápidamente. Pero se recomienda utilizar las siguientes soluciones para resolver la causa raíz:

Solución 1:

Planifique correctamente la distribución del servicio y el espacio en disco del plano de datos para evitar el escenario donde **el número de contenedores de servicio multiplicado por el tamaño básico** es mayor que el tamaño del thin pool del nodo. Para ampliar el espacio del thin pool, consulte [Ampliación de la capacidad del disco del nodo](#).

Solución 2:

Cree y elimine archivos en contenedores de servicio en el almacenamiento local (por ejemplo, emptyDir y hostPath) o en el directorio de almacenamiento en la nube montado en el contenedor. Tales archivos no ocupan el espacio de thin pool.

Solución 3:

Si el sistema operativo utiliza OverlayFS, los servicios se pueden desplegar en dichos nodos para evitar el problema de que el espacio en disco ocupado por los archivos creados o eliminados en el contenedor no se libere inmediatamente.

4.2.12 ¿En qué puertos escucha un nodo?

Tabla 4-3 Puertos de escucha de un nodo de trabajo

Puerto de destino	Protocolo	Descripción
10248	TCP	Puerto de comprobación de estado para kubelet
10250	TCP	Puerto de servicio de kubelet para proporcionar información de monitoreo sobre cargas de trabajo en nodos y canales de acceso para contenedores
10255	TCP	Puerto de solo lectura de kubelet para proporcionar información de monitoreo sobre las cargas de trabajo en el nodo

Puerto de destino	Protocolo	Descripción
Puerto dinámico (relacionado con el rango de la máquina host, por ejemplo, el parámetro del kernel <code>net.ipv4.ip_local_port_range</code>)	TCP	Puerto aleatorio escuchado por kubelet, que se utiliza para comunicarse con CRI Shim para obtener el URL EXEC.
10249	TCP	Puerto métrico de kube-proxy para proporcionar información de monitoreo de kube-proxy
10256	TCP	Puerto de comprobación de estado para kube-proxy
Puerto dinámico (32768-65535)	TCP	Puerto de escucha de WebSocket para funciones como docker exec
Puerto dinámico (32768-65535)	TCP	Puerto de escucha de WebSocket para funciones como containerd exec
28001	TCP	Puerto de escucha local de ICAgent para recibir los registros de syslog del nodo
28002	TCP	Puerto de comprobación de estado para ICAgent
20101	TCP	Puerto de comprobación de estado de yangtse-agent/canal-agent (involucrado cuando se utiliza el modelo de red de túneles de contenedores)
20104	TCP	Puerto métrico de yangtse-agent/canal-agent para proporcionar información de monitoreo de componentes (involucrado cuando se utiliza el modelo de red de túnel de contenedores)
3125	TCP	Puerto de escucha de chequeo de estado de everest-csi-driver
3126	TCP	Puerto de pprof everest-csi-driver
19900	TCP	Puerto del servidor para la comprobación de estado de node-problem-detector

Puerto de destino	Protocolo	Descripción
19901	TCP	Puerto para conectar el detector de problemas de nodo a Prometheus para recopilar datos de monitorización
4789	UDP	Puerto de escucha de OVS, que se utiliza para transmitir paquetes VXLAN en redes de contenedores (involucrado cuando se utiliza el modelo de red de túnel de contenedores)
4789	UDPv6	Puerto de escucha de OVS, que se utiliza para transmitir paquetes VXLAN en redes de contenedores (involucrado cuando se utiliza el modelo de red de túnel de contenedores)
Puerto dinámico (30000-32767)	TCP	Puerto de escucha de kube-proxy para el balanceo de carga de capa 4. Kubernetes asigna un puerto aleatorio a Services de NodePort y de Loadbalancer. El número de puerto predeterminado oscila entre 30000 y 32767.
Puerto dinámico (30000-32767)	UDP	Puerto de escucha de kube-proxy para el balanceo de carga de capa 4. Kubernetes asigna un puerto aleatorio a Services de NodePort y de Loadbalancer. El número de puerto predeterminado oscila entre 30000 y 32767.
123	UDP	Puerto de escucha de ntpd utilizado para la sincronización de tiempo
20202	TCP	Puerto de escucha de PodLB para el balanceo de carga de capa 7, que reenvía las solicitudes de extracción de imágenes de contenedor.

4.2.13 ¿Cómo puedo rectificar fallas cuando se utiliza el controlador de NVIDIA para iniciar contenedores en nodos de GPU?

¿Se produjo un evento de error de programación de recursos en un nodo de clúster?

Síntomas

Un nodo se está ejecutando correctamente y tiene recursos de GPU. Sin embargo, se muestra la siguiente información de error:

0/9 nodos disponibles: 9 insuficiente nvidia.com/gpu

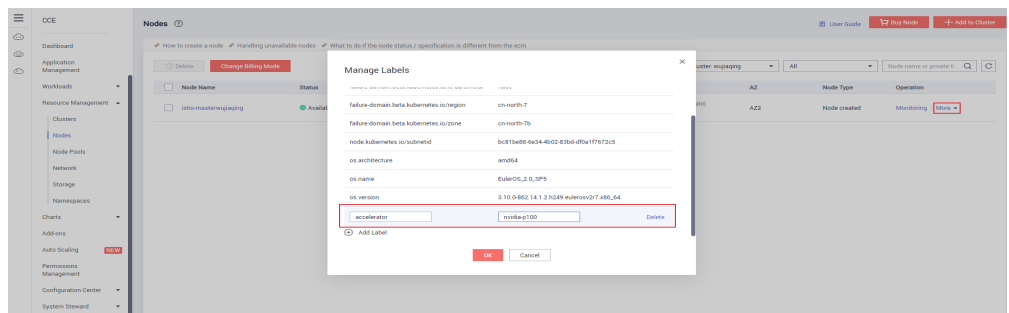
Análisis

1. Compruebe si el nodo está conectado con la etiqueta de NVIDIA.

```

root@chenyngdu-test-98835 ~]# kubectl get node --show-labels
NAME              STATUS    ROLES    AGE   VERSION   LABELS
172.16.0.180      Ready    <none>   6h26m v1.13.10-r1-CCE2.0.28.B001  accelerator=nvidia-p100, beta.kubernetes.io/arch=amd64, beta.kubernetes.io/os=linux, failure-domain.beta.kubernetes.io/is-hardware=cn-east-2b, failure-domain.beta.kubernetes.io/region=cn-east-2, failure-domain.beta.kubernetes.io/zone=cn-east-2b, kubernetes.io/availablezone=cn-east-2b, kubernetes.io/eni-quotas=12, kubernetes.io/hostname=172.16.0.180, node.kubernetes.io/subnet-id=4883a3c2-f89f-412d-bd3a-5a2892c5833a, os.architecture=amd64, os.name=EulerOS_2.0_SP5, os.version=3.10.0-862.14.1.2.h249.eulerosv2r7.x86_64
root@chenyngdu-test-98835 ~]#

```



2. Compruebe si el controlador de NVIDIA se está ejecutando correctamente.

Inicie sesión en el nodo donde se está ejecutando el complemento y vea el log de instalación del controlador en la siguiente ruta:

```
/opt/cloud/cce/nvidia/nvidia_installer.log
```

Vea los logs de salida estándar del contenedor de NVIDIA.

Filtre el ID del contenedor ejecutando el siguiente comando:

```
docker ps -a | grep nvidia
```

Vea los logs ejecutando el siguiente comando:

```
docker logs Container ID
```

¿Qué debo hacer si la versión de NVIDIA notificada por un servicio y la versión de CUDA no coinciden?

Ejecute el siguiente comando para comprobar la versión de CUDA en el contenedor:

```
cat /usr/local/cuda/version.txt
```

Compruebe si la versión de CUDA compatible con la versión del controlador de NVIDIA del nodo donde se encuentra el contenedor contiene la versión de CUDA del contenedor.

Enlaces útiles

[¿Qué debo hacer si se produce un error al desplegar un servicio en el nodo de GPU?](#)

4.3 Cambio de especificaciones

4.3.1 ¿Cómo cambio las especificaciones de nodo en un clúster de CCE?

Notas y restricciones

Los nodos de clúster de CCE Turbo de ciertas especificaciones solo se pueden crear en CCE y no se pueden modificar en la consola ECS. Puede invocar a la API de ECS para modificar las especificaciones. Para obtener más información, consulte [Modificación de las especificaciones de un ECS](#).

Solución

⚠ ATENCIÓN

Si el nodo cuyas especificaciones deben cambiarse se acepta en el clúster para su gestión, quite el nodo del clúster y, a continuación, cambie las especificaciones del nodo para evitar que afecten a los servicios.

- Paso 1** Inicie sesión en la consola de CCE y haga clic en el clúster. En el panel de navegación, elija **Nodes**. Haga clic en el nombre del nodo para mostrar la página de detalles de ECS.
- Paso 2** En la esquina superior derecha de la página de detalles de ECS, haga clic en **Stop**. Después de detener el ECS, elija **More > Modify Specifications**.
- Paso 3** En la página **Modify ECS Specifications**, seleccione un nombre de la variante y haga clic en **Submit** para finalizar la modificación de la especificación. Vuelva a la página de lista de ECS y elija **More > Start** para iniciar el ECS.
- Paso 4** Inicie sesión en la consola de CCE y haga clic en el clúster. En el panel de navegación, elija **Nodes**. Busque el nodo de destino en la lista de nodos y haga clic en **Sync Server Data** en la columna **Operation**. Una vez completada la sincronización, puede ver que las especificaciones de nodo son las mismas que las especificaciones modificadas del ECS.

---Fin

Problemas comunes

Después de cambiar las especificaciones de un nodo configurado con políticas de gestión de CPU, es posible que el nodo no se reinicie o que no se creen cargas de trabajo. En este caso, consulte [¿Qué debo hacer si no puedo reiniciar o crear cargas de trabajo en un nodo después de modificar las especificaciones del nodo?](#) para rectificar la falla.

4.3.2 ¿Qué debo hacer si no puedo reiniciar o crear cargas de trabajo en un nodo después de modificar las especificaciones del nodo?

Contexto

La opción de kubelet **cpu-manager-policy** es **static** por defecto, permitiendo que los pods con ciertas características de recursos reciban una mayor afinidad de CPU y exclusividad en el nodo. Si modifica las especificaciones del nodo de CCE en la consola de ECS, la información original de la CPU no coincide con la nueva información de la CPU. Como resultado, las cargas de trabajo del nodo no se pueden reiniciar ni crear.

Para obtener más información, consulte [Control de políticas de gestión de CPU en el nodo](#).

Impacto

Los clústeres que han habilitado una política de gestión de CPU se verán afectados.

Solución

Paso 1 Inicie sesión en el nodo de CCE (ECS) y elimine el archivo **cpu_manager_state**.

Ejemplo de comando para la eliminación de archivos:

```
rm -rf /mnt/paas/kubernetes/kubelet/cpu_manager_state
```

Paso 2 Reinicie el nodo o kubelet. El siguiente es el comando de reinicio kubelet:

```
systemctl restart kubelet
```

Paso 3 Compruebe que las cargas de trabajo del nodo se pueden reiniciar o crear correctamente.

----Fin

4.3.3 ¿Puedo cambiar la dirección IP de un nodo en un clúster de CCE?

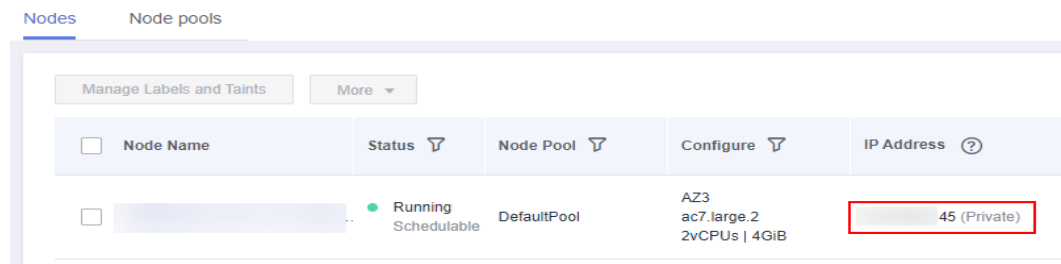
- IP privada: No. Actualmente, los clústeres de CCE utilizan la IP privada de un nodo como nombre de nodo de Kubernetes, que no se puede cambiar. Cambiar el nombre hará que el nodo no esté disponible.
- IP pública: Sí. La IP pública de un nodo se puede cambiar en la consola de ECS.

¿Cómo puedo restaurar un nodo después de cambiar su IP privada?

Después de cambiar la IP privada de un nodo, el nodo no está disponible. Necesita cambiarlo de nuevo a la IP original.

Paso 1 En la consola de CCE, vea los detalles del nodo y busque la dirección IP y la subred del nodo.

Figura 4-7 Dirección IP privada y subred del nodo



Paso 2 Inicie sesión en la consola de ECS, localice y detenga el nodo, vaya a la página de detalles del nodo y cambie la dirección IP privada en la página de ficha **Network Interfaces**. Tenga en cuenta que debe seleccionar la subred correspondiente.

Figura 4-8 Cambio de la dirección IP privada

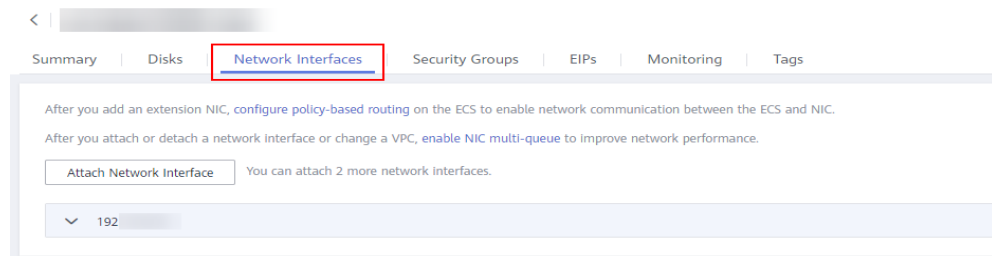
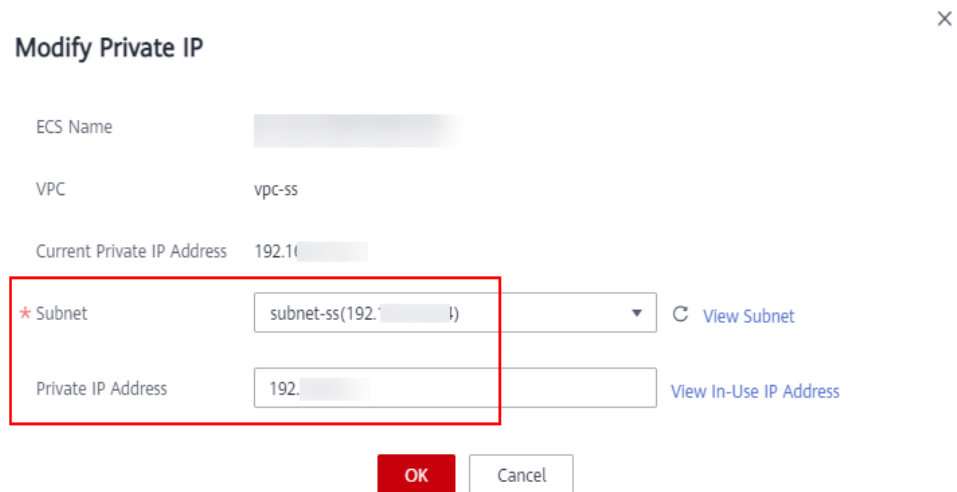


Figura 4-9 Cambio de la dirección IP privada



Paso 3 Una vez completada la modificación, reinicie el nodo.

----Fin

4.4 Núcleo de nodos

4.4.1 Cuando las aplicaciones se crean y eliminan repetidamente en un nodo de CentOS con una versión de kernel anterior, se produce una fuga de cgroup Kmem de vez en cuando

Síntoma

En escenarios donde la versión del núcleo de los nodos de CentOS 7.6 es anterior a 3.10.0-1062.12.1.el7.x86_64 (principalmente en clústeres de la versión 1.17.9), la fuga de cgroup kmem ocurre cuando las aplicaciones se crean repetidamente. Como resultado, hay memoria de nodo pero no se pueden crear nuevos nodos, y se muestra el mensaje de error "Cannot allocate memory" (No se puede asignar memoria).

Causa posible

Cuando se crea una aplicación repetidamente, se crea un cgroup de memoria temporal. Sin embargo, cuando se elimina la aplicación, el núcleo ha eliminado el cgroup (se ha eliminado el directorio cgroup correspondiente de `/sys/fs/cgroup/memory`), pero el cgroup no se libera en el núcleo. Como resultado, el núcleo considera que el número real de cgroups es inconsistente. Cuando el número de cgroups residuales alcanza el límite superior del nodo, no se pueden crear pods en el nodo.

Solución

- Utilice el parámetro `cgroup.memory=nokmem` globalmente en el núcleo para deshabilitar kmem para evitar fugas.
- Los clústeres de v1.17 ya no se mantienen. Para resolver este problema, actualice el clúster a v1.19 o posterior y restablezca el sistema operativo del nodo a la versión más reciente. Asegúrese de que la versión del núcleo es posterior a 3.10.0-1062.12.1.el7.x86_64.

4.4.2 Problemas causados por la configuración `conn_reuse_mode` en el modo de reenvío IPVS de clústeres de CCE

Síntoma

En el modo de reenvío IPVS utilizado en un clúster de CCE, puede haber una latencia de 1 segundo cuando un Service accede al clúster de CCE. Esto se debe a un error en la reutilización de las conexiones IPVS de Kubernetes.

Parámetro de reutilización de conexión de IPVS

La política de reutilización de puertos de IPVS viene determinada por el parámetro `net.ipv4.vs.conn_reuse_mode` del núcleo.

1. Si `net.ipv4.vs.conn_reuse_mode` se establece en `0`, IPVS no reprograma una nueva conexión, sino que reenvía la nueva conexión al RS original (IPVS backend).
2. Si `net.ipv4.vs.conn_reuse_mode` se establece en `1`, IPVS reprograma una nueva conexión.

Problemas causados por la reutilización de la conexión de IPVS

- **Problema 1**

Si `net.ipv4.vs.conn_reuse_mode` se establece en **0**, IPVS no programa de forma proactiva nuevas conexiones con reutilización de puertos ni activa ninguna operación de terminación o desconexión de la conexión. Los paquetes de datos de las nuevas conexiones se reenviarán directamente al RS original. Si se ha eliminado el pod de backend, se produce una excepción. Sin embargo, de acuerdo con la lógica de implementación actual, el RS no será borrado por kube-proxy siempre y cuando las solicitudes de conexión para la reutilización del puerto se envíen continuamente.

- **Problema 2**

Si `net.ipv4.vs.conn_reuse_mode` se establece en **1**, si el puerto de origen es el mismo que el de una conexión anterior en un escenario de alta simultaneidad, la conexión no se reutiliza sino que se reprograma. De acuerdo con la lógica de procesamiento de `ip_vs_in()`, si `net.ipv4.vs.contrack` está habilitado, se descarta el primer paquete SYN. Como resultado, el paquete SYN se retransmitirá, conduciendo a una latencia de 1 segundo. Como resultado, el rendimiento se deteriora.

Configuración de la comunidad e impacto en los clústeres de CCE

En Kubernetes 1.17 y versiones anteriores, el valor predeterminado de `net.ipv4.vs.conn_reuse_mode` es **0**. A partir de Kubernetes 1.19, puede determinar si habilitar `net.ipv4.vs.conn_reuse_mode` en función de la versión del núcleo. Si la versión del núcleo es posterior a 4.1, establezca `net.ipv4.vs.conn_reuse_mode` en **1**. En otros casos, conserve el valor predeterminado **0**.

Impacto en los nodos de CCE

1. En clústeres de CCE de 1.17 y versiones anteriores, si se utiliza IPVS para reenviar datos, el **problema 1** se produce cuando `net.ipv4.vs.conn_reuse_mode` se establece en **0**. El RS no se puede quitar debido a la reutilización del puerto.
2. En los clústeres de CCE de 1.19:
 - Si está utilizando EulerOS 2.5 o CentOS 7.6, el **problema 1** se produce cuando `net.ipv4.vs.conn_reuse_mode` se establece en **0**. El RS no se puede quitar debido a la reutilización del puerto.
 - Si está usando EulerOS 2.9 o Ubuntu 18.04, el **problema 2** se produce cuando `net.ipv4.vs.conn_reuse_mode` se establece en **1**. Se produce una latencia de 1 segundo en escenarios de alta simultaneidad.

Sugerencias

Si los problemas anteriores afectan a sus servicios, tome las siguientes medidas:

1. Utilice un clúster cuyo modo de reenvío sea iptables.
2. Si el impacto de este problema es leve, seleccione una versión del sistema operativo adecuada para clústeres de 1.19.

Plan de Rectificación

CCE ha solucionado los problemas relacionados en EulerOS 2.9. Restablezca el nodo o crear un nuevo nodo para resolver el problema.

Se han corregido las siguientes versiones del kernel:

- x86: 4.18.0-147.5.1.6.h686.eulerosv2r9.x86_64
- Arm: 4.19.90-vhulk2103.1.0.h584.eulerosv2r9.aarch64

Problema de la comunidad de Kubernetes: <https://github.com/kubernetes/kubernetes/issues/81775>

4.4.3 ¿Por qué los pods son desalojados por kubelet debido a estadísticas anormales de cgroup?

Síntoma

En un nodo de brazo, los pod son desalojados por kubelet debido a las estadísticas anormales de cgroup. Como resultado, el nodo funciona anormalmente.

kubelet sigue desalojando los pod. Después de que todos los contenedores están muertos, kubelet todavía considera que la memoria es insuficiente.

```

0621 14:33:26.820449 5176 setters.go:74] Using node IP: "192.168.160.181"
0621 14:33:27.866390 5176 eviction_manager.go:395] eviction manager: attempting to reclaim memory
0621 14:33:27.866453 5176 eviction_manager.go:406] eviction manager: must evict pod(s) to reclaim memory
0621 14:33:27.866466 5176 eviction_manager.go:417] eviction manager: eviction thresholds have been met, but no pods are active to evict
0621 14:33:36.826267 5176 setters.go:74] Using node IP: "192.168.160.181"
0621 14:33:37.953876 5176 eviction_manager.go:395] eviction manager: attempting to reclaim memory
0621 14:33:37.953941 5176 eviction_manager.go:406] eviction manager: must evict pod(s) to reclaim memory
0621 14:33:37.953954 5176 eviction_manager.go:417] eviction manager: eviction thresholds have been met, but no pods are active to evict
0621 14:33:46.830638 5176 setters.go:74] Using node IP: "192.168.160.181"
0621 14:33:48.041573 5176 eviction_manager.go:395] eviction manager: attempting to reclaim memory
0621 14:33:48.041639 5176 eviction_manager.go:406] eviction manager: must evict pod(s) to reclaim memory
0621 14:33:48.041654 5176 eviction_manager.go:417] eviction manager: eviction thresholds have been met, but no pods are active to evict
0621 14:33:56.842191 5176 setters.go:74] Using node IP: "192.168.160.181"
0621 14:33:58.129728 5176 eviction_manager.go:395] eviction manager: attempting to reclaim memory
0621 14:33:58.129794 5176 eviction_manager.go:406] eviction manager: must evict pod(s) to reclaim memory
0621 14:33:58.129809 5176 eviction_manager.go:417] eviction manager: eviction thresholds have been met, but no pods are active to evict
0621 14:34:06.846538 5176 setters.go:74] Using node IP: "192.168.160.181"
0621 14:34:08.217755 5176 eviction_manager.go:395] eviction manager: attempting to reclaim memory
0621 14:34:08.217832 5176 eviction_manager.go:406] eviction manager: must evict pod(s) to reclaim memory
0621 14:34:08.217845 5176 eviction_manager.go:417] eviction manager: eviction thresholds have been met, but no pods are active to evict

```

De hecho, el uso de recursos es normal.

```

top - 14:34:46 up 135 days, 22:42, 2 users, load average: 0.09, 0.17, 0.17
Tasks: 222 total, 1 running, 221 sleeping, 0 stopped, 0 zombie
%Cpu(s): 0.3 us, 1.4 sy, 0.0 ni, 98.2 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st
MiB Mem : 22.9/15509.0 [|||||||||||||||||||||]
MiB Swap: 0.0/0.0 [ ]

```

El valor de `usage_in_bytes` de cgroup en el directorio `/sys/fs/cgroup/memory` es anormal.

```

# cd /sys/fs/cgroup/memory
# cat memory.usage_in_bytes
17618837504

```

Causa posible

En un nodo Arm, el núcleo de EulerOS 2.8 y 2.9 tiene un error, que hace que kubelet desaloje los pods y resulta en la falta de disponibilidad del servicio.

📖 NOTA

Este problema se ha resuelto en las siguientes versiones:

- EulerOS 2.8: kernel-4.19.36-vhulk1907.1.0.h1088.eulerosv2r8.aarch64
- EulerOS 2.9: kernel-4.19.90-vhulk2103.1.0.h539.eulerosv2r9.aarch64

Solución

- Si la versión de clúster es 1.19.16-r0, 1.21.7-r0, 1.23.5-r0, 1.25.1-r0 o posterior, restablezca el sistema operativo del nodo a la versión más reciente.

- Si la versión de clúster no cumple con los requisitos, actualice el clúster a la versión especificada y, a continuación, restablezca el sistema operativo del nodo a la versión más reciente.

4.4.4 Cuando se produce OOM del contenedor en el nodo de CentOS con una versión anterior del kernel, el sistema de archivos Ext4 se suspende ocasionalmente

Síntoma

Si la versión del núcleo de un nodo de CentOS 7.6 es anterior a 3.10.0-1160.66.1.el7.x86_64 y OOM ocurre en el contenedor en el nodo, es posible que no se pueda acceder a todos los contenedores en el nodo y procesos tales como Docker y jdb están en el estado D. La falla se rectifica después de reiniciar el nodo.

```
[<ffffffff99986832>] ? mutex_lock+0x12/0x2f
[<ffffffff9944d243>] do_sync_write+0x93/0xe8
[<ffffffff9944dd38>] vfs_write+0xc8/0x1f8
[<ffffffff9944eb8f>] Sys_write+0x7f/0xf8
[<ffffffff99994f92>] system call fastpath+0x25/0x2a
INFO: task dockerd:4393 blocked for more than 120 seconds.
"echo 0 > /proc/sys/kernel/hung_task_timeout_secs" disables this
dockerd      D ffff8bc      0 4393      1 0x00000000
Call Trace:
[<ffffffff99987dd9>] schedule+0x29/0x78
[<ffffffffffc8358885>] wait_transaction_locked+0x85/0xd8 [jbd2]
[<ffffffff992c6f88>] ? wake_up_atomic_t+0x38/0x38
[<ffffffffffc8358378>] add_transaction_credits+0x278/0x318 [jbd2]
```

Causa posible

Quando el uso de memoria de un contenedor de servicio excede su límite de memoria, se activa OOM de cgroup y el núcleo del sistema termina el contenedor. El contenedor de cgroup de OOM activa ocasionalmente la suspensión del sistema de archivos ext4 en CentOS 7, y ext4/jbd2 se suspende permanentemente debido al bloqueo. Todas las tareas que realizan la operación de E/S en el sistema de archivos se ven afectadas.

Solución

- Solución temporal: Reinicie el nodo para rectificar temporalmente la falla.
- Evolución a largo plazo:
 - Si la versión de clúster es 1.19.16-r0, 1.21.7-r0, 1.23.5-r0, 1.25.1-r0 o posterior, restablezca el sistema operativo del nodo a la versión más reciente.
 - Si la versión de clúster no cumple con los requisitos, actualice el clúster a la versión especificada y, a continuación, restablezca el sistema operativo del nodo a la versión más reciente.

5 Grupo de nodos

5.1 ¿Qué debo hacer si no se muestra ningún registro de creación de nodos cuando se está expandiendo el grupo de nodos?

Síntoma

El grupo de nodos sigue estando en el estado de expansión, pero no se muestra ningún registro de creación de nodos en el registro de operación.

Solución de problemas

Comprobar y rectificar las fallas siguientes:

- Si el tenant está en mora o el papel del token está restringido.
- Si los nodos de esta variante se han agotado.
- Si el ECS o la cuota de memoria del tenant es insuficiente.
- Si la capacidad de ECS del tenant no se verifica. Si se crean demasiados nodos a la vez, la verificación de capacidad puede fallar.

Solución

- Si el tenant está en mora, renueve la cuenta lo antes posible.
- Si los nodos de ECS de una variante se han agotado, utilice los nodos de otras variantes.
- Si la cuota de ECS o de memoria es insuficiente, aumente la cuota.
- Si la verificación de la capacidad de ECS falla, realice la verificación de nuevo.

6 Carga de trabajo

6.1 Anomalías de la carga de trabajo

6.1.1 ¿Cómo uso eventos para corregir cargas de trabajo anormales?

Si una carga de trabajo es anormal, primero puede comprobar los eventos de pod para localizar la falla y luego corregirla haciendo referencia a [Tabla 6-1](#).

Tabla 6-1 Métodos de resolución de problemas

Información del evento	Estado del pod	Solución
Error al programar los pods.	Pending	Para obtener más información, véase ¿Qué debo hacer si falla la programación de pods? .
Error al extraer imágenes.	ImagePullBackOff	Para obtener más información, véase ¿Qué debo hacer si un pod no logra extraer la imagen? .
Error al iniciar contenedores.	CreateContainerError CrashLoopBackOff	Para obtener más información, véase ¿Qué debo hacer si falla el inicio del contenedor? .
El estado de la cápsula es de Evicted y la cápsula sigue siendo desalojada.	Evicted	Para obtener más información, véase ¿Qué debo hacer si un pod no es desalojado? .

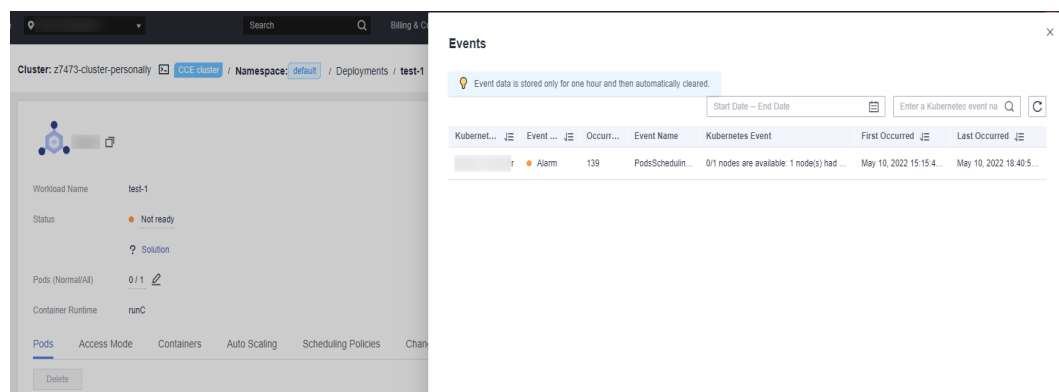
Información del evento	Estado del pod	Solución
El volumen de almacenamiento no se puede montar en la cápsula.	Pending	Para obtener más información, véase ¿Qué debo hacer si no se puede montar un volumen de almacenamiento o si el tiempo de montaje se agota? .
La cápsula se mantiene Creating .	Creating	Para obtener más información, véase ¿Qué debo hacer si una carga de trabajo permanece en el estado de creación? .
El pod se mantiene Terminating .	Terminating	Para obtener más información, véase ¿Qué debo hacer si no se pueden eliminar los pods en el estado de terminación? .
El estado de la cápsula es Stopped .	Stopped	Para obtener más información, véase ¿Qué debo hacer si una carga de trabajo se detiene debido a la eliminación de pods? .

Consulta de eventos de pod

Ejecute el comando `kubectl describe pod pod name` para ver los eventos de pod o inicie sesión en la consola de CCE y vea los eventos de pod en la página de detalles de la carga de trabajo.

```
$ kubectl describe pod prepare-58bd7bdf9-fthrp
...
Events:
  Type       Reason             Age   From                    Message
  ----       -
  Warning    FailedScheduling   49s   default-scheduler      0/2 nodes are available: 2
  Insufficient cpu.
  Warning    FailedScheduling   49s   default-scheduler      0/2 nodes are available: 2
  Insufficient cpu.
```

Figura 6-1 Consulta de eventos de pod



6.1.2 ¿Qué debo hacer si falla la programación de pods?

Localización de fallas

Si el pod se encuentra en el estado **Pending** y el evento contiene información de falla de programación de pod, localice la causa basándose en la información del evento. Para obtener más información acerca de cómo ver eventos, consulte [¿Cómo uso eventos para corregir cargas de trabajo anormales?](#).

Proceso de solución de problemas

Determine la causa basándose en la información del evento, tal como aparece en [Tabla 6-2](#).

Tabla 6-2 Error de programación de pod

Información del evento	Motivo y solución
no nodes available to schedule pods.	No hay ningún nodo disponible en el clúster. Concepto de comprobación 1: Si un nodo está disponible en el clúster
0/2 nodes are available: 2 Insufficient cpu. 0/2 nodes are available: 2 Insufficient memory.	Los recursos de nodo (CPU y memoria) son insuficientes. Concepto de comprobación 2: Si los recursos de nodo (CPU y memoria) son suficientes
0/2 nodes are available: 1 node(s) didn't match node selector, 1 node(s) didn't match pod affinity rules, 1 node(s) didn't match pod affinity/anti-affinity.	Las configuraciones de afinidad de nodo y pod son mutuamente excluyentes. Ningún nodo cumple con los requisitos del pod. Concepto de comprobación 3: Configuración de afinidad y antiafinidad de la carga de trabajo
0/2 nodes are available: 2 node(s) had volume node affinity conflict.	El volumen de EVS montado en el pod y el nodo no están en la misma AZ. Concepto de comprobación 4: Si el volumen y el nodo de la carga de trabajo residen en la misma AZ
0/1 nodes are available: 1 node(s) had taints that the pod didn't tolerate.	Existen marcas en el nodo, pero el pod no puede tolerar estas manchas. Concepto de comprobación 5: Toleración a la mancha de los pods
0/7 nodes are available: 7 Insufficient ephemeral-storage.	El espacio de almacenamiento efímero del nodo es insuficiente. Concepto de comprobación 6: Uso del volumen efímero

Información del evento	Motivo y solución
0/1 nodes are available: 1 everest driver not found at node	El controlador everest-csi en el nodo no está en el estado de ejecución. Concepto de comprobación 7: Si everest funciona correctamente
Failed to create pod sandbox: ... Create more free space in thin pool or use dm.min_free_space option to change behavior	El espacio de thin pool del nodo es insuficiente. Concepto de comprobación 8: Espacio de thin pool

Concepto de comprobación 1: Si un nodo está disponible en el clúster

Inicie sesión en la consola de CCE y compruebe si el estado del nodo es **Available**.

Alternativamente, ejecute el siguiente comando para comprobar si el estado del nodo es de **Ready**:

```
$ kubectl get node
NAME                STATUS    ROLES    AGE   VERSION
192.168.0.37        Ready    <none>   21d   v1.19.10-r1.0.0-source-121-gb9675686c54267
192.168.0.71        Ready    <none>   21d   v1.19.10-r1.0.0-source-121-gb9675686c54267
```

Si el estado de todos los nodos es **Not Ready**, no hay ningún nodo disponible en el clúster.

Solución

- Agregue un nodo. Si no se configura una política de afinidad para la carga de trabajo, el pod se migrará automáticamente al nuevo nodo para garantizar que los servicios se ejecuten correctamente.
- Localice el nodo no disponible y rectifique el error. Para obtener más información, véase [¿Qué debo hacer si un clúster está disponible pero algunos nodos no están disponibles?](#).
- Restablezca el nodo no disponible. Para obtener más información, consulte [Restablecer un nodo](#).

Concepto de comprobación 2: Si los recursos de nodo (CPU y memoria) son suficientes

0/2 nodes are available: 2 Insufficient cpu. Esto significa que no quedan CPU suficientes.

0/2 nodes are available: 2 Insufficient memory. Esto significa la memoria insuficiente.

Si los recursos solicitados por el pod exceden los recursos asignables del nodo donde se ejecuta el pod, el nodo no puede proporcionar los recursos requeridos para ejecutar nuevos pods y la planificación del pod en el nodo fallará definitivamente.

Node Name	Status	Roles	IP Address	Pods (Allocat...)	CPU Request...	Memory Request...	Runtime Versio... OS Version
example2-75620...	Run... Scheduled	DefaultP...	AZ3 c7.xlarge.2 4vCPUs 8GiB	10.1.0.55...	8 / 110	52.3% 88.01%	57.36% 93.37% docker//18.9.0 EulerOS 2.0 (S...

Si el número de recursos que se pueden asignar a un nodo es menor que el número de recursos que solicita un pod, el nodo no cumple los requisitos de recursos del pod. Como resultado, la programación falla.

Solución

Agregar nodos al clúster. La ampliación es la solución común a la insuficiencia de recursos.

Concepto de comprobación 3: Configuración de afinidad y antiafinidad de la carga de trabajo

Las políticas de afinidad inapropiadas causarán un error en la programación de pods.

Ejemplo:

Se establece una relación antiafinidad entre la carga de trabajo 1 y la carga de trabajo 2. La carga de trabajo 1 se despliega en el nodo 1 mientras que la carga de trabajo 2 se despliega en el nodo 2.

Cuando intenta desplegar la carga de trabajo 3 en el nodo 1 y establecer una relación de afinidad con la carga de trabajo 2, se produce un conflicto, lo que resulta en un error de despliegue de la carga de trabajo.

0/2 nodes are available: 1 node(s) no coincidió con **node selector**, 1 nodo (s) no coincidió con **pod affinity rules**, 1 nodo (s) no coincidió con **pod affinity/anti-affinity**.

- **node selector** indica que no se cumple la afinidad del nodo.
- **pod affinity rules** indican que no se cumple la afinidad del pod.
- **pod affinity/anti-affinity** indica que no se cumple la afinidad/antiafinidad del pod.

Solución

- Al agregar la afinidad de carga de trabajo-carga de trabajo y las políticas de afinidad de carga de trabajo-nodo, asegúrese de que los dos tipos de políticas no entren en conflicto. De lo contrario, el despliegue de carga de trabajo fallará.
- Si la carga de trabajo tiene una política de afinidad de nodo, asegúrese de que **supportContainer** en la etiqueta del nodo de afinidad está establecido en **true**. De lo contrario, los pods no se pueden programar en el nodo de afinidad y se genera el siguiente evento:

```
No nodes are available that match all of the following predicates: MatchNodeSelector, NodeNotSupportsContainer
```

Si el valor es de **false**, la programación falla.

Concepto de comprobación 4: Si el volumen y el nodo de la carga de trabajo residen en la misma AZ

0/2 nodes are available: 2 node(s) had volume node affinity conflict. Se produce un conflicto de afinidad entre volúmenes y nodos. Como resultado, la programación falla.

Esto se debe a que los discos de EVS no se pueden conectar a los nodos entre las AZ. Por ejemplo, si el volumen de EVS se encuentra en AZ 1 y el nodo se encuentra en AZ 2, la planificación falla.

El volumen de EVS creado en CCE tiene la configuración de afinidad de forma predeterminada, como se muestra a continuación.

```
kind: PersistentVolume
apiVersion: v1
metadata:
  name: pvc-c29bfac7-efa3-40e6-b8d6-229d8a5372ac
spec:
  ...
  nodeAffinity:
    required:
      nodeSelectorTerms:
        - matchExpressions:
            - key: failure-domain.beta.kubernetes.io/zone
              operator: In
              values:
                - ap-southeast-1a
```

Solución

En la AZ donde reside el nodo de la carga de trabajo, cree un volumen. Alternativamente, cree una carga de trabajo idéntica y seleccione un volumen de almacenamiento en la nube asignado automáticamente.

Concepto de comprobación 5: Toleración a la mancha de los pods

0/1 nodes are available: 1 node(s) had taints that the pod didn't tolerate. Esto significa que el nodo está contaminado y el pod no se puede programar para el nodo.

Comprueba las manchas en el nodo. Si se muestra la siguiente información, existen manchas en el nodo:

```
$ kubectl describe node 192.168.0.37
Name:          192.168.0.37
...
Taints:        key1=value1:NoSchedule
...

```

En algunos casos, el sistema agrega automáticamente una mancha a un nodo. Las manchas incorporadas actuales incluyen:

- `node.kubernetes.io/not-ready`: El nodo no está listo.
- `node.kubernetes.io/unreachable`: El controlador de nodo no puede acceder al nodo.
- `node.kubernetes.io/memory-pressure`: El nodo tiene presión de memoria.
- `node.kubernetes.io/disk-pressure`: El nodo tiene presión de disco. Siga las instrucciones descritas en [Concepto de comprobación 4: Si el espacio en disco del nodo es insuficiente](#) para manejarlo.
- `node.kubernetes.io/pid-pressure`: El nodo está bajo presión de PID. Siga las instrucciones en [Cambio de límites del ID de proceso \(kernel.pid_max\)](#) para manejarlo.
- `node.kubernetes.io/network-unavailable`: La red del nodo no está disponible.
- `node.kubernetes.io/unschedulable`: No se puede programar el nodo.
- `node.cloudprovider.kubernetes.io/uninitialized`: Si se especifica un controlador de plataforma en la nube externo cuando se inicia kubelet, kubelet agrega una mancha al nodo actual y lo marca como no disponible. Después de que **cloud-controller-manager** inicialice el nodo, kubelet elimina la mancha.

Solución

Para programar el pod en el nodo, utilice uno de los métodos siguientes:

- Si un usuario agrega la mancha, puede eliminar la mancha en el nodo. Si la mancha es **agregada automáticamente por el sistema**, la mancha se eliminará automáticamente después de que se corrija la falla.
- Especifique una tolerancia para el pod que contiene la mancha. Para obtener más información, consulte **Manchas y tolerancias**.

```
apiVersion: v1
kind: Pod
metadata:
  name: nginx
spec:
  containers:
  - name: nginx
    image: nginx:alpine
  tolerations:
  - key: "key1"
    operator: "Equal"
    value: "value1"
    effect: "NoSchedule"
```

Concepto de comprobación 6: Uso del volumen efímero

0/7 nodes are available: 7 Insufficient ephemeral-storage. Esto significa el almacenamiento efímero insuficiente del nodo.

Compruebe si el tamaño del volumen efímero en el pod es limitado. Si el tamaño del volumen efímero requerido por la aplicación excede la capacidad existente del nodo, la aplicación no se puede programar. Para resolver este problema, cambie el tamaño del volumen efímero o amplíe la capacidad del disco del nodo.

```
apiVersion: v1
kind: Pod
metadata:
  name: frontend
spec:
  containers:
  - name: app
    image: images.my-company.example/app:v4
  resources:
    requests:
      ephemeral-storage: "2Gi"
    limits:
      ephemeral-storage: "4Gi"
  volumeMounts:
  - name: ephemeral
    mountPath: "/tmp"
  volumes:
  - name: ephemeral
    emptyDir: {}
```

Concepto de comprobación 7: Si everest funciona correctamente

0/1 nodes are available: 1 everest driver not found at node. Esto significa que el everest-csi-driver de everest no se inicia correctamente en el nodo.

Compruebe el daemon llamado **everest-csi-driver** en el espacio de nombres del sistema kube y verifique si el pod se ha iniciado correctamente. Si no es así, elimine el pod. El demonio reiniciará el pod.

Concepto de comprobación 8: Espacio de thin pool

Un disco de datos de 100 GB dedicado a Docker está montado en el nuevo nodo. Para obtener más información, consulte [Asignación de espacio en disco de datos](#). Si el espacio en disco de datos es insuficiente, no se puede crear el pod.

Solución 1

Puede ejecutar el siguiente comando para borrar las imágenes de Docker no utilizadas:

```
docker system prune -a
```

NOTA

Este comando eliminará todas las imágenes de Docker no utilizadas. Ejercite precaución cuando ejecute este comando.

Solución 2

También puede ampliar la capacidad del disco mediante el procedimiento siguiente:

Paso 1 Amplíe la capacidad del disco de datos en la consola de EVS.

Paso 2 Inicie sesión en la consola de CCE y haga clic en el clúster. En el panel de navegación, elija **Nodes**. Haga clic en **More > Sync Server Data** en la fila que contiene el nodo de destino.

Paso 3 Inicie sesión en el nodo de destino.

Paso 4 Ejecute el comando **lsblk** para comprobar la información del dispositivo de bloque del nodo.

Un disco de datos se divide en función del **Rootfs** de almacenamiento contenedor:

- **Overlayfs:** No se asigna ningún thin pool independiente. Los datos de imagen se almacenan en el disco **dockersys**.

```
# lsblk
NAME                MAJ:MIN RM   SIZE RO TYPE MOUNTPOINT
sda                  8:0    0    50G  0 disk
└─sda1                8:1    0    50G  0 part /
sdb                  8:16   0   200G  0 disk
└─vgpaas-dockersys 253:0   0    90G  0 lvm  /var/lib/docker #
Space used by Docker.
└─vgpaas-kubernetes 253:1   0    10G  0 lvm  /mnt/paas/kubernetes/kubelet #
Space used by Kubernetes.
```

Ejecute los siguientes comandos en el nodo para agregar la nueva capacidad de disco al disco **dockersys**:

```
pvresize /dev/sdb
lvextend -l+100%FREE -n vgpaas/dockersys
resize2fs /dev/vgpaas/dockersys
```

- **Devicemapper:** Se asigna un thin pool para almacenar datos de imagen.

```
# lsblk
NAME                MAJ:MIN RM   SIZE RO TYPE MOUNTPOINT
sda                  8:0    0    50G  0 disk
└─sda1                8:1    0    50G  0 part /
sdb                  8:16   0   200G  0 disk
└─vgpaas-dockersys 253:0   0    18G  0 lvm  /var/lib/
docker
└─vgpaas-thinpool_tmeta 253:1   0     3G  0 lvm
  └─vgpaas-thinpool    253:3   0    67G  0 lvm
# Thin pool space.
...
└─vgpaas-thinpool_tdata 253:2   0    67G  0 lvm
  └─vgpaas-thinpool    253:3   0    67G  0 lvm
...
```

```
└─vgpaas-kubernetes          253:4    0    10G  0 lvm  /mnt/paas/
kubernetes/kubelet
```

- Ejecute los siguientes comandos en el nodo para agregar la nueva capacidad de disco al disco **thinpool**:

```
pvresize /dev/sdb
lvextend -l+100%FREE -n vgpaas/thinpool
```

- Ejecute los siguientes comandos en el nodo para agregar la nueva capacidad de disco al disco **dockersys**:

```
pvresize /dev/sdb
lvextend -l+100%FREE -n vgpaas/dockersys
resize2fs /dev/vgpaas/dockersys
```

---Fin

6.1.3 ¿Qué debo hacer si un pod no logra extraer la imagen?

Localización de fallas

Si el estado del pod es **ImagePullBackOff**, no se puede extraer la imagen. Para obtener más información sobre cómo ver los eventos de Kubernetes, consulte [Consulta de eventos de pod](#).

Proceso de solución de problemas

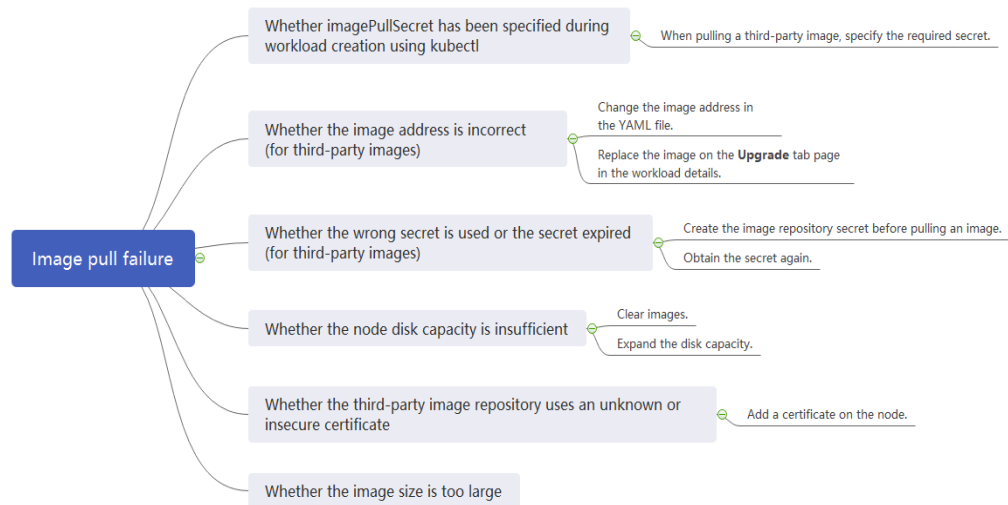
Determine la causa basándose en la información del evento, tal como aparece en [Tabla 6-3](#).

Tabla 6-3 FailedPullImage

Información del evento	Motivo y solución
Failed to pull image "xxx": rpc error: code = Unknown desc = Error response from daemon: Get xxx: denied: You may not login yet	No ha iniciado sesión en el repositorio de imágenes. Concepto de comprobación 1: si se especifica imagePullSecret cuando se utiliza kubectl para crear una carga de trabajo
Failed to pull image "nginx:v1.1": rpc error: code = Unknown desc = Error response from daemon: Get https://registry-1.docker.io/v2/: dial tcp: lookup registry-1.docker.io: no such host	La dirección de la imagen está configurada incorrectamente. Concepto de comprobación 2: Si la dirección de la imagen es correcta cuando se utiliza una imagen de terceros Concepto de comprobación 3: Si se utiliza un secreto incorrecto cuando se utiliza una imagen de terceros
Failed to pull image "docker.io/bitnami/nginx:1.22.0-debian-11-r3": rpc error: code = Unknown desc = Error response from daemon: Get https://registry-1.docker.io/v2/: net/http: request canceled while waiting for connection (Client.Timeout exceeded while awaiting headers)	Error al conectarse al repositorio de imágenes debido a la red desconectada. Concepto de comprobación 7: Conexión al repositorio de Imágenes

Información del evento	Motivo y solución
Failed create pod sandbox: rpc error: code = Unknown desc = failed to create a sandbox for pod "nginx-6dc48bf8b6-18xrw": Error response from daemon: mkdir xxxxx: no space left on device	El espacio en disco es insuficiente. Concepto de comprobación 4: Si el espacio en disco del nodo es insuficiente
Failed to pull image "xxx": rpc error: code = Unknown desc = error pulling image configuration: xxx x509: certificate signed by unknown authority	El repositorio de imágenes de terceros del que se extrae la imagen utiliza un certificado desconocido o inseguro. Concepto de comprobación 5: Si el repositorio de imágenes remoto utiliza un certificado desconocido o inseguro
Failed to pull image "XXX": rpc error: code = Unknown desc = context canceled	El tamaño de la imagen es demasiado grande. Concepto de comprobación 6: Si el tamaño de la imagen es demasiado grande
Failed to pull image "docker.io/bitnami/nginx:1.22.0-debian-11-r3": rpc error: code = Unknown desc = Error response from daemon: Get https://registry-1.docker.io/v2/: net/http: request canceled while waiting for connection (Client.Timeout exceeded while awaiting headers)	Concepto de comprobación 7: Conexión al repositorio de Imágenes
ERROR: toomanyrequests: Too Many Requests. O you have reached your pull rate limit, you may increase the limit by authenticating an upgrading	La velocidad es limitada porque el número de veces de extracción de imágenes alcanza el límite superior. Concepto de comprobación 8: Si el número de veces de imágenes públicas alcanza el límite superior

Figura 6-2 Proceso de solución de problemas



Concepto de comprobación 1: si se especifica imagePullSecret cuando se utiliza kubectl para crear una carga de trabajo

Si el estado de la carga de trabajo es anormal y se muestra un evento de Kubernetes que indica que el pod no puede extraer la imagen, compruebe si el campo **imagePullSecrets** existe en el archivo YAML.

Conceptos a comprobar

- Si se necesita extraer una imagen de SWR, el parámetro **name** debe establecerse en **default-secret**.

```
apiVersion: extensions/v1beta1
kind: Deployment
metadata:
  name: nginx
spec:
  replicas: 1
  selector:
    matchLabels:
      app: nginx
  strategy:
    type: RollingUpdate
  template:
    metadata:
      labels:
        app: nginx
    spec:
      containers:
      - image: nginx
        imagePullPolicy: Always
        name: nginx
        imagePullSecrets:
        - name: default-secret
```

- Si es necesario extraer una imagen de un repositorio de imágenes de terceros, el parámetro **imagePullSecrets** debe establecerse en el nombre secreto creado.

Cuando utilice kubectl para crear una carga de trabajo a partir de una imagen de terceros, especifique el campo **imagePullSecret**, en el que **name** indica el nombre del secreto utilizado para extraer la imagen. Para obtener más información sobre cómo crear un secreto, consulte [Uso de kubectl](#).

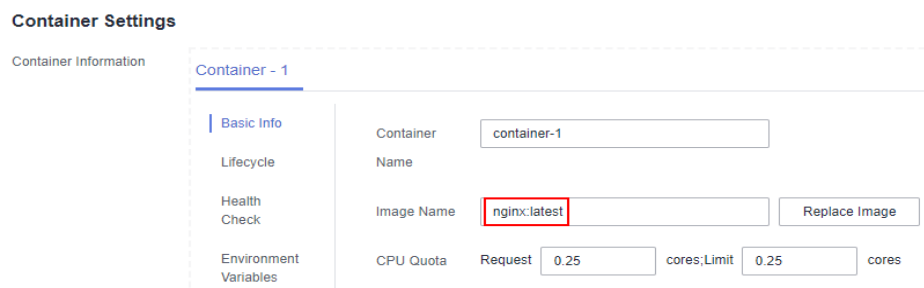
Concepto de comprobación 2: Si la dirección de la imagen es correcta cuando se utiliza una imagen de terceros

CCE le permite crear cargas de trabajo utilizando imágenes extraídas de repositorios de imágenes de terceros.

Ingrese la dirección de imagen de terceros según los requisitos. El formato debe ser **ip:port/path/name:version** o **name:version**. Si no se especifica ninguna etiqueta, se utiliza **latest** de forma predeterminada.

- Para un repositorio privado, introduzca una dirección de imagen con el formato **ip:port/path/name:version**.
- Para un repositorio de Docker de código abierto, introduzca una dirección de imagen en el formato de **name:version**, por ejemplo, **nginx:latest**.

Figura 6-3 Uso de una imagen de terceros



La siguiente información se muestra cuando no se puede extraer una imagen debido a la dirección de imagen incorrecta proporcionada.

```
Failed to pull image "nginx:v1.1": rpc error: code = Unknown desc = Error response from daemon: Get https://registry-1.docker.io/v2/: dial tcp: lookup registry-1.docker.io: no such host
```

Solución

Puede editar el archivo YAML para modificar la dirección de la imagen o iniciar sesión en la consola de CCE para reemplazar la imagen en la página de ficha **Upgrade** de la página de detalles de la carga de trabajo.

Concepto de comprobación 3: Si se utiliza un secreto incorrecto cuando se utiliza una imagen de terceros

Generalmente, se puede acceder a un repositorio de imágenes de terceros solo después de la autenticación (usando su cuenta y contraseña). CCE utiliza el modo de autenticación secreta para extraer imágenes. Por lo tanto, debe crear un secreto para un repositorio de imágenes antes de extraer imágenes del repositorio.

Solución

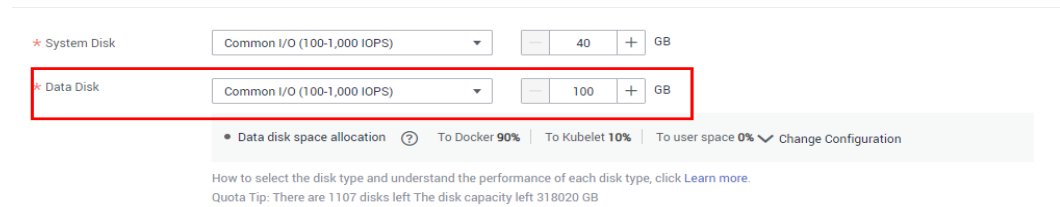
Si su secreto es incorrecto, las imágenes no se extraerán. En este caso, crea un nuevo secreto.

Para crear un secreto, consulte [Uso de kubectl](#).

Concepto de comprobación 4: Si el espacio en disco del nodo es insuficiente

Cuando se crea un nodo, se enlaza un disco de datos al nodo. Si el espacio en disco de datos es insuficiente, la extracción de imagen fallará.

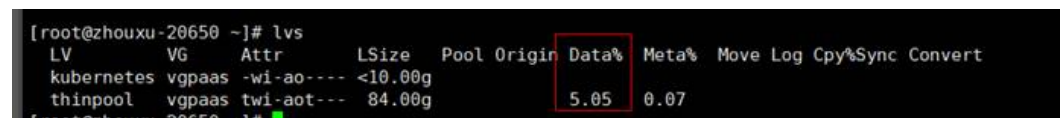
Figura 6-4 Capacidad del disco de datos (GB)



Si el evento Kubernetes contiene la siguiente información, el nodo no tiene espacio en disco para almacenar imágenes. Es necesario limpiar imágenes o ampliar la capacidad del disco.

```
Failed create pod sandbox: rpc error: code = Unknown desc = failed to create a
sandbox for pod "nginx-6dc48bf8b6-18xrw": Error response from daemon: mkdir
xxxxxx: no space left on device
```

Ejecute el comando `lvs` para comprobar el espacio en disco para almacenar imágenes en el nodo.



Ejecute el siguiente comando para limpiar imágenes:

```
docker rmi -f {Image ID}
```

Para ampliar la capacidad del disco, realice los siguientes pasos:

- Paso 1** Amplíe la capacidad del disco de datos en la consola de EVS.
- Paso 2** Inicie sesión en la consola de CCE y haga clic en el clúster. En el panel de navegación, elija **Nodes**. Haga clic en **More > Sync Server Data** en la fila que contiene el nodo de destino.
- Paso 3** Inicie sesión en el nodo de destino.
- Paso 4** Ejecute el comando `lsblk` para comprobar la información del dispositivo de bloque del nodo.

Un disco de datos se divide en función del **Rootfs** de almacenamiento contenedor:

- **Overlayfs:** No se asigna ningún thin pool independiente. Los datos de imagen se almacenan en el disco **dockersys**.

```
# lsblk
NAME                                MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
sda                                  8:0    0   50G  0 disk
├─sda1                               8:1    0   50G  0 part /
sdb                                  8:16   0  200G  0 disk
├─vgpaas-dockersys 253:0    0   90G  0 lvm  /var/lib/docker #
Space used by Docker.
├─vgpaas-kubernetes 253:1    0   10G  0 lvm  /mnt/paas/kubernetes/kubelet #
Space used by Kubernetes.
```

Ejecute los siguientes comandos en el nodo para agregar la nueva capacidad de disco al disco **dockersys**:

```
pvresize /dev/sdb
lvextend -l+100%FREE -n vgpaas/dockersys
resize2fs /dev/vgpaas/dockersys
```

- **Devicemapper:** Se asigna un thin pool para almacenar datos de imagen.

```
# lsblk
NAME                                MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
sda                                  8:0    0   50G  0 disk
├─sda1                               8:1    0   50G  0 part /
sdb                                  8:16   0  200G  0 disk
├─vgpaas-dockersys                   253:0   0   18G  0 lvm  /var/lib/
docker
├─vgpaas-thinpool_tmeta               253:1   0    3G  0 lvm
└─vgpaas-thinpool                    253:3   0   67G  0 lvm
# Thin pool space.
...
├─vgpaas-thinpool_tdata               253:2   0   67G  0 lvm
└─vgpaas-thinpool                    253:3   0   67G  0 lvm
...
└─vgpaas-kubernetes                  253:4   0   10G  0 lvm  /mnt/paas/
kubernetes/kubelet
```

- Ejecute los siguientes comandos en el nodo para agregar la nueva capacidad de disco al disco **thinpool**:

```
pvresize /dev/sdb
lvextend -l+100%FREE -n vgpaas/thinpool
```

- Ejecute los siguientes comandos en el nodo para agregar la nueva capacidad de disco al disco **dockersys**:

```
pvresize /dev/sdb
lvextend -l+100%FREE -n vgpaas/dockersys
resize2fs /dev/vgpaas/dockersys
```

---Fin

Concepto de comprobación 5: Si el repositorio de imágenes remoto utiliza un certificado desconocido o inseguro

Cuando un pod extrae una imagen de un repositorio de imágenes de terceros que utiliza un certificado desconocido o inseguro, la imagen no se extrae del nodo. La lista de eventos de pod contiene el evento "Failed to pull the image" con la causa "x509: certificate signed by unknown authority".

NOTA

Se mejora la seguridad de las imágenes de EulerOS 2.9. Algunos certificados inseguros o caducados se eliminan del sistema. Es normal que este error se notifique en EulerOS 2.9 pero no o algunas imágenes de terceros en otros tipos de nodos. También puede realizar las siguientes operaciones para rectificar la falla.

Solución

- Paso 1** Compruebe la dirección IP y el número de puerto del servidor de imágenes de terceros para el que se muestra el mensaje de error "unknown authority".

Puede ver la dirección IP y el número de puerto del servidor de imágenes de terceros para el que se reporta el error en la información de evento "Failed to pull image".

```
Failed to pull image "bitnami/redis-cluster:latest": rpc error: code = Unknown
desc = error pulling image configuration: Get https://
production.cloudflare.docker.com/registry-v2/docker/registry/v2/blobs/sha256/e8/
e83853f03a2e792614e7c1e6de75d63e2d6d633b4e7c39b9d700792ee50f7b56/data?
verify=1636972064-AQb15RActnudzV%2F3EShZwnq0e8%3D: x509: certificate signed by
unknown authority
```

La dirección IP del servidor de imágenes de terceros es *production.cloudflare.docker.com* y el número de puerto HTTPS predeterminado es *443*.

Paso 2 Cargue el certificado raíz del servidor de imágenes de terceros en el nodo donde se va a descargar la imagen de terceros.

Ejecute los siguientes comandos en los nodos de EulerOS y de CentOS con *{server_url}*: *{server_port}* reemplazado por la dirección IP y el número de puerto obtenidos en el paso 1, por ejemplo, **production.cloudflare.docker.com:443**:

Si el motor de contenedores del nodo es containerd, reemplace **systemctl restart docker** por **systemctl restart containerd**.

```
openssl s_client -showcerts -connect {server_url}:{server_port} < /dev/null | sed
-ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > /etc/pki/ca-trust/source/
anchors/tmp_ca.crt
update-ca-trust
systemctl restart docker
```

Ejecute el siguiente comando en los nodos de Ubuntu:

```
openssl s_client -showcerts -connect {server_url}:{server_port} < /dev/null | sed
-ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > /usr/local/share/ca-
certificates/tmp_ca.crt
update-ca-trust
systemctl restart docker
```

----Fin

Concepto de comprobación 6: Si el tamaño de la imagen es demasiado grande

La lista de eventos de pod contiene el evento "Failed to pull image". Esto puede ser causado por un tamaño de imagen grande.

```
Failed to pull image "XXX": rpc error: code = Unknown desc = context canceled
```

Inicie sesión en el nodo y ejecute el comando **docker pull** para extraer manualmente la imagen. La imagen se extrae correctamente.

Causa raíz

El valor predeterminado de **image-pull-progress-deadline** es 1 minuto. Si el progreso de extracción de imagen no se actualiza en 1 minuto, se cancela la extracción de imagen. Si el rendimiento del nodo es deficiente o el tamaño de la imagen es demasiado grande, es posible que la imagen no se extraiga y que la carga de trabajo no se inicie.

Solución

- (Recomendado) Método 1: Inicie sesión en el nodo, ejecute el comando **docker pull** para extraer manualmente la imagen y compruebe si **imagePullPolicy** de la carga de trabajo es **IfNotPresent** (configuración de política predeterminada). En este caso, la imagen que se ha extraído al host local se utiliza para crear la carga de trabajo.
- Método 2: Modifique los parámetros de configuración de kubelet.

Para un clúster de v1.15 o posterior, ejecute el siguiente comando:

```
vi /opt/cloud/cce/kubernetes/kubelet/kubelet
```

Para un clúster anterior a v1.15, ejecute el siguiente comando:

```
vi /var/paas/kubernetes/kubelet/kubelet
```

Agregue **--image-pull-progress-deadline=30m** al final del parámetro **DAEMON_ARGS**. **30m** indica 30 minutos. Este valor se puede modificar según se requiera. La configuración agregada y la configuración existente están separadas por un espacio.

```
DAEMON_ARGS=""
--cloud-provider=external --general-config-dir=/opt/cloud/cce/conf --image-pull-progress-deadline=30m
```

Ejecute el siguiente comando para reiniciar kubelet:

```
systemctl restart kubelet
```

Espere un rato y compruebe si el estado del kubelet es **running**.

```
systemctl status kubelet
```

```
● kubelet.service - Cloud Container Engine Kubelet Service
   Loaded: loaded (/usr/lib/systemd/system/kubelet.service; enabled; vendor preset: disabled)
   Active: active (running) since Thu 2021-11-25 16:46:53 CST; 7s ago
     Process: 25557 ExecStop=/bin/sh -c /usr/bin/pkill kubelet (code=exited, status=0/SUCCESS)
```

La carga de trabajo se inicia correctamente y la imagen se extrae correctamente.

Concepto de comprobación 7: Conexión al repositorio de Imágenes

Síntoma

Se muestra el siguiente mensaje de error durante la creación de la carga de trabajo:

```
Failed to pull image "docker.io/bitnami/nginx:1.22.0-debian-11-r3": rpc error:
code = Unknown desc = Error response from daemon: Get https://
registry-1.docker.io/v2/: net/http: request canceled while waiting for connection
(Client.Timeout exceeded while awaiting headers)
```

Causa

Error al conectarse al repositorio de imágenes debido a la red desconectada. SWR le permite extraer imágenes del repositorio oficial de Docker. Para extraer imágenes de otros repositorios, primero debe conectarse a los repositorios.

Solución

- Vincule una dirección IP pública (EIP) al nodo que extrae la imagen.
- Suba la imagen a SWR y luego extraiga la imagen de SWR.

Concepto de comprobación 8: Si el número de veces de imágenes públicas alcanza el límite superior

Síntoma

Se muestra el siguiente mensaje de error durante la creación de la carga de trabajo:

```
ERROR: toomanyrequests: Too Many Requests.
```

O

```
you have reached your pull rate limit, you may increase the limit by
authenticating an upgrading: https://www.docker.com/increase-rate-limits.
```

Causa

Docker Hub establece el número máximo de solicitudes de extracción de imágenes de contenedor. Para obtener más información, consulte [Comprender el límite de velocidad de Docker Hub](#).

Solución

Empuje la imagen utilizada con frecuencia a SWR y luego extraiga la imagen de SWR.

6.1.4 ¿Qué debo hacer si falla el inicio del contenedor?

Localización de fallas

En la página de detalles de una carga de trabajo, si se muestra un evento que indica que el contenedor no se inicia, realice los siguientes pasos para localizar el error:

Paso 1 Inicie sesión en el nodo donde se encuentra la carga de trabajo anormal.

Paso 2 Compruebe el ID del contenedor donde el pod de carga de trabajo sale de forma anormal.

```
docker ps -a | grep $podName
```

Paso 3 Vea los logs del contenedor correspondiente.

```
docker logs $containerID
```

Rectifique la falla de la carga de trabajo basado en logs.

Paso 4 Compruebe los logs de errores.

```
cat /var/log/messages | grep $containerID | grep oom
```

Compruebe si OOM del sistema se activa en función de los logs.

---Fin

Proceso de solución de problemas

Determine la causa basándose en la información del evento, tal como aparece en [Tabla 6-4](#).

Tabla 6-4 Error en el inicio del contenedor

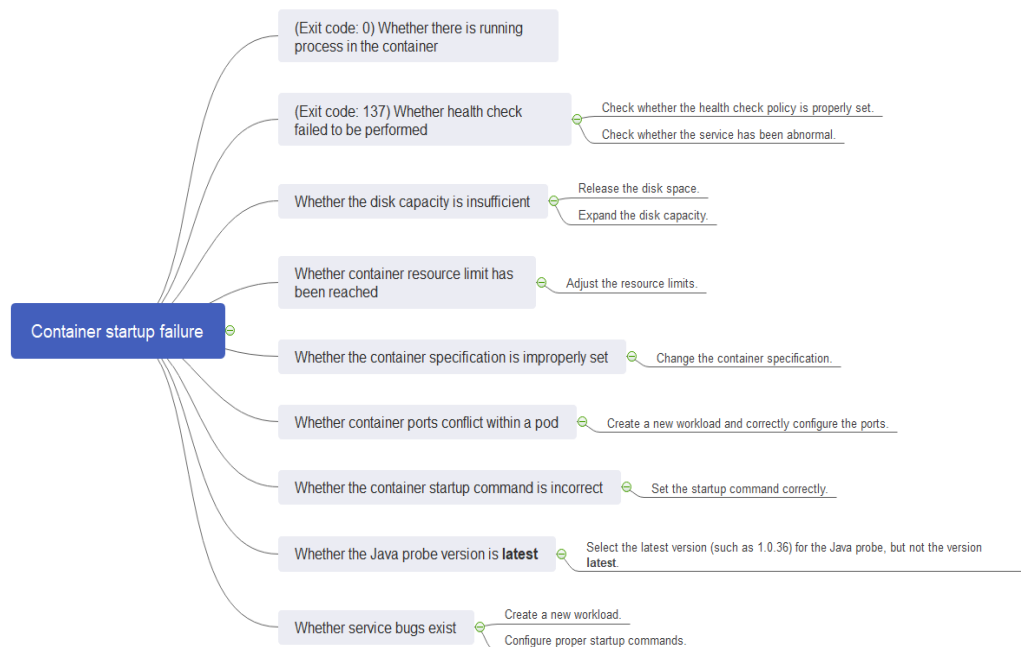
Log o evento	Motivo y solución
El log contiene la salida (0).	No existe ningún proceso en el contenedor. Compruebe si el contenedor está funcionando correctamente. Concepto de comprobación 1: Si hay procesos que siguen ejecutándose en el contenedor (Código de salida: 0)
Información del evento: Liveness probe failed: Get http... El log contiene la salida (137).	La comprobación de estado falla. Concepto de comprobación 2: Si no se realiza la comprobación de estado (Código de salida: 137)
Información del evento: Thin Pool tiene 15991 bloques de datos libres que son menos que el mínimo requerido 16383 bloques de datos libres. Cree más espacio libre en el thin pool o use la opción dm.min_free_space para cambiar el comportamiento	El espacio en disco es insuficiente. Limpie el espacio en disco. Concepto de comprobación 3: Si el espacio en disco del contenedor es insuficiente

Log o evento	Motivo y solución
La palabra clave OOM existe en el log.	<p>La memoria es insuficiente.</p> <p>Concepto de comprobación 4: Si se ha alcanzado el límite superior de los recursos de contenedores</p> <p>Concepto de comprobación 5: Si los límites de recursos están configurados incorrectamente para el contenedor</p>
Dirección ya en uso	<p>Se produce un conflicto entre los puertos contenedor en el pod.</p> <p>Concepto de comprobación 6: Si los puertos de contenedores en el mismo pod entran en conflicto entre sí</p>

Además de las posibles causas precedentes, hay otras tres causas posibles:

- **Concepto de comprobación 7: Si el comando de inicio del contenedor está correctamente configurado**
- **Concepto de comprobación 8: Si la versión de la sonda de Java es la última**
- **Concepto de comprobación 9: Si el servicio de usuario tiene un error**
- Utilice la imagen correcta cuando cree una carga de trabajo en un nodo Arm.

Figura 6-5 Proceso de solución de problemas



Concepto de comprobación 1: Si hay procesos que siguen ejecutándose en el contenedor (Código de salida: 0)

Paso 1 Inicie sesión en el nodo donde se encuentra la carga de trabajo anormal.

Paso 2 Vea el estado del contenedor.

```
docker ps -a | grep $podName
```

Ejemplo:

```
[root@xxx ~]# docker ps -a | grep test
1f59a7f4cf77        613055f01959          "/bin/bash"         10 seconds ago    Exited (0) 10 seconds ago
k8s_container-0_test-66b79cbbd7-htcjf_default_5c388617-ac32-11e9-9168-fa163ec28742_1
2c73ac8717cc      cce-pause:2.0         "/pause"            12 seconds ago    Up 12 seconds
k8s_POD_test-66b79cbbd7-htcjf_default_5c388617-ac32-11e9-9168-fa163ec28742_0
```

Si no existe ningún proceso en ejecución en el contenedor, se muestra el código de estado **Exited (0)**.

----Fin

Concepto de comprobación 2: Si no se realiza la comprobación de estado (Código de salida: 137)

La comprobación de estado configurada para una carga de trabajo se realiza en los servicios periódicamente. Si se produce una excepción, el pod informa de un evento y el pod no se reinicia.

Si se configura la comprobación de estado de tipo de vida (exploración de vida de carga de trabajo) para la carga de trabajo y el número de fallas de comprobación de estado excede el umbral, se reiniciarán los contenedores en el pod. En la página de detalles de la carga de trabajo, si los eventos de Kubernetes contienen **Liveness probe failed: Get http...**, se produce un error en la comprobación de estado.

Solución

En la página de detalles de la carga de trabajo, elija **Upgrade > Advanced Settings > Health Check** de estado para comprobar si la política de comprobación de estado está configurada correctamente y si los servicios son normales.

Concepto de comprobación 3: Si el espacio en disco del contenedor es insuficiente

El siguiente mensaje hace referencia al disco de Thin Pool asignado desde el disco de Docker seleccionado durante la creación del nodo. Puede ejecutar el comando **lvs** como usuario **root** para ver el uso actual del disco.

```
Thin Pool has 15991 free data blocks which are less than minimum required 16383 free data blocks. Create more free space in thin pool or use dm.min_free_space option to change behavior
```

```
## lvs
LV          VG      Attr      LSize   Pool Origin Data%  Meta%   Move Log Cpy%Sync Convert
dockersys  vgpaa  -wi-ao--- <18.00g
kubernetes vgpaa  -wi-ao--- <18.00g
thinpool   vgpaa  twi-aot--- 67.00g   98.04  1.32
```

Solución

Solución 1

Puede ejecutar el siguiente comando para borrar las imágenes basura no utilizadas:

```
docker system prune -a
```

📖 NOTA

Este comando eliminará todas las imágenes de Docker no utilizadas. Ejercite precaución cuando ejecute este comando.

Solución 2

También puede ampliar la capacidad del disco mediante el procedimiento siguiente:

Paso 1 Amplíe la capacidad del disco de datos en la consola de EVS.

Paso 2 Inicie sesión en la consola de CCE y haga clic en el clúster. En el panel de navegación, elija **Nodes**. Haga clic en **More > Sync Server Data** en la fila que contiene el nodo de destino.

Paso 3 Inicie sesión en el nodo de destino.

Paso 4 Ejecute el comando **lsblk** para comprobar la información del dispositivo de bloque del nodo.

Un disco de datos se divide en función del **Rootfs** de almacenamiento contenedor:

- **Overlayfs:** No se asigna ningún thin pool independiente. Los datos de imagen se almacenan en el disco **dockersys**.

```
# lsblk
NAME                MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
sda                  8:0    0   50G  0 disk
└─sda1                8:1    0   50G  0 part /
sdb                  8:16   0  200G  0 disk
└─vgpaas-dockersys 253:0   0   90G  0 lvm  /var/lib/docker #
Space used by Docker.
└─vgpaas-kubernetes 253:1   0   10G  0 lvm  /mnt/paas/kubernetes/kubelet #
Space used by Kubernetes.
```

Ejecute los siguientes comandos en el nodo para agregar la nueva capacidad de disco al disco **dockersys**:

```
pvresize /dev/sdb
lvextend -l+100%FREE -n vgpaas/dockersys
resize2fs /dev/vgpaas/dockersys
```

- **Devicemapper:** Se asigna un thin pool para almacenar datos de imagen.

```
# lsblk
NAME                MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
sda                  8:0    0   50G  0 disk
└─sda1                8:1    0   50G  0 part /
sdb                  8:16   0  200G  0 disk
└─vgpaas-dockersys 253:0   0   18G  0 lvm  /var/lib/
docker
└─vgpaas-thinpool_tmeta 253:1   0    3G  0 lvm
└─┬─vgpaas-thinpool 253:3   0   67G  0 lvm
# Thin pool space.
...
└─vgpaas-thinpool_tdata 253:2   0   67G  0 lvm
└─┬─vgpaas-thinpool 253:3   0   67G  0 lvm
...
└─vgpaas-kubernetes 253:4   0   10G  0 lvm  /mnt/paas/
kubernetes/kubelet
```

- Ejecute los siguientes comandos en el nodo para agregar la nueva capacidad de disco al disco **thinpool**:

```
pvresize /dev/sdb
lvextend -l+100%FREE -n vgpaas/thinpool
```

- Ejecute los siguientes comandos en el nodo para agregar la nueva capacidad de disco al disco **dockersys**:

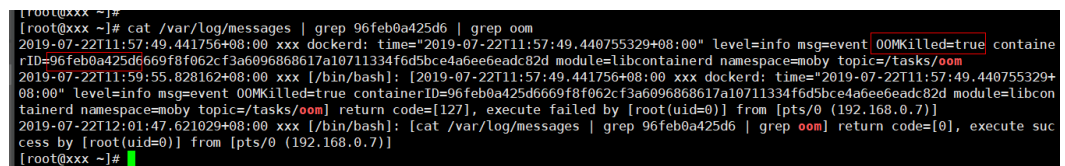

```
pvresize /dev/sdb
lvextend -l+100%FREE -n vgpaas/dockersys
resize2fs /dev/vgpaas/dockersys
```

----Fin

Concepto de comprobación 4: Si se ha alcanzado el límite superior de los recursos de contenedores

Si se ha alcanzado el límite superior de los recursos del contenedor, OOM se mostrará en los detalles del evento, así como en el log:

```
cat /var/log/messages | grep 96feb0a425d6 | grep oom
```



```
[root@xxx ~]# cat /var/log/messages | grep 96feb0a425d6 | grep oom
2019-07-22T11:57:49.441756+08:00 xxx dockerd: time="2019-07-22T11:57:49.440755329+08:00" level=info msg=event OOMKilled=true containe
rID=96feb0a425d6669f8f062cf3a6096868617a10711334f6d5bce4a6ee6eadc82d module=libcontainerd namespace=moby topic=/tasks/oom
2019-07-22T11:59:55.828162+08:00 xxx [/bin/bash]: [2019-07-22T11:57:49.441756+08:00 xxx dockerd: time="2019-07-22T11:57:49.440755329+
08:00" level=info msg=event OOMKilled=true containerID=96feb0a425d6669f8f062cf3a6096868617a10711334f6d5bce4a6ee6eadc82d module=libcon
tainerd namespace=moby topic=/tasks/oom] return code=[127], execute failed by [root(uid=0)] from [pts/0 (192.168.0.7)]
2019-07-22T12:01:47.621029+08:00 xxx [/bin/bash]: [cat /var/log/messages | grep 96feb0a425d6 | grep oom] return code=[0], execute suc
cess by [root(uid=0)] from [pts/0 (192.168.0.7)]
[root@xxx ~]#
```

Cuando se crea una carga de trabajo, si los recursos solicitados superan el límite superior configurado, se activa la OOM del sistema y el contenedor sale inesperadamente.

Concepto de comprobación 5: Si los límites de recursos están configurados incorrectamente para el contenedor

Si los límites de recursos establecidos para el contenedor durante la creación de la carga de trabajo son menores que los necesarios, no se puede reiniciar el contenedor.

Concepto de comprobación 6: Si los puertos de contenedores en el mismo pod entran en conflicto entre sí

Paso 1 Inicie sesión en el nodo donde se encuentra la carga de trabajo anormal.

Paso 2 Compruebe el ID del contenedor donde el pod de carga de trabajo sale de forma anormal.

```
docker ps -a | grep $podName
```

Paso 3 Vea los logs del contenedor correspondiente.

```
docker logs $containerID
```

Rectifique la falla de la carga de trabajo basado en logs. Como se muestra en la siguiente figura, los puertos de contenedor en el mismo pod entran en conflicto. Como resultado, el contenedor no se inicia.

Figura 6-6 Falla de reinicio del contenedor debido a un conflicto de puerto de contenedor

```
[root@k8s-POD_test2-65dbb945d6-xh9n2_default_324-94b7-11e9-aa5f-fa163e07fc60_0 ~]# docker ps -a|grep test2
aebc17c4d66c          94818572c4ef          "nginx -g 'daemon ..." 8 se
conds ago           Exited (1) 5 seconds ago      k8s_container-1_test2-65dbb945d6-xh9n2_defau
lt_38892324-94b7-11e9-aa5f-fa163e07fc60_3
0c43d629292e        nginx                "nginx -g 'daemon ..." Abou
t a minute ago     Up About a minute           k8s_container-0_test2-65dbb945d6-xh9n2_defau
lt_38892324-94b7-11e9-aa5f-fa163e07fc60_0
3484b34393ce        cfe-pause:11.23.1    "/pause"                Abou
t a minute ago     Up About a minute           k8s_POD_test2-65dbb945d6-xh9n2_default_38892
324-94b7-11e9-aa5f-fa163e07fc60_0
[root@k8s-POD_test2-65dbb945d6-xh9n2_default_324-94b7-11e9-aa5f-fa163e07fc60_0 ~]# docker logs aebc17c4d66c
2019/06/22 06:31:29 [emerg] 1#1: bind() to 0.0.0.0:80 failed (98: Address already in use)
nginx: [emerg] bind() to 0.0.0.0:80 failed (98: Address already in use)
2019/06/22 06:31:29 [emerg] 1#1: bind() to 0.0.0.0:80 failed (98: Address already in use)
nginx: [emerg] bind() to 0.0.0.0:80 failed (98: Address already in use)
2019/06/22 06:31:29 [emerg] 1#1: bind() to 0.0.0.0:80 failed (98: Address already in use)
nginx: [emerg] bind() to 0.0.0.0:80 failed (98: Address already in use)
2019/06/22 06:31:29 [emerg] 1#1: bind() to 0.0.0.0:80 failed (98: Address already in use)
nginx: [emerg] bind() to 0.0.0.0:80 failed (98: Address already in use)
2019/06/22 06:31:29 [emerg] 1#1: bind() to 0.0.0.0:80 failed (98: Address already in use)
nginx: [emerg] bind() to 0.0.0.0:80 failed (98: Address already in use)
2019/06/22 06:31:29 [emerg] 1#1: still could not bind()
nginx: [emerg] still could not bind()
```

----Fin

Solución

Vuelva a crear la carga de trabajo y establezca un número de puerto que no utilice ningún otro pod.

Concepto de comprobación 7: Si el comando de inicio del contenedor está correctamente configurado

Los mensajes de error son los siguientes:

```
[root@k8s-POD_test1-dbc59fc55-8gr9f_default_2a0-94ba-11e9-aa5f-fa163e07fc60_0 ~]# docker ps -a|grep test1
2ae258d570c2          94818572c4ef          "/bin/sh -c 'sleep ..." 14 s
econds ago           Up 12 seconds                k8s_container-0_test1-dbc59fc55-8gr9f_defau
lt_19f0d2a0-94ba-11e9-aa5f-fa163e07fc60_1
492b258c1e89          94818572c4ef          "/bin/sh -c 'sleep ..." Abou
t a minute ago       Exited (1) 14 seconds ago     k8s_container-0_test1-dbc59fc55-8gr9f_defau
lt_19f0d2a0-94ba-11e9-aa5f-fa163e07fc60_0
2fcd00990111        cfe-pause:11.23.1    "/pause"                Abou
t a minute ago     Up About a minute           k8s_POD_test1-dbc59fc55-8gr9f_default_19f0d
2a0-94ba-11e9-aa5f-fa163e07fc60_0
[root@k8s-POD_test1-dbc59fc55-8gr9f_default_2a0-94ba-11e9-aa5f-fa163e07fc60_0 ~]# docker logs 492b258c1e89
cat: /tmp/test: No such file or directory
```

Solución

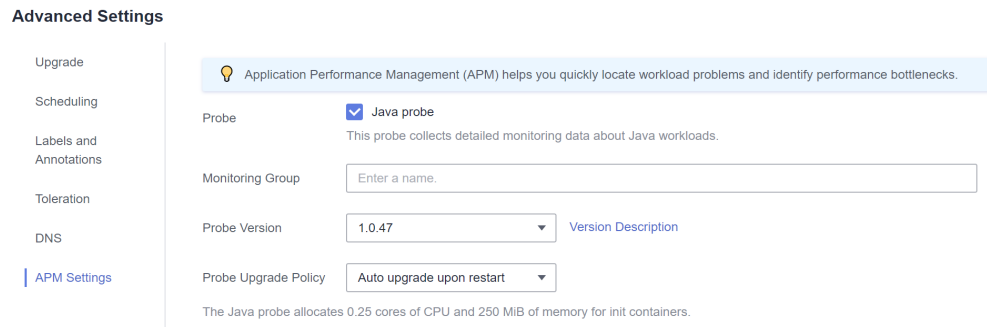
Inicie sesión en la consola de CCE. En la página de detalles de la carga de trabajo, elija **Upgrade > Advanced Settings > Lifecycle** para comprobar si el comando de inicio está configurado correctamente.

Concepto de comprobación 8: Si la versión de la sonda de Java es la última

Se produce el evento de Kubernetes "Created container init-pinpoint".

Solución

1. Al crear una carga de trabajo, seleccione la última versión de sondeo de Java específica (por ejemplo, **1.0.36** y no la opción **latest**) en la ficha **APM Settings** del área **Advanced Settings**.



2. Si seleccionó **latest** para el sondeo de Java durante la creación de la carga de trabajo, puede actualizar la carga de trabajo y cambiarla a la versión más reciente específica (por ejemplo, **1.0.36**).

Concepto de comprobación 9: Si el servicio de usuario tiene un error

Compruebe si el comando de inicio de la carga de trabajo se ejecuta correctamente o si la carga de trabajo tiene un error.

Paso 1 Inicie sesión en el nodo donde se encuentra la carga de trabajo anormal.

Paso 2 Compruebe el ID del contenedor donde el pod de carga de trabajo sale de forma anormal.

```
docker ps -a | grep $podName
```

Paso 3 Vea los logs del contenedor correspondiente.

```
docker logs $containerID
```

Nota: En el comando anterior, *containerID* indica el ID del contenedor que ha salido.

Figura 6-7 Comando de inicio incorrecto del contenedor

```
[root@dcb-ha-11638 ~]# docker ps -a | grep nginx
cf0352f6617f9      3f8a4339aadd      "/bin/bash /tmp/test." 2 minutes ago
ExitCode(127)      k8s_container-0_nginx-267
0177225-kt929_test_d6402ef7-4e0f-11e8-b4f7-fa163e74044e_5
c2176ce394a1      cfe-pause:3.7.6   "/pause"             5 minutes ago
Up 5 minutes      k8s_POD_nginx-2670177225-
kt929_test_d6402ef7-4e0f-11e8-b4f7-fa163e74044e_0
[root@dcb-ha-11638 ~]# docker logs cf035
/bin/bash: /tmp/test.sh: No such file or directory
[root@dcb-ha-11638 ~]#
```

Como se muestra en la figura anterior, el contenedor no puede iniciarse debido a un comando de inicio incorrecto. Para otros errores, rectifique los errores basados en los registros.

----Fin

Solución

Cree una nueva carga de trabajo y configure un comando de inicio correcto.

6.1.5 ¿Qué debo hacer si un pod no es desalojado?

Qué es el desalojo

Cuando se produce una excepción en un nodo, Kubernetes desaloja los pods del nodo para garantizar la disponibilidad de la carga de trabajo.

En Kubernetes, tanto kube-controller-manager como kubelet pueden desalojar pods.

- **Desalojo desplegado por kube-controller-manager**

kube-controller-manager consiste en múltiples controladores, y el desalojo es desplegado por el controlador de nodo. El controlador comprueba periódicamente el estado de todos los nodos. Cuando un nodo está en el estado **NotReady** durante un período de tiempo, todos los pods del nodo son desalojados.

kube-controller-manager proporciona los siguientes parámetros de inicio para controlar los desalojos:

- **pod-eviction-timeout**: intervalo en el que un nodo está inactivo, tras el cual se desalojan los pods de ese nodo. El intervalo predeterminado es 5 minutos.
- **node-eviction-rate**: velocidad a la que se desalojan los nodos, que se implementa mediante el algoritmo de control de tráfico de bucket de testigos. El valor predeterminado es **0.1**, lo que indica que se desalojan 0.1 nodos por segundo. Obsérvese que esta velocidad no es la velocidad a la que se desalojan los pods, sino la velocidad a la que se desalojan los nodos. Es decir, se borra un nodo cada 10 segundos.
- **secondary-node-eviction-rate**: tasa de desalojo secundario. Cuando un gran número de nodos están abajo en el clúster, la tasa de desalojo disminuye. El valor predeterminado es **0.01**.
- **unhealthy-zone-threshold**: umbral para que una zona se considere insalubre. Este parámetro determina cuándo habilitar la tasa de desalojo secundario. El valor predeterminado es **0.55**. Es decir, si el porcentaje de nodos descendentes en una zona supera el 55%, la zona no está sana.
- **large-cluster-size-threshold**: umbral para que un clúster se considere grande. Cuando el número de nodos en una zona excede este umbral, la zona se considera como un clúster grande. Si el porcentaje de nodos inactivos en un clúster grande supera el 55%, la tasa de desalojo se reduce a 0.01. Si el grupo es pequeño, la tasa de desalojo se reduce a 0.

- **Desalojo desplegado por kubelet**

Si se van a utilizar recursos de un nodo, kubelet ejecuta la política de desalojo basada en la prioridad de pod, el uso de recursos y la solicitud de recursos. Si los pods tienen la misma prioridad, el pod que usa la mayoría de los recursos o las solicitudes de la mayoría de los recursos será desalojado primero.

kube-controller-manager desaloja todos los pods en un nodo, mientras que kubelet desaloja ciertos pods en un nodo. Los pods a desalojar son determinadas por la QoS de pods. kubelet comprueba periódicamente la memoria y los recursos de disco del nodo. Si los recursos son insuficientes, los pods son desalojados en función de la prioridad.

Hay umbrales de desahucio blandos y umbrales de desahucio duros.

- **Soft eviction threshold**: Se establece un período de gracia para los recursos de nodo. kubelet recuperará recursos de nodo asociados con este umbral si se excede ese período de gracia. Si el uso de recursos de nodo alcanza este umbral pero cae por debajo de él antes de que se exceda el período de gracia, kubelet no desalojará los pods del nodo.
- **Hard eviction threshold**: Los pods son desalojados inmediatamente una vez que se alcanza este umbral.

kubelet proporciona los siguientes parámetros para controlar los desalojos:

- **eviction-soft** describe un conjunto de umbrales de desalojo que, si se cumplen durante un período de gracia correspondiente, desencadenarían un desalojo de pod.

Por ejemplo, si **memory.available** es inferior a 1.5 Gi, el desalojo de pod se ejecuta solo después de que se exceda el período de gracia especificado por **eviction-soft-grace-period**.

- **eviction-soft-grace-period**: un conjunto de períodos de gracia de desalojo que corresponden a cuánto tiempo debe mantenerse un umbral de desalojo suave antes de activar un desalojo de pod. El valor predeterminado es 90 segundos.
- **eviction-max-pod-grace-period**: período de gracia máximo permitido para usar cuando se terminan los pods en respuesta a un umbral de desalojo suave que se cumple.
- **eviction-pressure-transition-period**: duración por la cual el kubelet tiene que esperar antes de salir de una condición de presión de desalojo. El valor predeterminado es 5 minutos. Si el tiempo excede el umbral, el nodo se establece en presión de memoria o presión de disco y, a continuación, se inicia el desalojo de pod.
- **eviction-minimum-reclaim**: número mínimo de recursos que se deben reclamar en cada desalojo.
- **eviction-hard** describe un conjunto de umbrales de desalojo (como **memory.available<1Gi**) que, si se cumplen, activarían un desalojo de pod.

Localización de fallas

Si los pods no se desalojan cuando el nodo está defectuoso, realice los siguientes pasos para localizar la falla:

Después de ejecutar el siguiente comando, el resultado del comando muestra que muchos pods están en el estado Evicted.

```
kubectl get pods
```

Los resultados de la comprobación se registrarán en los logs de kubelet del nodo. Puede ejecutar el siguiente comando para buscar la información:

```
cat /var/paas/sys/log/kubernetes/kubelet.log | grep -i Evicted -C3
```

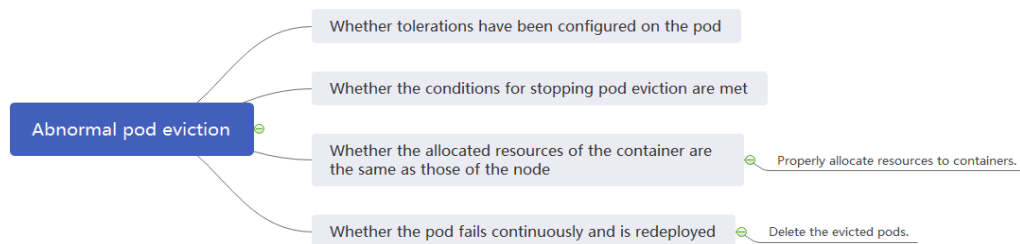
Proceso de solución de problemas

Los métodos de resolución de problemas se ordenan en función de la probabilidad de ocurrencia de las posibles causas. Se recomienda comprobar las posibles causas de alta probabilidad a baja probabilidad para localizar rápidamente la causa del problema.

Si la falla persiste después de rectificar una posible causa, compruebe otras posibles causas.

- **Concepto de comprobación 1: Si las tolerancias se han configurado en el pod**
- **Concepto de comprobación 2: Si se cumplen las condiciones para detener el desalojo de pods**
- **Concepto de comprobación 3: Si los recursos asignados del contenedor son los mismos que los del nodo**
- **Concepto de comprobación 4: Si el pod falla continuamente y se redistribuye**

Figura 6-8 Proceso de solución de problemas



Concepto de comprobación 1: Si las tolerancias se han configurado en el pod

Utilice `kubectl` o elija **More > Edit YAML** junto a la carga de trabajo correspondiente para comprobar si las tolerancias están instaladas en la carga de trabajo. Para obtener más información, véase <https://kubernetes.io/docs/concepts/configuration/taint-and-toleration/>.

Concepto de comprobación 2: Si se cumplen las condiciones para detener el desalojo de pods

Si el número de nodos en un clúster es menor que 50 y el número de nodos defectuosos representa más del 55% del total de nodos, el desalojo de pod se suspenderá. En este caso, Kubernetes intentará desalojar la carga de trabajo del nodo defectuoso. Para obtener más información, véase <https://kubernetes.io/docs/concepts/architecture/nodes/>.

Concepto de comprobación 3: Si los recursos asignados del contenedor son los mismos que los del nodo

Un contenedor desalojado se programa con frecuencia en el nodo original.

Causa posible

Un nodo desaloja un contenedor basado en el uso de recursos del nodo. El contenedor desalojado se programa según los recursos de nodo asignados. El desalojo y la programación se basan en diferentes reglas. Por lo tanto, un contenedor desalojado puede programarse de nuevo en el nodo original.

Solución

Asigne los recursos correctamente a cada contenedor.

Concepto de comprobación 4: Si el pod falla continuamente y se redistribuye

Un pod de carga de trabajo en el clúster falla y se está redistribuyendo constantemente.

Análisis

Después de que un pod es desalojado y programado para un nuevo nodo, si los pods en ese nodo también están siendo desalojados, el pod será desalojado de nuevo. Los pods pueden ser desalojados repetidamente.

Si el desalojo es activado por `kube-controller-manager`, se deja un pod en el estado `Terminating`. Solo se elimina automáticamente después de que se restablezca el nodo en el que

se encuentra el contenedor. Si el nodo se ha eliminado o no se puede restaurar debido a otras razones, puede eliminar por la fuerza el pod.

Si el desalojo es provocado por kubelet, se deja un pod en el estado Evicted. Solo se utiliza para la localización posterior de fallas y se puede eliminar directamente.

Solución

Ejecute el siguiente comando para eliminar los pods desalojados:

```
kubectl get pods <namespace> | grep Evicted | awk '{print $1}' | xargs kubectl delete pod <namespace>
```

En el comando anterior <namespace> indica el nombre del espacio de nombres. Establezca en función de los requisitos del sitio.

Referencia

Kubelet no elimina los pods desalojados

Envío de un ticket de servicio

Si el problema persiste [envíe un ticket de servicio](#).

6.1.6 ¿Qué debo hacer si no se puede montar un volumen de almacenamiento o si el tiempo de montaje se agota?

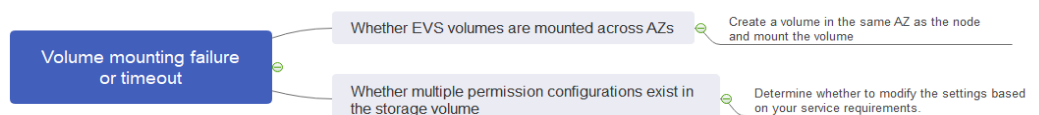
Localización de fallas

Los métodos de resolución de problemas se ordenan en función de la probabilidad de ocurrencia de las posibles causas. Se recomienda comprobar las posibles causas de alta probabilidad a baja probabilidad para localizar rápidamente la causa del problema.

Si la falla persiste después de rectificar una posible causa, compruebe otras posibles causas.

- **Concepto de comprobación 1: Si los volúmenes de EVS están montados en las AZ**
- **Concepto de comprobación 2: Si existen múltiples configuraciones de permisos en el volumen de almacenamiento**
- **Concepto de comprobación 3: Si hay más de una réplica para una Deployment con volúmenes de EVS**
- **Concepto de comprobación 4: Si el sistema de archivos de disco de EVS está dañado**

Figura 6-9 Localización de fallas



Concepto de comprobación 1: Si los volúmenes de EVS están montados en las AZ

Síntomas

El montaje de un volumen de EVS en un StatefulSet se agota.

Localización de fallas

Si el nodo es de **AZ 1** pero el volumen que se va a montar es de **AZ 2**, el tiempo de montaje se agota y el volumen no se puede montar.

Solución

Cree un volumen en la misma AZ que el nodo y monte el volumen.

Concepto de comprobación 2: Si existen múltiples configuraciones de permisos en el volumen de almacenamiento

Si el volumen que se va a montar almacena demasiados datos e implica configuraciones relacionadas con permisos, los permisos de archivo deben modificarse uno por uno, lo que da como resultado el tiempo de espera del montaje.

Localización de fallas

- Compruebe si el campo **securityContext** contiene **runAsuser** y **fsGroup**. **securityContext** es un campo de Kubernetes que define la configuración de permisos y control de acceso de pods o contenedores.
- Compruebe si los comandos de inicio contienen comandos utilizados para consultar o modificar permisos de archivo, como **ls**, **chmod** y **chown**.

Solución

Determine si desea modificar la configuración en función de sus requisitos de servicio.

Concepto de comprobación 3: Si hay más de una réplica para una Deployment con volúmenes de EVS

Síntomas

No se puede crear el pod y se informa de un evento que indica que no se puede agregar el almacenamiento.

```
Multi-Attach error for volume "pvc-62a7a7d9-9dc8-42a2-8366-0f5ef9db5b60" Volume is already used by pod(s) testttt-7b774658cb-1c98h
```

Localización de fallas

Compruebe si el número de réplicas de la Deployment es mayor que 1.

Si la Deployment utiliza un volumen de EVS, el número de réplicas solo puede ser 1. Si especifica más de dos pods para la Deployment en el backend, CCE no restringe la creación de la implementación. Sin embargo, si estos pods se programan para diferentes nodos, algunos pods no se pueden iniciar porque los volúmenes EVS utilizados por los pods no se pueden montar en los nodos.

Solución

Establezca el número de réplicas de la Deployment que utiliza un volumen de EVS en 1 o utilice otros tipos de volumen.

Concepto de comprobación 4: Si el sistema de archivos de disco de EVS está dañado

Síntomas

El pod no se puede crear y se muestra información similar a la siguiente, que indica que el sistema de archivos de disco está dañado:

```
MountVolume.MountDevice failed for volume "pvc-08178474-c58c-4820-a828-14437d46ba6f" : rpc error: code = Internal desc = [09060def-afd0-11ec-9664-fa163eef47d0] /dev/sda has file system, but it is detected to be damaged
```

Solución

Haga una copia de respaldo del disco en EVS y ejecute el siguiente comando para restaurar el sistema de archivos:

```
fsck -y {Drive letter}
```

6.1.7 ¿Qué debo hacer si una carga de trabajo permanece en el estado de creación?

Síntoma

Después de cambiar el nodo, la carga de trabajo en el nodo siempre está en el estado de creación.

Impacto

Los clústeres que han habilitado una política de gestión de CPU se verán afectados.

Solución

La opción de kubelet **cpu-manager-policy** es **static** por defecto. Esto permite otorgar una afinidad y exclusividad mejoradas de la CPU a los pods con ciertas características de recursos en el nodo. Si modifica las especificaciones del nodo de CCE en la consola de ECS, la información original de la CPU no coincide con la nueva información de la CPU. Como resultado, las cargas de trabajo del nodo no se pueden reiniciar ni crear.

Paso 1 Inicie sesión en el nodo de CCE (ECS) y elimine el archivo **cpu_manager_state**.

Ejemplo del comando para eliminar el archivo:

```
rm -rf /mnt/paas/kubernetes/kubelet/cpu_manager_state
```

Paso 2 Reinicie el nodo o kubelet. El siguiente es el comando de reinicio kubelet:

```
systemctl restart kubelet
```

Compruebe que las cargas de trabajo del nodo se pueden reiniciar o crear correctamente.

Para obtener más información, véase [¿Qué debo hacer si no puedo reiniciar o crear cargas de trabajo en un nodo después de modificar las especificaciones del nodo?](#).

----Fin

6.1.8 ¿Qué debo hacer si no se pueden eliminar los pods en el estado de terminación?

Síntoma

Cuando un nodo está en el estado Unavailable, CCE migra los pods de contenedor en el nodo y establece los pods que se ejecutan en el nodo en el estado **Terminating**.

Después de restaurar el nodo, los pods en estado **Terminating** se eliminan automáticamente.

Sin embargo, algunos pods permanecen en el estado **Terminating**.

```
#kubectl get pod -n aos
NAME                                READY   STATUS    RESTARTS   AGE
aos-apiserver-5f8f5b5585-s9192     1/1    Terminating    0         3dlh
aos-cmdbserver-789bf5b497-6rwrq    1/1    Running         0         3dlh
aos-controller-545d78bs8d-vm6j9    1/1    Running         3         3dlh
```

La ejecución de **kubectrl delete pods <podname> -n <namespace>** no puede eliminar los pods.

```
kubectrl delete pods aos-apiserver-5f8f5b5585-s9192 -n aos
```

Solución

Puede ejecutar el siguiente comando para eliminar a la fuerza los pods creados de cualquier manera:

```
kubectrl delete pods <pod> --grace-period=0 --force
```

Por lo tanto, ejecute el siguiente comando para eliminar el pod:

```
kubectrl delete pods aos-apiserver-5f8f5b5585-s9192 --grace-period=0 --force
```

6.1.9 ¿Qué debo hacer si una carga de trabajo se detiene debido a la eliminación de pods?

Problema

Una carga de trabajo está en estado **Stopped**.

Causa:

El campo **metadata.enable** del archivo YAML de la carga de trabajo es **false**. Como resultado, el pod de la carga de trabajo se elimina y la carga de trabajo está en el estado detenido.

```
kind: Deployment
apiVersion: apps/v1
metadata:
  name: test
  namespace: default
  selfLink: /apis/apps/v1/namespaces/default/deployments/test
  uid: b130db9f-9306-11e9-a2a9-fa163eaff9f7
  resourceVersion: '7314771'
  generation: 1
  creationTimestamp: '2019-06-20T02:54:16Z'
  labels:
    appgroup: ''
  annotations:
    deployment.kubernetes.io/revision: '1'
    description: ''
  enable: false
spec:
```

Solución

Elimine el campo **enable** o configúrelo en **true**.

6.1.10 ¿Qué debo hacer si se produce un error al desplegar un servicio en el nodo de GPU?

Síntoma

Las siguientes excepciones se producen cuando los servicios se despliegan en los nodos de la GPU en un clúster de CCE:

1. No se puede consultar la memoria de la GPU de los contenedores.
2. Se despliegan siete servicios de GPU, pero solo se puede acceder a dos de ellos correctamente. Los errores se notifican durante el inicio de los cinco servicios restantes.
 - Las versiones de CUDA de los dos servicios a los que se puede acceder correctamente son 10.1 y 10.0, respectivamente.
 - Las versiones de CUDA de los servicios que fallan también son 10.0 y 10.1.
3. Los archivos llamados **core.*** se encuentran en los contenedores de servicio de la GPU. No existían los archivos de este tipo en ninguno de los despliegues anteriores.

Localización de fallas

1. La versión del controlador del complemento gpu es demasiado antigua. Después de descargar e instalar un nuevo controlador, se rectifica la falla.
2. Las cargas de trabajo no declaran que se requieren los recursos de GPU.

Solución sugerida

Después de instalar el complemento gpu-device en el nodo, la herramienta de línea de comandos nvidia-smi se almacena en el directorio **/opt/cloud/cce/nvidia/bin**. Si la herramienta de línea de comandos aún no está disponible después de instalar el complemento, la causa común es que el controlador de NVIDIA no se puede instalar. Compruebe si el controlador de NVIDIA se ha descargado correctamente. (El archivo del controlador se puede encontrar en el directorio **/opt/cloud/cce/nvidia**.)

Si la dirección del controlador es incorrecta, desinstale el complemento, vuelva a instalarlo y configure la dirección correcta.

NOTA

Se recomienda almacenar el controlador de NVIDIA en el bucket de OBS y establecer la política del bucket para que sea de lectura pública.

Enlaces útiles

- [¿Cómo puedo rectificar fallas cuando se utiliza el controlador de NVIDIA para iniciar contenedores en nodos de GPU?](#)
- [Instalar el complemento gpu](#)

6.1.11 ¿Qué debo hacer si se notifican los errores relacionados con sandbox cuando el pod permanece en el estado de creación?

Síntoma

El pod permanece en el estado de creación durante mucho tiempo, y se notifican los errores relacionados con el sandbox.

```
Failed create pod sandbox: rpc error: code = Unknown desc = [ failed to setup sandbox .....
```

Solución

Seleccione un método de solución de problemas para el clúster:

Clústeres de V1.13

NOTA

Este método solo se aplica a clústeres de v1.13.

1. Los errores de entorno aislado generalmente son causados por el inicio anormal de los componentes del contenedor en el nodo. Puede ejecutar el comando **systemctl status canal** para comprobar los componentes del contenedor y ejecutar el comando **systemctl restart canal** para reiniciar el componente anormal.
2. Todos los componentes del contenedor en el nodo son normales, pero falta el archivo de la CNI **loopback**. El error es el siguiente: **network: failed to find complemento "loopback" in path [/opt/cni/bin]**. Puede copiar una versión completa del archivo **loopback** de la región actual u otras regiones que compartan las mismas versiones de clúster (se pueden ignorar las versiones menores) y colocar el archivo **loopback** en la ruta de acceso **/opt/cni/bin/**. A continuación, reinicie el componente de canal.

Clústeres anteriores a V1.13

1. Los errores de entorno aislado generalmente son causados por el inicio anormal de los componentes del contenedor en el nodo. Puede ejecutar el comando **su paas -c '/var/paas/monit/bin/monit summary'** para comprobar los componentes del contenedor y ejecutar el comando **su paas -c '/var/paas/monit/bin/monit restart canal'** para reiniciar el componente anormal.
2. Todos los componentes del contenedor en el nodo son normales, pero falta el archivo de la CNI **loopback**. El error es el siguiente: **network: failed to find complemento "loopback" in path [/opt/cni/bin]**. Puede copiar una versión completa del archivo **loopback** de la región actual u otras regiones que compartan las mismas versiones de clúster (se pueden ignorar las versiones menores) y colocar el archivo **loopback** en la ruta de acceso **/opt/cni/bin/**. A continuación, reinicie el componente de canal.

6.1.12 ¿Por qué el pod no escribe datos?

Eventos de pod

El sistema de archivos del nodo donde se encuentra el pod está dañado. Como resultado, el pod recién creado no puede escribir datos en **/var/lib/kubelet/device-plugins/.xxxxx**. Pueden ocurrir eventos similares a los siguientes en el pod:

```
Message: Pod Update Plugin resources failed due to failed to write checkpoint
file "kubelet_internal_checkpoint": open /var/lib/kubelet/device-plugins/.xxxxxx:
read-only file system, which is unexpected.
```

```
[root@10.0.0-213 paaa]# kubectl describe pod trunlport-test1-d84dc649-zxfpk
Name:          trunlport-test1-d84dc649-zxfpk
Namespace:    default
Priority:      0
Node:         10.0.0.77/
Start Time:   Sat, 20 Feb 2021 16:43:35 +0800
Labels:       app=trunlport-test1
              pod-template-hash=d84dc649
              version=v1
Annotations:  kubernetes.io/psp: psp-global
              metrics.alpha.kubernetes.io/custom-endpoints: [{"api":"","path":"","port":"","names":""}]
Status:       Failed
Reason:       UnexpectedAdmissionError
Message:      Pod Update plugin resources failed due to failed to write checkpoint file "kubelet_internal_checkpoint": open /var/lib/kubelet/device-plugins/.762832416: read-only file sys
tem, which is unexpected.
IP:           <none>
Controlled By: ReplicaSet/trunlport-test1-d84dc649
Containers:
  container-0:
    Image:      100.125.4.7:28262/cce-test/tomcat:latest
    Port:       <none>
    Host Port:  <none>
    Limits:
      cpu:      250m
      memory:   512Mi
    Requests:
      cpu:      250m
      memory:   512Mi
    Environment:
      <none>
```

Tales pods anormales se registran en eventos de error pero no ocupan recursos del sistema.

Procedimiento

Hay muchas causas para las excepciones del sistema de archivos, por ejemplo, el nodo principal físico se enciende o apaga inesperadamente. Si los sistemas de archivos no se restauran y un gran número de pods se vuelve anormal (lo que no afecta a los servicios), realice los siguientes pasos:

Paso 1 Ejecute el comando `kubectl drain <node-name>` para marcar el nodo como no programado y desaloje los pods existentes a otros nodos.

```
kubectl drain <node-name>
```

Paso 2 Localice la causa de la excepción del sistema de archivos y rectifique la falla.

Paso 3 Ejecute el siguiente comando para hacer que el nodo sea programable:

```
kubectl uncordon <node-name>
```

----Fin

Limpieza de los pod anormales

- El mecanismo de recolección de basura de kubelet es el mismo que el de la comunidad. Después de borrar el propietario (por ejemplo, Deployment) del pod, también se borra el pod anormal.
- Puede ejecutar el comando kubelet para eliminar el pod registrado como anormal.

6.1.13 ¿Por qué se suspende la creación o eliminación de pods en un nodo donde está montado el almacenamiento de archivos?

Síntoma

En el nodo en el que se montan los volúmenes de SFS o de SFS Turbo, las tareas de eliminación de pods permanecen en estado **Stopping** y las tareas de creación de pods siguen siendo **Creating**.

Causas posibles

- El almacenamiento de archivos backend se elimina. Como resultado, no se puede acceder al punto de montaje.

- La red entre el nodo y el almacenamiento de archivos es anormal. Como resultado, no se puede acceder al punto de montaje.

Solución

Paso 1 Inicie sesión en el nodo en el que está montado el almacenamiento de archivos y ejecute el siguiente comando para encontrar la ruta de montaje del almacenamiento de archivos:

findmnt

Ejemplo de ruta de montaje: **/mnt/paas/kubernetes/kubelet/pods/7b88feaf-71d6-4e6f-8965-f5f0766d9f35/volumes/kubernetes.io~csi/sfs-turbo-ls/mount**

Paso 2 Ejecute el siguiente comando para acceder a la carpeta de almacenamiento de archivos:

```
cd /mnt/paas/kubernetes/kubelet/pods/7b88feaf-71d6-4e6f-8965-f5f0766d9f35/volumes/  
kubernetes.io~csi/sfs-turbo-ls/mount
```

Si el acceso falla, el almacenamiento de archivos se elimina o la red entre el almacenamiento de archivos y el nodo es anormal.

Paso 3 Ejecute el comando **umount -l** para desmontar el almacenamiento de archivos.

```
umount -l /mnt/paas/kubernetes/kubelet/pods/7b88feaf-71d6-4e6f-8965-f5f0766d9f35/  
volumes/kubernetes.io~csi/sfs-turbo-ls/mount
```

Paso 4 Reinicie kubelet.

```
systemctl restart kubelet
```

----Fin

Causa raíz

Este problema suele ocurrir cuando los montajes duros se utilizan para el almacenamiento de archivos. En este modo, todos los procesos que acceden al punto de montaje se cuelgan hasta que el acceso se realiza correctamente. Puede utilizar soportes blandos para evitar este problema. Para obtener más información, consulte [Configuración de las opciones de montaje](#).

6.1.14 Códigos de salida

Cuando un contenedor no se inicia o termina, los eventos de Kubernetes registran el código de salida para informar de la causa. En esta sección se describe cómo localizar fallas con un código de salida.

Consulta de un código de salida

Puede usar `kubectl` para conectarse al clúster y ejecutar el siguiente comando para comprobar el pod:

```
kubectl describe pod {pod name}
```

En la salida del comando, el campo **Exit Code** indica el código de estado de la última salida del programa. Si el valor no es **0**, el programa sale anormalmente. Puede analizar más a fondo la causa con este código.

```
Containers:  
container-1:
```

```

Container ID: ...
Image: ...
Image ID: ...
Ports: ...
Host Ports: ...
Args: ...
State: Running
  Started: Sat, 28 Jan 2023 09:06:53 +0000
Last State: Terminated
  Reason: Error
  Exit Code: 255
  Started: Sat, 28 Jan 2023 09:01:33 +0000
  Finished: Sat, 28 Jan 2023 09:05:11 +0000
Ready: True
Restart Count: 1
    
```

Descripción

El código de salida varía de 0 a 255.

- Si el código de salida es 0, el contenedor sale normalmente.
- Generalmente, la salida anormal es causada por el programa y tal código de salida varía de 1 a 128. En escenarios especiales, el código de salida varía de 129 a 255.
- Cuando un programa sale debido a interrupciones externas, el código de salida varía de 129 a 255. Cuando el sistema operativo envía **una señal de interrupción** al programa, el código existente es el valor de señal de interrupción más 128. Por ejemplo, si el valor de señal de interrupción de **SIGKILL** es 9, el código de estado de salida es 137 (9 + 128).
- Si el código existente no está en el rango de 0 a 255, por ejemplo, exit(-1), el código de salida se convierte automáticamente en un valor que está dentro del rango de 0 a 255.

Si el código existente es un número positivo, la fórmula de conversión es la siguiente:

```
code % 256
```

Si el código de salida es un número negativo, la fórmula de conversión es la siguiente:

```
256 - (|code| % 256)
```

Para obtener más información, consulte [Códigos de salida con significados especiales](#).

Códigos de salida comunes

Tabla 6-5 Códigos de salida comunes

Código de salida	Nombre	Descripción
0	Salida normal	El contenedor sale normalmente. Este código de estado no indica necesariamente que se produce una excepción. Cuando no hay ningún proceso en el contenedor también se puede mostrar 0.
1	Error de programa común	Hay muchas causas para esta excepción, la mayoría de las cuales son causadas por el programa. Necesita localizar la causa con los logs de contenedor. Por ejemplo, este error se produce cuando se ejecuta una imagen x86 en un nodo de Arm.

Código de salida	Nombre	Descripción
125	El contenedor no se está ejecutando.	Las causas posibles son: <ul style="list-style-type: none"> ● Se utiliza un indicador indefinido en el comando, por ejemplo, docker run --abcd. ● El comando definido por el usuario en la imagen no tiene permisos suficientes en el host local. ● El motor de contenedor no es compatible con el sistema operativo host o hardware.
126	Error de llamada al comando	El comando llamado en la imagen no se puede ejecutar. Por ejemplo, el permiso de archivo es insuficiente o el archivo no se puede ejecutar.
127	No se puede encontrar el archivo o directorio.	No se puede encontrar el archivo o directorio especificado en la imagen.
128	Parámetro de salida no válido	El contenedor sale pero no se proporciona ningún código de salida válido. Esto puede deberse a múltiples motivos. Es necesario localizar aún más la causa. Por ejemplo, una aplicación que se ejecuta en el nodo de containerd intenta invocar al comando de docker.
137	Terminación inmediata (SIGKILL)	El programa es terminado por la señal SIGKILL . Las causas comunes son las siguientes: <ul style="list-style-type: none"> ● El uso de memoria del contenedor en el pod alcanza el límite de recursos. Por ejemplo, la falta de memoria (OOM) hace que cgroup detenga el contenedor por la fuerza. ● Si ocurre OOM, el núcleo del nodo detiene algunos procesos para liberar la memoria. Como resultado, el contenedor puede terminarse. ● Si la comprobación de estado contenedor falla, kubelet detiene el contenedor. ● Otros procesos externos, como scripts maliciosos, detienen el contenedor por la fuerza.
139	Error de segmentación (SIGSEGV)	El contenedor recibe la señal SIGSEGV del sistema operativo porque el contenedor intenta acceder a una ubicación de memoria no autorizada.
143	Terminación agraciada (SIGTERM)	El contenedor se cierra correctamente según las instrucciones del host. Generalmente, este código de salida 143 no requiere solución de problemas.
255	El código de salida está fuera de rango.	El código de salida de contenedor está fuera de rango. Por ejemplo, la salida (-1) puede usarse para una salida anormal, y -1 se convierte automáticamente en 255. Se requiere más solución de problemas.

Señal de interrupción estándar de Linux

Puede ejecutar el comando **kill -l** para ver las señales y los valores correspondientes en el SO Linux.

Tabla 6-6 Señales de interrupción estándar de Linux comunes

Señal	Valor	Acción	Confirmación
SIGHUP	1	Term	Se envía cuando finaliza la conexión del terminal de usuario (normal o anormal).
SIGINT	2	Term	Señal de terminación del programa, que es enviada por el terminal pulsando Ctrl+C .
SIGQUIT	3	Core	De manera similar a SIGINT , el terminal envía el comando exit. Generalmente, el comando de salida se controla pulsando Ctrl+\ .
SIGILL	4	Core	Instrucción no válida, generalmente porque se produce un error en el archivo ejecutable.
SIGABRT	6	Core	Señal generada cuando se invoca la función abortar. El proceso termina anormalmente.
SIGFPE	8	Core	Se produce un error aritmético de coma flotante. También se producen otros errores aritméticos como el divisor 0.
SIGKILL	9	Term	Se termina cualquier proceso.
SIGSEGV	11	Core	Intento de acceder a una ubicación de memoria no autorizada.
SIGPIPE	13	Term	La tubería está desconectada.
SIGALRM	14	Term	Indica la temporización del reloj.
SIGTERM	15	Term	Señal de fin de proceso, que suele ser la salida normal del programa.
SIGUSR1	10	Term	Esta es una señal definida por el usuario en las aplicaciones.
SIGUSR2	12	Term	Esta es una señal definida por el usuario en las aplicaciones.
SIGCHLD	17	Ign	Esta señal se genera cuando un subprocesso finaliza o se interrumpe.
SIGCONT	18	Cont	Reanuda un proceso detenido.

Señal	Valor	Acción	Confirmación
SIGSTOP	19	Stop	Suspender la ejecución de un proceso.
SIGTSTP	20	Stop	Detener un proceso.
SIGTTIN	21	Stop	El proceso en segundo plano lee el valor de entrada del terminal.
SIGTTOU	22	Stop	El proceso en segundo plano lee el valor de salida del terminal.

6.2 Configuración del contenedor

6.2.1 ¿Cuándo se utiliza el procesamiento previo a la parada?

El procesamiento del servicio lleva mucho tiempo. El procesamiento previo a la parada se asegura de que durante una actualización, un pod se elimina solo cuando se ha procesado el servicio en el pod.

6.2.2 ¿Cómo configuro un FQDN para acceder a un contenedor especificado en el mismo espacio de nombres?

Contexto

Al crear una carga de trabajo, los usuarios pueden especificar un contenedor, un pod y un espacio de nombres como un FQDN para acceder al contenedor en el mismo espacio de nombres.

FQDN significa Fully Qualified Domain Name, que contiene tanto el nombre de host como el nombre de dominio. Estos dos nombres se combinan usando un punto (.).

Por ejemplo, si el nombre de host es de **bigserver** y el nombre de dominio es **mycompany.com**, el FQDN es **bigserver.mycompany.com**.

Solución

Solución 1: Utilice el nombre de dominio para la detección de servicios. El nombre del host y el espacio de nombres deben estar preconfigurados. El nombre de dominio del servicio registrado tiene el formato *service name.namespace name.svc.cluster.local*. La limitación de esta solución es que el centro de registro debe desplegarse usando contenedores.

Solución 2: Utilice la red host para implementar contenedores y, a continuación, configure la afinidad entre los contenedores y un nodo en el clúster. De esta manera, se puede determinar la dirección de servicio (es decir, la dirección de nodo) de los contenedores. La dirección registrada es la dirección IP del nodo donde se encuentra el servicio. Esta solución le permite implementar el centro de registro mediante máquinas virtuales, mientras que la desventaja es que la red host no es tan eficiente como la red contenedora.

6.2.3 ¿Qué debo hacer si las sondas de chequeo médico fallan ocasionalmente?

Cuando las sondas de vida y disponibilidad no realizan la comprobación de estado, localice primero la falla de servicio.

Las causas comunes son las siguientes:

- El procesamiento del servicio lleva mucho tiempo. Como resultado, el tiempo de respuesta se agotó.
- La configuración de la conexión Tomcat y el tiempo de espera son demasiado largos (por ejemplo, demasiadas conexiones o hilos). Como resultado, el tiempo de respuesta se agotó.
- El rendimiento del nodo donde se encuentra el contenedor, tal como la E/S del disco, alcanza el cuello de botella. Como resultado, el procesamiento del servicio se agota.

6.2.4 ¿Cómo configuro el valor umask para un contenedor?

Síntoma

Un contenedor se inicia en modo **tailf /dev/null** y el permiso del directorio es **700** después de ejecutar manualmente el script de inicio. Si Kubernetes inicia el contenedor sin **tailf**, el permiso de directorio obtenido es **751**.

Solución

La razón es que los valores umask establecidos en los dos modos de inicio anteriores son diferentes. Por lo tanto, los permisos en los directorios creados son diferentes.

El valor umask se utiliza para establecer el permiso predeterminado para un archivo o directorio recién creado. Si el valor umask es demasiado pequeño, los usuarios del grupo u otros usuarios tendrán permisos excesivos, lo que plantea amenazas de seguridad para el sistema. Por lo tanto, el valor umask predeterminado para todos los usuarios se establece en **0077**. Es decir, el permiso predeterminado en los directorios creados por los usuarios es **700** y el permiso predeterminado en los archivos es **600**.

Puede agregar el siguiente contenido al script de inicio para establecer el permiso en el directorio creado a **700**:

1. Agregue **umask 0077** al archivo **/etc/bashrc** y a todos los archivos de **/etc/profile.d/**.
2. Ejecute el siguiente comando:

```
echo "umask 0077" >> $FILE
```

NOTA

FILE indica el nombre del archivo, por ejemplo, **echo "umask 0077" >> /etc/bashrc**.

3. Establezca el propietario y el grupo del archivo **/etc/bashrc** y todos los archivos de **/etc/profile.d/** en **root**.
4. Ejecute el siguiente comando:

```
chown root.root $FILE
```

6.2.5 ¿Qué puedo hacer si se informa de un error cuando se inicia un contenedor desplegado después de que se especifique el parámetro de memoria de pila de inicio de JVM para ENTRYPOINT en Dockerfile?

Descripción del problema

Después de especificar el parámetro de memoria de pila de inicio JVM para ENTRYPOINT en Dockerfile, se muestra un mensaje de error "invalid initial heap size" durante el inicio del contenedor desplegado, como se muestra en la siguiente figura:

```
[root@ecs ~]# docker run swr.cn-east-2.myhuaweicloud.com/xxxxxx/xxxxxx:xxxxxx rvice
Invalid initial heap size: -Xms2g -Xmx2g
Error: Could not create the Java Virtual Machine.
Error: A fatal exception has occurred. Program will exit.
```

Respuesta

Compruebe la configuración de ENTRYPOINT. Los siguientes ajustes son incorrectos:

```
ENTRYPOINT ["java", "-Xms2g -Xmx2g", "-jar", "xxx.jar"]
```

Puede utilizar cualquiera de los métodos siguientes para resolver el problema:

- **(Recomendado)** Escribe el comando de inicio del contenedor en el archivo **Workloads > Container Settings > Lifecycle > Startup Command** y, a continuación, el contenedor se puede iniciar correctamente.
- Cambie el formato del comando de inicio **ENTRYPOINT** a lo siguiente:

```
ENTRYPOINT exec java -Xmx2g -Xms2g -jar xxx.jar
```

6.2.6 ¿Qué es el mecanismo de reintento cuando CCE no puede iniciar un pod?

CCE es un servicio de Kubernetes totalmente administrado y es totalmente compatible con las API de Kubernetes y kubectl.

En Kubernetes, la especificación de un pod contiene un campo **restartPolicy**. El valor de **restartPolicy** puede ser **Always**, **OnFailure** o **Never**. El valor predeterminado es **Always**.

- **Always**: Cuando un contenedor falla, kubelet reinicia automáticamente el contenedor.
- **OnFailure**: Cuando un contenedor deja de funcionar y el código de salida no es 0 (que indica la salida normal), kubelet reinicia automáticamente el contenedor.
- **Never**: kubelet no reinicia el contenedor independientemente del estado de funcionamiento del contenedor.

restartPolicy se aplica a todos los contenedores de un pod.

restartPolicy solo se refiere a los reinicios de los contenedores por kubelet en el mismo nodo. Cuando los contenedores en un pod salen, kubelet los reinicia con un retardo exponencial de retroceso (10s, 20s, 40s y ...), que se tapa a los cinco minutos. Una vez que un contenedor ha estado funcionando durante 10 minutos sin ningún problema, kubelet restablece el temporizador de retroceso de reinicio para el contenedor.

Los ajustes de **restartPolicy** varían en función del controlador:

- **Replication Controller (RC) y DaemonSet:** `restartPolicy` deben ajustarse a **Always** para garantizar el funcionamiento continuo de los contenedores.
- **Job:** `restartPolicy` debe establecerse en **OnFailure** o **Never** para asegurarse de que los contenedores no se reinician después de ejecutarse.

6.3 Monitoreo de alarmas

6.3.1 ¿Durante cuánto tiempo se almacenan los eventos de una carga de trabajo?

En un clúster de v1.7.3-r12, 1.9.2-r3, o una versión posterior, la información de eventos de una carga de trabajo se almacena durante una hora, después de lo cual los datos se borran automáticamente.

En clústeres anteriores a 1.7.3-r12, los eventos se almacenan durante 24 horas.

6.4 Políticas de planificación

6.4.1 ¿Cómo distribuyo uniformemente varios pods a cada nodo?

El componente kube-scheduler en Kubernetes es la programación responsable de pods. Para cada pod recién creado u otros pods no programados, kube-scheduler selecciona un nodo óptimo de ellos para ejecutarse. kube-scheduler selecciona un nodo para un pod en una operación de 2 pasos: filtrado y puntuación. En la etapa de filtrado, todos los nodos en los que es factible programar el pod son filtrados. En la etapa de puntuación, kube-scheduler clasifica los nodos restantes para elegir la colocación de cápsulas más adecuada. Finalmente, kube-scheduler programa el pod al nodo con la puntuación más alta. Si hay más de un nodo con las puntuaciones iguales, kube-scheduler selecciona uno de ellos al azar.

BalancedResourceAllocation es solo una de las prioridades de puntuación. Otros elementos de puntuación también pueden causar una distribución desigual. Para obtener más información sobre la programación, consulte [Kubernetes Scheduler](#) y [Políticas de programación](#).

Puede configurar las políticas de antiafinidad de pods para distribuir los pods de manera uniforme en diferentes nodos.

Por ejemplo:

```
kind: Deployment
apiVersion: apps/v1
metadata:
  name: nginx
  namespace: default
spec:
  replicas: 2
  selector:
    matchLabels:
      app: nginx
  template:
    metadata:
      labels:
        app: nginx
    spec:
      containers:
```

```
- name: container-0
  image: nginx:alpine
  resources:
    limits:
      cpu: 250m
      memory: 512Mi
    requests:
      cpu: 250m
      memory: 512Mi
  affinity:
    podAntiAffinity:
      preferredDuringSchedulingIgnoredDuringExecution:
        - podAffinityTerm:
            labelSelector:
              matchExpressions:
                - key: app
                  operator: In
                  values:
                    - nginx
            namespaces:
              - default
            topologyKey: kubernetes.io/hostname
        # It takes effect on the
node.
    imagePullSecrets:
      - name: default-secret
```

6.4.2 ¿Cómo puedo evitar que un contenedor en un nodo sea desalojado?

Contexto

Durante la planificación de la carga de trabajo, dos contenedores en un nodo pueden competir por recursos. Como resultado, kubelet desaloja a ambos contenedores. En esta sección se describe cómo establecer una política para conservar uno de los contenedores.

Solución

kubelet utiliza los siguientes criterios para desalojar un pod:

- Calidad de Service (QoS): **BestEffort**, **Burstable** y **Guaranteed**
- Recursos consumidos basados en la solicitud de programación del pod

Los pods de diferentes clases de QoS son desalojados en la siguiente secuencia:

BestEffort -> Burstable -> Guaranteed

- Pods de BestEffort: Estos pods tienen la prioridad más baja. Serán los primeros en morir si el sistema se queda sin memoria.
- Pods de burstable: Estos pods se matarán si el sistema se queda sin memoria y no existen pods de BestEffort.
- Pods de Guaranteed: Estos pods se matarán si el sistema se queda sin memoria y no existen pods de Burstable o de BestEffort.

 **NOTA**

- Si los procesos en un pod se eliminan debido al uso excesivo de recursos (mientras que los recursos del nodo son todavía suficientes), el sistema tiende a reiniciar el contenedor o a crear un pod.
- Si los recursos son suficientes, puede asignar la clase QoS de Guaranteed a todos los pods. De esta manera, se utilizan más recursos informáticos para mejorar el rendimiento y la estabilidad del servicio, reduciendo el tiempo y los costos de solución de problemas.
- Para mejorar la utilización de los recursos, asigne la clase QoS Guaranteed a los pods de servicio y Burstable o BestEffort a otros pods (por ejemplo, filebeat).

6.4.3 ¿Por qué los pods no se distribuyen uniformemente a los nodos?

El componente kube-scheduler en Kubernetes es la programación responsable de pods. Para cada pod recién creado u otros pods no programados, kube-scheduler selecciona un nodo óptimo de ellos para ejecutarse. kube-scheduler selecciona un nodo para un pod en una operación de 2 pasos: filtrado y puntuación. En la etapa de filtrado, todos los nodos en los que es factible programar el pod son filtrados. En la etapa de puntuación, kube-scheduler clasifica los nodos restantes para elegir la colocación de cápsulas más adecuada. Finalmente, kube-scheduler programa el pod al nodo con la puntuación más alta. Si hay más de un nodo con las puntuaciones iguales, kube-scheduler selecciona uno de ellos al azar.

BalancedResourceAllocation es solo una de las prioridades de puntuación. Otros elementos de puntuación también pueden causar una distribución desigual. Para obtener más información sobre la programación, consulte [Kubernetes Scheduler](#) y [Políticas de programación](#).

6.4.4 ¿Cómo desalojo todos los pods de un nodo?

Puede ejecutar el comando **kubectl drain** para desalojar de forma segura todos los pods de un nodo.

 **NOTA**

De forma predeterminada, el comando **kubectl drain** conserva algunos pods del sistema, por ejemplo, everest-csi-driver.

Paso 1 Utilice kubectl para conectarse al clúster.

Paso 2 Compruebe los nodos en el clúster.

```
kubectl get node
```

Paso 3 Seleccione un nodo y vea todos los pods del nodo.

```
kubectl get pod --all-namespaces -owide --field-selector  
spec.nodeName=192.168.0.160
```

Los pods en el nodo antes del desalojo son los siguientes:

NAMESPACE	NAME	READY	STATUS
RESTARTS	AGE	IP	NOMINATED NODE
			NODE
			READINESS
GATES			
default	nginx-5bcc57c74b-lgcvh	1/1	Running
0	7m25s	10.0.0.140	192.168.0.160 <none> <none>
kube-system	coredns-6fcd88c4c-97p6s	1/1	Running
0	3h16m	10.0.0.138	192.168.0.160 <none> <none>
kube-system	everest-csi-controller-56796f47cc-99dtm	1/1	Running
0	3h16m	10.0.0.139	192.168.0.160 <none> <none>
kube-system	everest-csi-driver-dpfz1	2/2	Running
2	12d	192.168.0.160	192.168.0.160 <none> <none>

```
kube-system  icagent-tpfpv  1/1  Running
1            12d         192.168.0.160  192.168.0.160  <none>  <none>
```

Paso 4 Desaloja todos los pods del nodo.

```
kubectl drain 192.168.0.160
```

Si existe un pod montado con almacenamiento local o controlado por un conjunto de DaemonSet en el nodo, el mensaje "error: unable to drain node "192.168.0.160", aborting command..." se mostrará. La orden de desalojo no tiene efecto. Puede agregar los siguientes parámetros al final del comando anterior para desalojar por la fuerza el pod:

- **--delete-emptydir-data**: desaloja por la fuerza los pods montados con almacenamiento local, por ejemplo, coredns.
- **--ignore-daemonsets**: desaloja por la fuerza los pods de DaemonSet, por ejemplo, everest-csi-driver.

En el ejemplo, ambos tipos de pods existen en el nodo. Por lo tanto, la orden de desalojo es la siguiente:

```
kubectl drain 192.168.0.160 --delete-emptydir-data --ignore-daemonsets
```

Paso 5 Después del desalojo, el nodo se marca automáticamente como no programado. Es decir, el nodo está contaminado **node.kubernetes.io/unschedulable = : NoSchedule**.

Después del desalojo, solo se conservan los pods del sistema en el nodo.

NAMESPACE	NAME	READY	STATUS	RESTARTS	AGE
IP	NODE	NOMINATED	READINESS	GATES	
kube-system	everest-csi-driver-dpfz1	2/2	Running	2	12d
192.168.0.160	192.168.0.160	<none>	<none>		
kube-system	icagent-tpfpv	1/1	Running	1	12d
192.168.0.160	192.168.0.160	<none>	<none>		

----Fin

Operaciones relacionadas

Operaciones de drain, cordon y uncordon de kubectl:

- **drain**: Desaloja de forma segura todos los pods de un nodo y marca el nodo como no programado.
- **cordon**: Marca el nodo como no programado. Es decir, el nodo está contaminado **node.kubernetes.io/unschedulable = : NoSchedule**.
- **uncordon**: Marca el nodo como programable.

Para obtener más información, consulte la [documentación de kubectl](#).

6.5 Otros

6.5.1 ¿Qué debo hacer si no se puede reiniciar una tarea programada después de haber sido detenida durante un período de tiempo?

Si una tarea programada se detiene durante la ejecución, antes de su reinicio, el sistema calcula la diferencia entre la última vez que la tarea se ejecutó con éxito y la hora actual y

compara la diferencia de tiempo con el período de tarea programada multiplicado por 100. Si la diferencia de tiempo es mayor que el período multiplicado por 100, la tarea programada no se activará de nuevo. Para obtener más información, consulte [Limitaciones de CronJob](#).

Por ejemplo, supongamos que un trabajo cron está configurado para crear un trabajo cada minuto a partir de las 08:30:00 y que el campo **startingDeadlineSeconds** no está definido. Si el controlador de trabajo cron deja de ejecutarse de 08:29:00 a 10:21:00, el trabajo no se iniciará debido a la diferencia de tiempo entre 08:29:00 y 10:21:00. 00 supera los 100 minutos, es decir, el número de tiempos de programación perdidos supera los 100 (en el ejemplo, un período de programación es de 1 minuto).

Si se establece el campo **startingDeadlineSeconds**, el controlador calcula el número de trabajos perdidos en los últimos x segundos (el x indica el valor de **startingDeadlineSeconds**). Por ejemplo, si **startingDeadlineSeconds** se establece en **200**, el controlador cuenta el número de trabajos perdidos en los últimos 200 segundos. En este caso, si el controlador de trabajo cron deja de ejecutarse de 08:29:00 a 10:21:00, el trabajo comenzará de nuevo a las 10:22:00, porque solo se pierden tres solicitudes de programación en los últimos 200 segundos (en el ejemplo, un periodo de programación es de 1 minuto).

Solución

Configure el parámetro **startingDeadlineSeconds** en un trabajo cron. Este parámetro solo se puede crear o modificar mediante kubectl o las API.

Ejemplo de YAML:

```
apiVersion: batch/v1
kind: CronJob
metadata:
  name: hello
spec:
  startingDeadlineSeconds: 200
  schedule: "* * * * *"
  jobTemplate:
    spec:
      template:
        spec:
          containers:
            - name: hello
              image: busybox:1.28
              imagePullPolicy: IfNotPresent
              command:
                - /bin/sh
                - -c
                - date; echo Hello
          restartPolicy: OnFailure
```

Si vuelve a crear un trabajo cron, puede evitar temporalmente este problema.

6.5.2 ¿Qué es un servicio sin cabeza cuando creo un StatefulSet?

El servicio de detección inter-pod de CCE corresponde al Service sin cabeza de Kubernetes. Los Services sin cabeza especifican **None** para la IP del clúster (spec:clusterIP) en YAML, lo que significa que no se asigna ninguna IP del clúster.

Diferencias entre los Services sin cabeza y los Services comunes

- Services comunes:

Un servicio puede estar respaldado por múltiples puntos de conexión (pods). Un cliente accede a la dirección IP del clúster y la solicitud se reenvía al servidor real basándose en

las reglas iptables o IPVS para implementar el equilibrio de carga. Por ejemplo, un Service tiene dos puntos de conexión, pero solo se devuelve la dirección de servicio durante la consulta de DNS. Las reglas iptables o IPVS determinan el servidor real al que accede el cliente. El cliente no puede acceder al punto de conexión especificado.

- Services sin cabeza:

Cuando se accede a un Service sin cabeza, se devuelve el punto de conexión real (dirección IP del pod). El Service sin cabeza apunta directamente a cada punto de conexión es decir, cada pod tiene un nombre de dominio DNS. De esta manera, los pods pueden acceder entre sí, logrando el descubrimiento y el acceso inter-pod.

Escenarios de aplicaciones de Service sin cabeza

Si no hay diferencia entre varios pods de una carga de trabajo, puede usar un servicio común y usar el clúster kube-proxy para implementar el balanceo de carga, por ejemplo, una Nginx Deployment.

Sin embargo, en algunos escenarios de aplicación, los pods de una carga de trabajo tienen diferentes roles. Por ejemplo, en un clúster de Redis, cada pod de Redis es diferente. Tienen una relación maestro/esclavo y necesitan comunicarse entre sí. En este caso, un Service común no puede acceder a un pod especificado con la dirección IP del clúster. Por lo tanto, debe permitir que el Service sin cabeza acceda directamente a la dirección IP real del pod para implementar el acceso mutuo entre pods.

Los Services sin cabeza trabajan con [StatefulSet](#) para desplegar las aplicaciones de stateful, como Redis y MySQL.

6.5.3 ¿Qué debo hacer si se muestra un mensaje de error "Auth is empty" cuando se extrae una imagen privada?

Descripción del problema

Cuando reemplaza la imagen de un contenedor en una carga de trabajo creada y usa una imagen cargada en la consola de CCE, aparece un mensaje de error "Auth is empty, only accept X-Auth-Token or Authorization" cuando se extrae la imagen cargada.

```
Failed to pull image "IP address:Port number /magicdoom/tidb-operator:latest":  
rpc error: code = Unknown desc = Error response from daemon: Get https://IP  
address:Port number /v2/magicdoom/tidb-operator/manifests/latest: error parsing  
HTTP 400 response body: json: cannot unmarshal number into Go struct field  
Error.code of type errcode.ErrorCode: "{\n"errors\": [\n{"code\":400,\n"message\":  
\"Auth is empty, only accept X-Auth-Token or Authorization.\"}]\n}"
```

Solución

Puede seleccionar una imagen privada para crear una aplicación en la consola de CCE. En este caso, CCE lleva automáticamente el secreto. Este problema no se producirá durante la actualización.

Cuando crea una carga de trabajo con una API, puede incluir el secreto en Deployments para evitar este problema durante la actualización.

```
imagePullSecrets:  
- name: default-secret
```

6.5.4 ¿Por qué no se puede programar un pod en un nodo?

- Paso 1** Compruebe si el nodo y el Docker son normales. Para obtener más información, véase [Concepto de comprobación 7: Si los componentes internos son normales](#).
- Paso 2** Si el nodo y el Docker son normales, compruebe si se ha configurado una política de afinidad para el pod. Para obtener más información, véase [Concepto de comprobación 3: Configuración de afinidad y antiafinidad de la carga de trabajo](#).
- Paso 3** Compruebe si los recursos en el nodo son suficientes. Si los recursos son insuficientes, amplíe la capacidad o agregue los nodos.

----Fin

6.5.5 ¿Qué es la política de extracción de imágenes para contenedores en un clúster de CCE?

Se requiere una imagen de contenedor para crear un contenedor. Las imágenes pueden almacenarse localmente o en un repositorio de imágenes remoto.

El campo **imagePullPolicy** del archivo de configuración de Kubernetes se utiliza para describir la política de extracción de imágenes. Este campo tiene las siguientes opciones de valor:

- **Always:** Siempre fuerce una extracción.
`imagePullPolicy: Always`
- **IfNotPresent:** La imagen se extrae solo si no está ya presente localmente.
`imagePullPolicy: IfNotPresent`
- **Never:** Se supone que la imagen existe localmente. No se hace ningún intento de extraer la imagen.
`imagePullPolicy: Never`

Descripción

1. Si este campo se establece en **Always**, la imagen se extrae del repositorio remoto cada vez que se inicia o se reinicia un contenedor.
Si **imagePullPolicy** se deja en blanco, el valor predeterminado de la política es **Always**.
2. Si la política está establecida en **IfNotPresent**:
 - a. Si la imagen requerida no existe localmente, se extraerá del repositorio remoto.
 - b. Si el contenido, excepto la etiqueta, de la imagen requerida es el mismo que el de la imagen local, y la imagen con esa etiqueta solo existe en el repositorio remoto, Kubernetes no extraerá la imagen del repositorio remoto.

6.5.6 ¿Por qué está desinstalado el punto de montaje de un contenedor Docker en el clúster Kunpeng?

Síntoma

Se desinstala el punto de montaje de un contenedor Docker en el clúster Kunpeng.

Causa posible

Si el nodo del clúster Kunpeng ejecuta EulerOS 2.8 y el campo **MountFlags=shared** está configurado en el archivo de servicio Docker, el punto de montaje del contenedor se desinstalará debido a la característica systemd.

Solución

Modifique el archivo Docker, elimine el campo **MountFlags=shared** y reinicie Docker.

Paso 1 Inicie sesión en el nodo.

Paso 2 Ejecute el siguiente comando para eliminar el campo **MountFlags=shared** del archivo de configuración y guarde el archivo:

```
vi /usr/lib/systemd/system/docker.service
```

```
[Service]
MountFlags=shared
Type=notify
EnvironmentFile=/etc/sysconfig/docker
EnvironmentFile=/etc/sysconfig/docker-storage
EnvironmentFile=/etc/sysconfig/docker-network
Environment=GOTRACEBACK=crash
```

Paso 3 Ejecute el siguiente comando para reiniciar Docker:

```
systemctl restart docker
```

----Fin

6.5.7 ¿Qué puedo hacer si falta una capa durante la extracción de imágenes?

Síntoma

Cuando se usa containerd como motor de contenedor, existe la posibilidad de que la capa de imagen falte cuando se tira de una imagen a un nodo. Como resultado, no se puede crear el contenedor de carga de trabajo.

```
vents:
Type      Reason      Age      From      Message
-----
Normal    Scheduled   54s     default-scheduler    Successfully assigned cattle-prometheus/prometheus-server-6c69469cf4-nfs7f to 10.14.11.139
Normal    SuccessfulMountVolume  55s     kubelet    Successfully mounted volumes for pod "prometheus-server-6c69469cf4-nfs7f_cattle-prometheus(48ac202a-649a-429c-91ca-573dbaabc72)"
Normal    SuccessfulUpdateSecurityGroup  52s     yamwise-controller    Successfully updated security group to "e6a07f09-df66-431a-8901-e60752653982"
Normal    Pulled      8s (x6 over 51s)  kubelet    Container image "100.125.0.29:5002/prometheus/busybox:1.29.2" already present on machine
Warning   FailedCreate  7s (x6 over 50s)  kubelet    Error: failed to create containerd container: error unpacking image: failed to extract layer sha256:f9f9e4e62f0689cd752390e14ade48bdec6f248899af5ab2f9ccaf54c299d: failed to get reader from content store: content digest sha256:8c3a7d61afbc60269f62c2c66445743ccc5ff22053ea209e9e6d0773b7056109: not found
```

Causa posible

Docker anterior a v1.10 es compatible con la capa cuyo **mediaType** es **application/octet-stream**. Sin embargo, containerd no es compatible con **application/octet-stream**. Como resultado, no se tira de la capa.

Solución

Puede utilizar cualquiera de los siguientes métodos para resolver este problema:

- Utilice Docker v1.11 o posterior para volver a empaquetar la imagen.

- Tire manualmente de la imagen.
 - a. Inicie sesión en el nodo.
 - b. Ejecute el siguiente comando para extraer la imagen:
ctr -n k8s.io images pull --user u:p images
 - c. Utilice la imagen recién obtenida para crear una carga de trabajo.

6.5.8 ¿Por qué el permiso de archivo y el usuario en el contenedor son signos de interrogación?

Síntoma

Si el SO del nodo es CentOS 7.6 o EulerOS 2.5 y el kernel de Debian GNU/Linux 11 (bullseye) se utiliza como contenedor de imagen base, se producen excepciones en los permisos de archivo y los usuarios.

```
[root@ ]# docker run -it debian:11 bash
root@a6b8fa7fcdea:/# ls -al
ls: cannot access 'dev': Operation not permitted
ls: cannot access 'root': Operation not permitted
ls: cannot access 'run': Operation not permitted
ls: cannot access 'lib': Operation not permitted
ls: cannot access 'mnt': Operation not permitted
ls: cannot access '.': Operation not permitted
ls: cannot access 'tmp': Operation not permitted
ls: cannot access 'proc': Operation not permitted
ls: cannot access 'bin': Operation not permitted
ls: cannot access 'srv': Operation not permitted
ls: cannot access 'sys': Operation not permitted
ls: cannot access 'var': Operation not permitted
ls: cannot access 'etc': Operation not permitted
ls: cannot access 'media': Operation not permitted
ls: cannot access 'usr': Operation not permitted
ls: cannot access 'sbin': Operation not permitted
ls: cannot access 'home': Operation not permitted
ls: cannot access 'boot': Operation not permitted
ls: cannot access 'lib64': Operation not permitted
ls: cannot access '..': Operation not permitted
ls: cannot access 'opt': Operation not permitted
ls: cannot access '.dockerenv': Operation not permitted
total 0
d????????? ? ? ? ?      ? .
d????????? ? ? ? ?      ? ..
-????????? ? ? ? ?      ? .dockerenv
d????????? ? ? ? ?      ? bin
d????????? ? ? ? ?      ? boot
d????????? ? ? ? ?      ? dev
d????????? ? ? ? ?      ? etc
d????????? ? ? ? ?      ? home
d????????? ? ? ? ?      ? lib
d????????? ? ? ? ?      ? lib64
d????????? ? ? ? ?      ? media
d????????? ? ? ? ?      ? mnt
d????????? ? ? ? ?      ? opt
d????????? ? ? ? ?      ? proc
d????????? ? ? ? ?      ? root
d????????? ? ? ? ?      ? run
d????????? ? ? ? ?      ? sbin
```

Impacto

Las excepciones se producen en los permisos de archivo y los usuarios de un contenedor.

Solución

CCE ofrece dos soluciones:

- Utilice Debian 9 o 10 como la imagen base del contenedor de servicio.
- Utilice EulerOS 2.9 o Ubuntu 18.04 como sistema operativo del nodo.

7 Redes

7.1 Planificación de la red

7.1.1 ¿Cuál es la relación entre clústeres, VPC y subredes?

Una nube privada virtual (VPC) es similar a una red de área local privada (LAN) gestionada por un gateway doméstico cuya dirección IP es 192.168.0.0/16. Una VPC es una red privada construida en la nube y proporciona un entorno de red básico para ejecutar los servidores en la nube elásticos (ECS), balanceos de carga elásticos (ELB) y middleware. Las redes de diferentes escalas se pueden configurar en función de los requisitos de servicio. Generalmente, puede establecer el bloque CIDR en 10.0.0.0/8 - 24, 172.16.0.0/12 - 24 o 192.168.0.0/16 - 24. El bloque CIDR más grande es 10.0.0.0/8, que corresponde a una red de clase A.

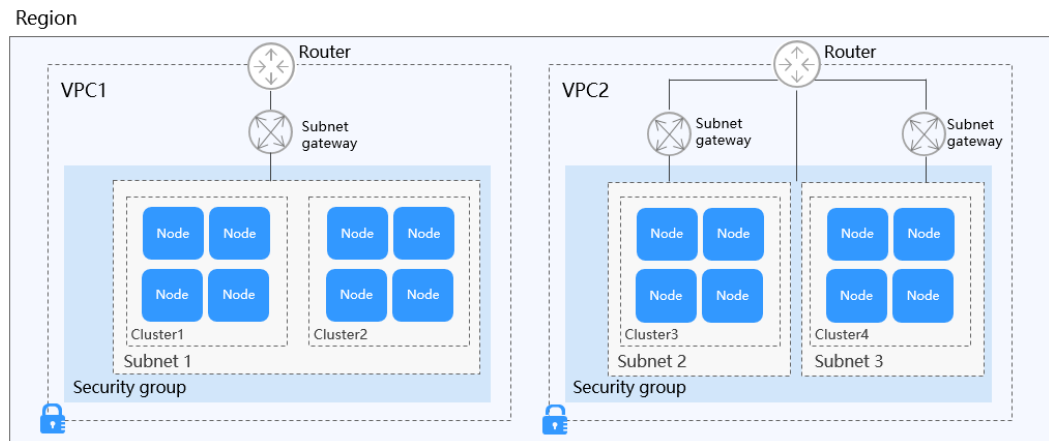
Una subred se puede dividir en varias subredes. Los grupos de seguridad se configuran para determinar si estas subredes pueden comunicarse entre sí. Esto garantiza que las subredes puedan aislarse entre sí, de modo que pueda desplegarse diferentes servicios en diferentes subredes.

Un clúster consta de uno o más servidores en la nube (también conocidos como nodos) en la misma VPC. Proporciona un grupo de recursos informáticos para ejecutar contenedores.

Como se muestra en [Figura 7-1](#), una región puede comprender múltiples VPC. Una VPC consta de una o más subredes. Las subredes se comunican entre sí a través de un gateway de subred. Se crea un clúster en una subred. Hay tres escenarios:

- Se crean los diferentes clústeres en las diferentes VPC.
- Se crean los diferentes clústeres en la misma subred.
- Se crean los diferentes clústeres en las diferentes subredes.

Figura 7-1 Relación entre clústeres, VPC y subredes



7.1.2 ¿Cómo puedo ver el bloque CIDR de VPC?

En la página de inicio de la consola de VPC, vea el **Name/ID** y el **CIDR Block** de las VPC. Puede modificar el bloque CIDR de una VPC o volver a crear una VPC.

Figura 7-2 Consulta del bloque CIDR de las VPC

You can create 45 more VPCs.

Name	IPv4 CIDR Block	Status	Subnet
vpc-demo	192.168.0.0/16	Normal	2
vpcdrs-database-fwx514861	192.168.0.0/16	Normal	1
vpc-test	192.168.0.0/16	Normal	1
CCE-AutoCreate-VPC-w5xvc	192.168.0.0/16	Normal	1
vpc-8d9c	192.168.0.0/16	Normal	1

7.1.3 ¿Cómo configuro el bloque CIDR de VPC y el bloque CIDR de subred para un clúster de CCE?

El bloque CIDR de una VPC no se puede cambiar después de crear la VPC. Al crear una VPC, asigne suficientes direcciones IP para la VPC y las subredes.

El bloque CIDR de subred se puede configurar en la consola de VPC seleccionando **Create VPC > Subnet CIDR Block** en la página **Create VPC**. Puede ver el número de direcciones IP disponibles en la configuración de bloque CIDR.

Si la máscara de subred no se establece correctamente, el número de nodos disponibles en el clúster puede ser insuficiente.

Por ejemplo:

- Si el clúster tiene 1000 nodos, puede establecer el bloque CIDR de subred en 192.168.0.0/20, que admite 4090 nodos.
- Si el bloque CIDR de VPC se establece en 192.168.0.0/16 y el bloque CIDR de subred se establece en 192.168.0.0/25, solo se admiten 122 nodos. Si crea un clúster con 200 nodos con esta VPC, solo se pueden agregar 122 nodos (incluidos los nodos maestros).

Figura 7-3 Consulta del número de direcciones IP disponibles

The screenshot shows the 'Create VPC' configuration page. Under the 'Basic Information' section, the 'IPv4 CIDR Block' is set to 172.16.0.0/24. Below this, there are three recommended CIDR blocks: 10.0.0.0/8-24, 172.16.0.0/12-24, and 192.168.0.0/16-24. In the 'Default Subnet' section, the 'AZ' is set to AZ1, and the 'IPv4 CIDR Block' is also set to 172.16.0.0/24. A red box highlights the text 'Available IP Addresses: 251' next to the CIDR block field. A warning message below states: 'The CIDR block cannot be modified after the subnet has been created.'

7.1.4 ¿Cómo configuro un bloque CIDR de contenedores para un clúster de CCE?

Inicie sesión en la consola de CCE y configure **Container CIDR Block** al crear un clúster.

Los bloques CIDR de contenedores disponibles son 10.0.0.0/8-18, 172.16.0.0/16-18 y 192.168.0.0/16-18.

Para agregar un bloque CIDR contenedor después de crear un clúster, vaya a la página de información del clúster y haga clic en **Add Container CIDR Block**.

AVISO

- Actualmente, los bloques CIDR de contenedor no se pueden agregar a los clústeres que utilizan la red de túneles de contenedor.
- El bloque CIDR de contenedor agregado no se puede eliminar.
- El bloque CIDR de servicio predeterminado es 10.247.0.0/16. Por lo tanto, el bloque CIDR del contenedor no puede ser 10.247.0.0/16.

The screenshot shows the configuration page for a CCE cluster named 'cce-test'. The left sidebar contains navigation options: Cluster Information, Resources (Nodes, Workloads, Networking, Storage, ConfigMaps and Secrets, Custom Resources, Namespaces), and O&M (Node Scaling, Workload Scaling, Add-ons, Charts, Cluster Upgrade, Logging, Container Intelligent Analysis). The main content area is divided into two sections: Basic Info and Networking Configuration.

Basic Info	
Name	cce-test
Cluster ID	[Redacted]
Type	CCE cluster
Cluster Version	v1.23
Patch Version	v1.23.5-r0
Status	Running
Cluster Scale	Nodes: 50
Created	Jan 29, 2023 14:35:38 GMT+08:00
Enterprise Project	default

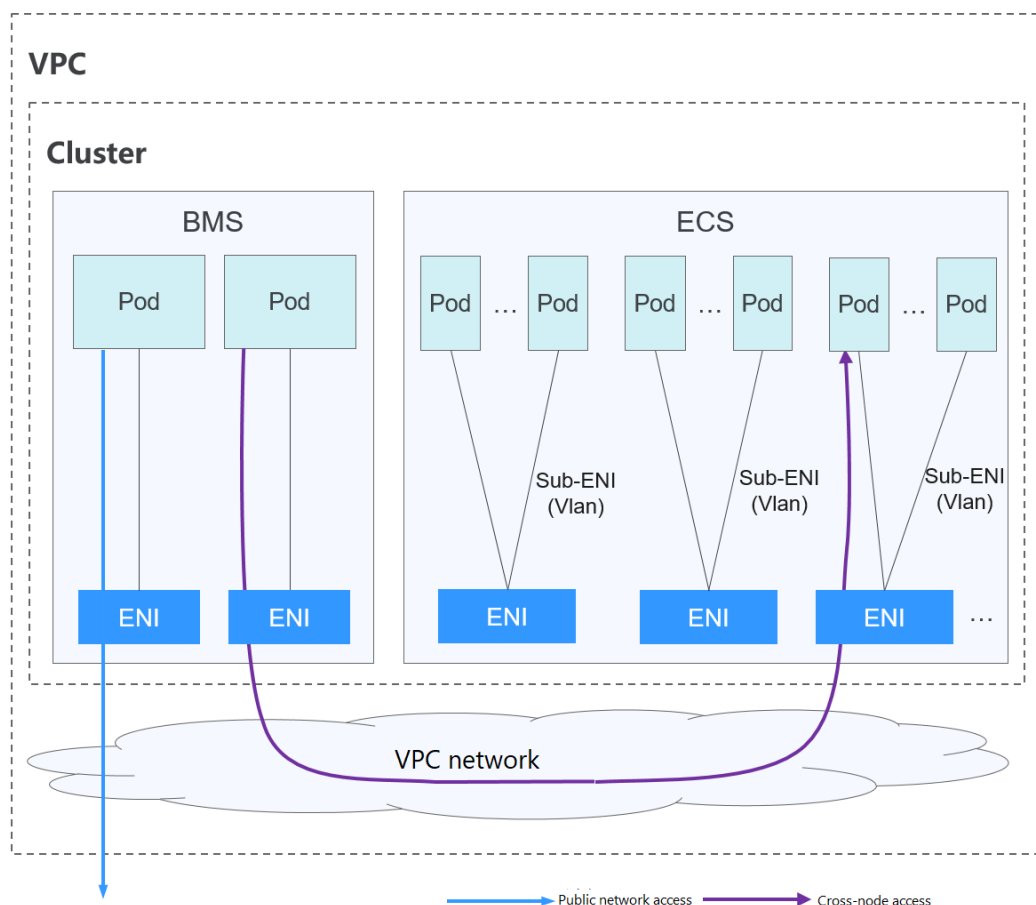
Networking Configuration	
Network Model	VPC network
VPC	vpc-cce
Subnet	subnet-cce
Container CIDR Block	10.0.0.0/16
	Add Container CIDR Block
Service CIDR Block	10.247.0.0/16
Forwarding	iptables
Default Node Security Group	cce-test-cce-node-hd6nf

7.1.5 ¿Cuándo debo usar la red nativa en la nube 2.0?

Cloud Native Network 2.0

Cloud Native Network 2.0 es una nueva solución de red de contenedor. Este modelo de red integra profundamente las interfaces de red elásticas nativas (ENI) de la VPC, utiliza el bloque CIDR de la VPC para asignar direcciones de contenedores y admite la transferencia de redes a contenedores con un balanceador de carga.

Figura 7-4 Cloud Native Network 2.0



Notes and Constraints

This network model is available only to CCE Turbo clusters.

Application Scenarios

- High performance requirements and use of other VPC network capabilities: Cloud Native Network 2.0 directly uses VPC, which delivers almost the same performance as the VPC network. Therefore, it is applicable to scenarios that have high requirements on bandwidth and latency, such as online live broadcast and e-commerce seckill.
- Large-scale networking: Cloud Native Network 2.0 supports a maximum of 2000 ECS nodes and 100,000 containers.

7.1.6 ¿Qué es la ENI?

Una interfaz de red elástica (ENI) es una tarjeta de red virtual. Puede crear y configurar las ENI y adjuntarlas a sus instancias de servidor en la nube (los ECS y BMS) para crear las redes flexibles y de alta disponibilidad.

Tipos de ENI

- Una interfaz de red principal se crea junto con una instancia de ECS de forma predeterminada, que no se puede separar de su ECS.

- Se puede crear y conectar una interfaz de red de extensión a un ECS, y se puede separar del ECS. El número de interfaces de red de extensión que puede conectar a un ECS varía según la variante de ECS.

Escenarios de aplicación

- Migración flexible

Puede desvincular una ENI de una instancia de servidor en la nube y, a continuación, adjuntarla a otra instancia. La ENI conserva su dirección IP privada, EIP y las reglas de grupo de seguridad. De esta manera, el tráfico de servicio en la instancia defectuosa se puede migrar rápidamente a la instancia en espera, implementando la recuperación de servicio rápida.

- Gestión independiente del tráfico

Puede adjuntar varias ENI que pertenecen a diferentes subredes en una VPC a la misma instancia y especificarlos para transportar el tráfico de red privada, el tráfico de red pública y el tráfico de red de gestión de la instancia, respectivamente. Puede configurar políticas de control de acceso y políticas de enrutamiento para cada subred y configurar reglas de grupo de seguridad para cada ENI para aislar las redes y el tráfico de servicio.

Restricciones

- Una instancia y sus interfaces de red de extensión deben estar en las mismas AZ, VPC y subred. Sin embargo, pueden pertenecer a diferentes grupos de seguridad.
- No se puede separar una interfaz de red principal de su ECS.
- El número de interfaces de red de extensión que puede conectar a un ECS varía según la variante de ECS.

7.1.7 Configuración de reglas de grupo de seguridad de clúster

CCE es una plataforma de contenedores universal. Sus reglas de grupo de seguridad predeterminadas se aplican a escenarios comunes. Cuando se crea un clúster, se crea automáticamente un grupo de seguridad para el nodo principal y el nodo de trabajo, por separado. El nombre del grupo de seguridad del nodo principal es **{Cluster name}-cce-control-{Random ID}** y el nombre del grupo de seguridad del nodo de trabajo es **{Cluster name}-cce-node-{Random ID}**. Si se utiliza un clúster de CCE Turbo, se crea un grupo de seguridad ENI adicional denominado **{Cluster name}-cce-eni-{Random ID}**.

Inicie sesión en la consola de gestión, seleccione **Service List > Networking > Virtual Private Cloud**. En la Consola de red, elija **Access Control > Security Groups**, busque la regla de grupo de seguridad del clúster de CCE y modifique y refuerce la regla de grupo de seguridad.

Si necesita especificar un grupo de seguridad de nodo al crear un clúster, active el puerto especificado haciendo referencia al [Reglas de grupo de seguridad para nodos de trabajo](#) creado automáticamente por el clúster para garantizar la comunicación de red normal en el clúster.

AVISO

La modificación o eliminación de reglas de grupo de seguridad puede afectar a la ejecución del clúster. Tenga cuidado al realizar esta operación. Si necesita modificar las reglas del grupo de seguridad, no modifique las reglas del puerto del que depende la ejecución de CCE.

Reglas de grupo de seguridad para nodos de trabajo

Entrada

El nombre del grupo de seguridad del nodo de trabajo creado automáticamente es **{Cluster name}-cce-node-{Random ID}**. En la siguiente figura se muestra la regla de entrada predeterminada. Se debe permitir el tráfico de todas las direcciones IP de origen definidas en el grupo de seguridad. Para obtener más información sobre los puertos, consulte [Tabla 7-1](#).

Figura 7-5 Grupo de seguridad predeterminado del nodo de trabajo en el modelo de red de VPC

Priority	Action	Protocol & Port	Type	Source	Description
1	Allow	UDP: All	IPv4	192.168.0.0/16	--
1	Allow	TCP: All	IPv4	192.168.0.0/16	--
1	Allow	ICMP: All	IPv4	test-vpc-cce-control-4hb4f	--
1	Allow	UDP: 30000-32767	IPv4	0.0.0.0	--
1	Allow	TCP: 30000-32767	IPv4	0.0.0.0	--
1	Allow	All	IPv4	10.0.0.0/16	--
1	Allow	All	IPv4	test-vpc-cce-node-4hb4f	--
1	Allow	TCP: 22	IPv4	0.0.0.0	Permit default Linux SSH port.

Tabla 7-1 Puertos predeterminados en el grupo de seguridad del nodo de trabajo en el modelo de red de VPC

Puerto	Dirección de origen predeterminada	Descripción	Modificable	Sugerencia de modificación
UDP: todos TCP: todos	Bloque CIDR de VPC	Se utiliza para el acceso mutuo entre nodos de trabajo y entre un nodo de trabajo y un nodo principal.	No	N/A
ICMP: todos	Bloque CIDR del nodo maestro	Se utiliza para que el nodo principal acceda a los nodos de trabajo.	No	N/A
TCP: 30000-32767 UDP: 30000-32767	Todas las direcciones IP	Intervalo de puertos de acceso predeterminado del NodePort Service en el clúster.	Sí	Estos puertos deben permitir solicitudes de VPC, contenedor y bloques de CIDR de ELB.

Puerto	Dirección de origen predeterminada	Descripción	Modificable	Sugerencia de modificación
Todos	Bloque CIDR de contenedores	Se utiliza para el acceso mutuo entre nodos y contenedores.	No	N/A
Todos	Bloque CIDR de nodo de trabajo	Se utiliza para el acceso mutuo entre nodos de trabajo.	No	N/A
TCP: 22	Todas las direcciones IP	Puerto que permite el acceso remoto a los ECS de Linux mediante SSH.	Recomendado	N/A

Figura 7-6 Grupo de seguridad predeterminado del nodo de trabajo en el modelo de red de túnel

Priority	Action	Protocol & Port	Type	Source	Description
1	Allow	UDP: All	IPv4	192.168.0.0/16	--
1	Allow	TCP: All	IPv4	192.168.0.0/16	--
1	Allow	ICMP: All	IPv4	test-vpc-cc-control-4hb4f	--
1	Allow	UDP: 30000-32767	IPv4	0.0.0.0	--
1	Allow	TCP: 30000-32767	IPv4	0.0.0.0	--
1	Allow	All	IPv4	10.0.0.0/16	--
1	Allow	All	IPv4	test-vpc-cc-node-4hb4f	--
1	Allow	TCP: 22	IPv4	0.0.0.0	Permit default Linux SSH port.

Tabla 7-2 Puertos predeterminados en el grupo de seguridad del nodo de trabajo en el modelo de red de túnel

Puerto	Dirección de origen predeterminada	Descripción	Modificable	Sugerencia de modificación
UDP: 4789	Todas las direcciones IP	Se utiliza para el acceso a la red entre contenedores.	No	N/A

Puerto	Dirección de origen predeterminada	Descripción	Modificable	Sugerencia de modificación
TCP: 10250	Bloque CIDR del nodo maestro	Utilizado por el nodo principal para acceder proactivamente a kubelet del nodo (por ejemplo, ejecutando kubectl exec {pod}).	No	N/A
TCP: 30000-32767 UDP: 30000-32767	Todas las direcciones IP	Intervalo de puertos de acceso predeterminado del NodePort Service en el clúster.	Sí	Estos puertos deben permitir solicitudes de VPC, contenedor y bloques de CIDR de ELB.
TCP: 22	Todas las direcciones IP	Puerto que permite el acceso remoto a los ECS de Linux mediante SSH.	Recomendado	N/A
Todos	Grupo de seguridad actual y bloque CIDR de VPC	Se debe permitir el tráfico de las direcciones IP de origen definidas en el grupo de seguridad y el bloque CIDR de VPC.	No	N/A

Salida

De forma predeterminada, todos los grupos de seguridad creados por CCE permiten todo el tráfico **outbound**. Se recomienda conservar la configuración. Si necesita reforzar las reglas salientes, asegúrese de que los siguientes puertos estén habilitados:

Tabla 7-3 Configuraciones mínimas de reglas de grupo de seguridad saliente para un nodo de trabajo

Puerto	CIDR permitido	Descripción
UDP: 53	Servidor DNS de subred	Se utiliza para la resolución de nombres de dominio.
UDP: 4789 (solo se requiere para clústeres que utilizan el modelo de red de túnel de contenedor)	Todas las direcciones IP	Se utiliza para el acceso a la red entre contenedores.
TCP: 5443	Bloque CIDR del nodo maestro	Puerto en el que escucha kube-apiserver del nodo principal.

Puerto	CIDR permitido	Descripción
TCP: 5444	Bloque de CIDR de VPC y bloque de CIDR de contenedor	Puerto de servicio de kube-apiserver, que proporciona gestión del ciclo de vida de los recursos de Kubernetes.
TCP: 6443	Bloque CIDR del nodo maestro	-
TCP: 8445	Bloque CIDR de VPC	Utilizado por el complemento de almacenamiento de un nodo de trabajo para acceder al nodo principal.
TCP: 9443	Bloque CIDR de VPC	Utilizado por el complemento de red de un nodo de trabajo para acceder al nodo principal.

Reglas del grupo de seguridad ENI

Se creará un grupo de seguridad llamado **{Cluster name}-cce-eni-{Random ID}** para el clúster de CCE Turbo. En la siguiente figura se muestra la regla de entrada predeterminada. Para obtener más información sobre los puertos, consulte [Tabla 7-4](#).

Priority	Action	Protocol & Port	Type	Source	Description
1	Allow	All	IPv4	192.168.0.0/16	--
1	Allow	All	IPv6	cluster-cce-eni-1wxu8	--

Tabla 7-4 Puertos predeterminados del grupo de seguridad ENI

Puerto	Dirección de origen predeterminada	Descripción	Modificable	Sugerencia de modificación
Todos	Grupo de seguridad actual y bloque CIDR de VPC	Se debe permitir el tráfico de las direcciones IP de origen definidas en el grupo de seguridad y el bloque CIDR de VPC.	No	N/A

Reglas del grupo de seguridad del nodo principal

El nombre del grupo de seguridad del nodo principal es **{Cluster name}-cce-control-{Random ID}**. En la siguiente figura se muestra la regla de entrada predeterminada. Se deben permitir todas las direcciones IP de origen definidas en el grupo de seguridad. Para obtener más información sobre los puertos, consulte [Tabla 7-5](#).

Figura 7-7 Reglas de grupo de seguridad para el nodo principal

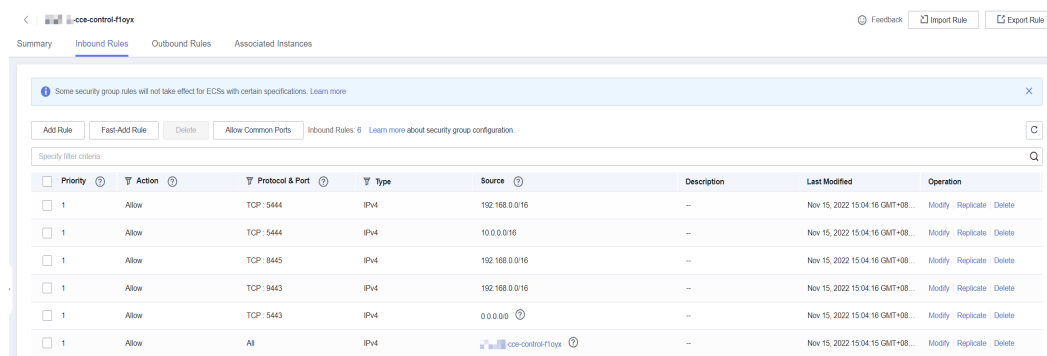


Tabla 7-5 Puertos predeterminados en el grupo de seguridad del nodo principal

Puerto	Dirección de origen predeterminada	Descripción	Modificable	Sugerencia de modificación
TCP: 5444	Bloque de CIDR de VPC y bloque de CIDR de contenedor	Puerto de servicio de kube-apiserver, que proporciona gestión del ciclo de vida de los recursos de Kubernetes.	No	N/A
UDP: 4789 (solo se requiere para clústeres que utilizan el modelo de red de túnel de contenedor)	Todas las direcciones IP	Se utiliza para el acceso a la red entre contenedores.	No	N/A
TCP: 9443	Bloque CIDR de VPC	Utilizado por el complemento de red de un nodo de trabajo para acceder al nodo principal.	No	N/A
TCP: 5443	Todas las direcciones IP	Puerto al que escucha kube-apiserver del nodo principal.	Sí	Los dos puertos deben permitir solicitudes de VPC y de bloques CIDR de contenedor y el bloque CIDR de plano de control de la malla de servicio alojada.

Puerto	Dirección de origen predeterminada	Descripción	Modificable	Sugerencia de modificación
TCP: 8445	Bloque CIDR de VPC	Utilizado por el complemento de almacenamiento de un nodo de trabajo para acceder al nodo principal.	No	N/A
Todos	Grupo de seguridad actual y bloque CIDR de VPC	Se debe permitir el tráfico de las direcciones IP de origen definidas en el grupo de seguridad y el bloque CIDR de VPC.	No	N/A

7.1.8 ¿Cómo configuro un bloque CIDR de servicio IPv6?

Contexto

Para crear un clúster de CCE Turbo de doble pila IPv4/IPv6, debe establecer un bloque CIDR de Service IPv6. El bloque CIDR predeterminado es **fc00::/112** que contiene 65536 direcciones IPv6. Si necesita personalizar un bloque CIDR de Service, puede consultar esta sección.

IPv6

Dirección IPv6

Una dirección IPv6 es una cadena binaria de 128 bits, cuatro veces la longitud de una dirección IPv4. La dirección IPv4 decimal se sustituye por la dirección IPv6 hexadecimal. La cadena se divide en ocho grupos, es decir, cada grupo contiene 16 bits. Estos grupos se separan con colones (:). Cada grupo consta de un número hexadecimal de cuatro dígitos (insensible a mayúsculas y minúsculas). Se admite un total de 32 dígitos hexadecimales.

Una dirección IPv6 se puede omitir de las siguientes maneras:

- Omisión de 0s principales: 0s se puede omitir si el grupo de colon comienza con 0s. Las siguientes direcciones IPv6 son las mismas.
 - ff01:0d28:03ee:0000:0000:0000:0000:0c23
 - ff01:d28:3ee:0000:0000:0000:0000:c23
 - ff01:d28:3ee:0:0:0:0:c23
- Omisión de hexetets de todos los-0s: Puede usar un (::) de dos puntos para representar una sola cadena contigua de segmentos de todos-0s. Un doble colon (::) solo se puede usar una vez.

Ejemplo:

Antes de la omisión	Después de la omisión
ff01:d28:3ee:0:0:0:c23	ff01:d28:3ee::c23
0:0:0:0:0:0:1	::1
0:0:0:0:0:0:0	::

Segmento de dirección IPv6

Un segmento de dirección IPv6 se expresa generalmente en formato de Classless Inter-Domain Routing (CIDR). Por lo general, se representa por una barra diagonal (/) seguida de un número, es decir, *IPv6 address/Prefix length*. La función del prefijo es similar a la de la máscara del segmento de dirección IPv4. El número de bits binarios ocupados por la parte de red representa los bits binarios ocupados por la parte de red. Una dirección IPv6 consiste en la parte de red y la parte de host. El prefijo especifica el número de bits ocupados por la parte de red, y los bits restantes son la parte de host.

Por ejemplo, el **fc00:d28::/32** indica un segmento de dirección IPv6 con un prefijo de 32 bits. Los primeros 32 bits (**fc00:d28** en modo binario) son la parte de red y los últimos 96 bits son la parte de anfitrión disponible.

Restricciones en bloques CIDR de Service IPv6

Al establecer el bloque CIDR del servicio de clúster, tenga en cuenta las siguientes restricciones:

- El bloque CIDR del Service IPv6 debe pertenecer al bloque CIDR **fc00::/8**. La dirección es una dirección local única (ULA). La ULA tiene un prefijo fijo **fc00::/7** que incluye **fc00::/8** y **fd00::/8**. Los dos rangos son similares a las direcciones de red IPv4 dedicadas **10.0.0.0/8**, **172.16.0.0/12** y **192.168.0.0/16**. Son equivalentes a bloques CIDR privados y solo se pueden usar en la red local.
- El prefijo varía de 112 a 120. Puede ajustar el número de direcciones ajustando el valor del prefijo. El número máximo de direcciones es 65536.

Ejemplo de un bloque CIDR de Service IPv6

De acuerdo con las restricciones, esta sección proporciona un ejemplo de configuración de un bloque CIDR IPv6 que contiene 8192 direcciones como referencia.

Paso 1 Establezca la longitud del prefijo en función del número de direcciones. La longitud del prefijo varía de 112 a 120.

En este ejemplo, se requieren 8192 direcciones, que están representadas por dígitos binarios de 13 bits. Por lo tanto, la longitud del prefijo es 115 (128 - 13).

Paso 2 Establezca la dirección de red IPv6, que debe pertenecer al bloque CIDR **fc00::/8**.

En este ejemplo, la longitud del prefijo es 115. Debido a que la dirección de red debe pertenecer al bloque CIDR **fc00::/8**, los primeros dígitos binarios de 8 bits son fijos. La dirección de red que puede modificarse varía desde el noveno bit hasta el 115 bit. El 116 bit al 128 bit es la parte de host.

Si la dirección IPv6 se escribe en formato binario, la siguiente información en negrita no se puede modificar cuando la longitud del prefijo es 115.

```
Binary: 1111 1100 **** **** ... ****0 0000 0000 0000/115
        |   |   |   |   |   |   |   |   |
Hexadecimal: f   c   x   x ... y   0   0   0/115
```

x es un dígito hexadecimal, y y puede ser 0, 2, 4, 6, 8, a, c o e.

---Fin

7.2 Network Fault

7.2.1 ¿Cómo se localiza una falla de red de carga de trabajo?

Proceso de solución de problemas

Los métodos de resolución de problemas se ordenan en función de la probabilidad de ocurrencia de las posibles causas. Se recomienda comprobar las posibles causas de alta probabilidad a baja probabilidad para localizar rápidamente la causa del problema.

Si la falla persiste después de rectificar una posible causa, compruebe otras posibles causas.

- **Concepto de comprobación 1: Contenedores y Puertos de Contenedores**
- **Concepto de comprobación 2: Dirección IP del nodo y puerto del nodo**
- **Concepto de comprobación 3: Dirección IP y puerto ELB**
- **Concepto de comprobación 4: Gateway de NAT + Puerto**
- **Concepto de comprobación 5: Si el grupo de seguridad del nodo donde se encuentra el contenedor permite el acceso**

Concepto de comprobación 1: Contenedores y Puertos de Contenedores

Inicie sesión en la consola de CCE o use `kubectl` para consultar la dirección IP del pod. A continuación, inicie sesión en el nodo o contenedor del clúster y ejecute el comando `curl` para invocar manualmente a la API. Compruebe si se devuelve el resultado esperado.

Si no se puede acceder a la dirección IP de `<container>:<port>`, se recomienda iniciar sesión en el contenedor de la aplicación y acceder a `<127.0.0.1>:<port>` para localizar el error.

Problemas comunes:

1. El puerto del contenedor está configurado incorrectamente (el contenedor no escucha el puerto de acceso).
2. El URL no existe (no existe ninguna ruta relacionada en el contenedor).
3. Se produce una excepción de servicio (un error de servicio en el contenedor).
4. Compruebe si el componente del núcleo de red del clúster es anormal (modelo de red de túnel de contenedor: componente de núcleo openwitch; modelo de red VPC: componente de núcleo ipvlan).

Concepto de comprobación 2: Dirección IP del nodo y puerto del nodo

Solo se puede acceder a los servicios NodePort o LoadBalancer mediante la dirección IP del nodo y el puerto del nodo.

- **NodePort Services:**

El puerto de acceso de un nodo es el puerto expuesto externamente por el nodo.

- **LoadBalancer Service:**

Puede ver el puerto de nodo de un servicio de LoadBalancer editando el archivo YAML.

Ejemplo:

nodePort: 30637 indica el puerto del nodo expuesto. **targetPort: 80** indica el puerto del pod expuesto. **port: 123** es el puerto de servicio expuesto. LoadBalancer Services también utilizan este puerto para configurar el oyente de ELB.

```
spec:
  ports:
    - name: cce-service-0
      protocol: TCP
      port: 123
      targetPort: 80
      nodePort: 30637
```

Después de encontrar el puerto de nodo (nodePort), acceda a <IP address>:<port> del nodo donde se encuentra el contenedor y compruebe si se devuelve el resultado esperado.

Problemas comunes:

1. El puerto de servicio no está permitido en las reglas entrantes del nodo.
2. Una ruta personalizada está configurada incorrectamente para el nodo.
3. La etiqueta del pod no coincide con la del Service (creado mediante kubectl o API).

Concepto de comprobación 3: Dirección IP y puerto ELB

Hay varias causas posibles si no se puede acceder a <IP address>:<port> del ELB, pero se puede acceder a <IP address>:<port> del nodo.

Causas posibles:

- El grupo de servidores backend del puerto o URL no cumple con las expectativas.
- El grupo de seguridad del nodo no ha expuesto el protocolo o puerto relacionado al ELB.
- La comprobación de estado del equilibrio de carga de capa 4 no está habilitada.
- El certificado utilizado para los servicios de equilibrio de carga de capa 7 ha caducado.

Problemas comunes:

1. Al exponer un balanceador de carga ELB de capa 4, si no ha habilitado la comprobación de estado en la consola, el balanceador de carga puede enrutar solicitudes a nodos anormales.
2. Para el acceso UDP, el puerto ICMP del nodo no se ha permitido en las reglas entrantes.
3. La etiqueta del pod no coincide con la del Service (creado mediante kubectl o API).

Concepto de comprobación 4: Gateway de NAT + Puerto

Generalmente, no se configura ninguna EIP para el servidor backend de NAT. De lo contrario, pueden producirse excepciones tales como pérdida de paquetes de red.

Concepto de comprobación 5: Si el grupo de seguridad del nodo donde se encuentra el contenedor permite el acceso

Inicie sesión en la consola de gestión, seleccione **Service List > Networking > Virtual Private Cloud**. En la Consola de red, elija **Access Control > Security Groups**, busque la regla de grupo de seguridad del clúster de CCE y modifique y refuerce la regla de grupo de seguridad.

- Clúster de CCE:

El nombre del grupo de seguridad del nodo es **{Cluster name}-cce-node-{Random characters}**.

- Clúster de CCE Turbo:

El nombre del grupo de seguridad del nodo es **{Cluster name}-cce-node-{Random characters}**.

El nombre del grupo de seguridad asociado a los contenedores es **{Cluster name}-cce-eni-{Random characters}**.

Comprobar los siguientes:

- Dirección IP, puerto y protocolo de una solicitud externa para acceder a las cargas de trabajo del clúster. Se deben permitir en la regla de entrada del grupo de seguridad del clúster.
- Dirección IP, puerto y protocolo de una solicitud de una carga de trabajo para visitar aplicaciones externas fuera del clúster. Se deben permitir en la regla de salida del grupo de seguridad del clúster.

Para obtener más información acerca de la configuración del grupo de seguridad, consulte [Configuración de reglas de grupo de seguridad de clúster](#).

7.2.2 ¿Por qué no se puede utilizar la dirección ELB para acceder a las cargas de trabajo en un clúster?

Síntoma

En un clúster (en un nodo o en un contenedor), la dirección ELB no se puede utilizar para acceder a cargas de trabajo.

Causa posible

If the service affinity of a LoadBalancer Service is set to the node level, that is, the value of **externalTrafficPolicy** is **Local**, the ELB address may fail to be accessed from the cluster (specifically, nodes or containers).

This is because when the LoadBalancer service is created, kube-proxy adds the ELB access address (external-ip) to iptables or IPVS. When the ELB address is accessed from the cluster, the ELB load balancer is not used. Instead, kube-proxy directly forwards the access request. The case depends on which container network model and service forwarding mode you use.

When **externalTrafficPolicy** is set to **Local**, the access may fail in the following scenarios:

Server	Client	Tunnel Network Cluster (IPVS)	VPC Network Cluster (IPVS)	Tunnel Network Cluster (iptables)	VPC Network Cluster (iptables)
NodePort Service	Same node	OK. The node where the pod runs is accessible, not any other nodes.	OK. The node where the pod runs is accessible.	OK. The node where the pod runs is accessible.	OK. The node where the pod runs is accessible.
	Cross-node	OK. The node where the pod runs is accessible, not any other nodes.	OK. The node where the pod runs is accessible.	OK. The node where the pod runs is accessible by visiting the node IP + port, not by any other ways.	OK. The node where the pod runs is accessible by visiting the node IP + port, not by any other ways.
	Containers on the same node	OK. The node where the pod runs is accessible, not any other nodes.	OK. The node where the pod runs is not accessible.	OK. The node where the pod runs is accessible.	OK. The node where the pod runs is not accessible.
	Containers across nodes	OK. The node where the pod runs is accessible, not any other nodes.	OK. The node where the pod runs is accessible.	OK. The node where the pod runs is accessible.	OK. The node where the pod runs is accessible.
LoadBalancer Service using a dedicated load balancer	Same node	Accessible for public networks, not private networks.	Accessible for public networks, not private networks.	Accessible for public networks, not private networks.	Accessible for public networks, not private networks.
	Containers on the same node	Accessible for public networks, not private networks.	Accessible for public networks, not private networks.	Accessible for public networks, not private networks.	Accessible for public networks, not private networks.

Local Service of the nginx-ingress add-on using a dedicated load balancer	Same node	Accessible for public networks, not private networks.	Accessible for public networks, not private networks.	Accessible for public networks, not private networks.	Accessible for public networks, not private networks.
	Containers on the same node	Accessible for public networks, not private networks.	Accessible for public networks, not private networks.	Accessible for public networks, not private networks.	Accessible for public networks, not private networks.

Solución

Se pueden utilizar los siguientes métodos para resolver este problema:

- **(Recomendado)** En el clúster, utilice el nombre de dominio de servicio o servicio de ClusterIP para el acceso.
- Establezca **externalTrafficPolicy** del servicio en **Cluster** es decir, la afinidad de servicio a nivel de clúster. Tenga en cuenta que esto afecta a la persistencia de la dirección de origen.

```
apiVersion: v1
kind: Service
metadata:
  annotations:
    kubernetes.io/elb.class: union
    kubernetes.io/elb.autocreate: '{"type":"public","bandwidth_name":"cce-bandwidth","bandwidth_chargemode":"traffic","bandwidth_size":5,"bandwidth_sharetype":"PER","eip_type":"5_bgp","name":"james"}'
  labels:
    app: nginx
    name: nginx
spec:
  externalTrafficPolicy: Cluster
  ports:
  - name: service0
    port: 80
    protocol: TCP
    targetPort: 80
  selector:
    app: nginx
  type: LoadBalancer
```

- Aprovechando la función de paso a través del Servicio, kube-proxy se omite cuando se utiliza la dirección de ELB para acceder. Primero se accede al balanceador de carga de ELB y, a continuación, a la carga de trabajo.

NOTA

- Después de configurar las redes de paso a través para un balanceador de carga dedicado, no se puede acceder a contenedores en el nodo donde se ejecuta la carga de trabajo a través del Service.
- Las redes de paso a través no son compatibles con clústeres de v1.15 o anteriores.
- En el modo de red IPVS, la configuración de paso a través del Service conectado al mismo ELB debe ser la misma.

```
apiVersion: v1
kind: Service
metadata:
```

```
annotations:
  kubernetes.io/elb.pass-through: "true"
  kubernetes.io/elb.class: union
  kubernetes.io/elb.autocreate: '{"type":"public","bandwidth_name":"cce-
bandwidth","bandwidth_chargemode":"traffic","bandwidth_size":
5,"bandwidth_sharetype":"PER","eip_type":"5_bgp","name":"james"}'
labels:
  app: nginx
  name: nginx
spec:
  externalTrafficPolicy: Local
  ports:
  - name: service0
    port: 80
    protocol: TCP
    targetPort: 80
  selector:
    app: nginx
  type: LoadBalancer
```

7.2.3 ¿Por qué no se puede acceder al ingreso fuera del clúster?

Ingresa solicitudes de reenvío basadas en los protocolos HTTP y HTTPS de capa 7. Como entrada del tráfico de clúster, las entradas usan nombres de dominio y rutas para lograr detalles más finos. Después de agregar una entrada a un clúster, es posible que no se obtenga acceso al clúster. Esta sección describe cómo localizar el error cuando un ingreso no se agrega o no se puede acceder a él. Antes de rectificar los problemas de ingreso, lea las siguientes precauciones y realice una autocomprobación:

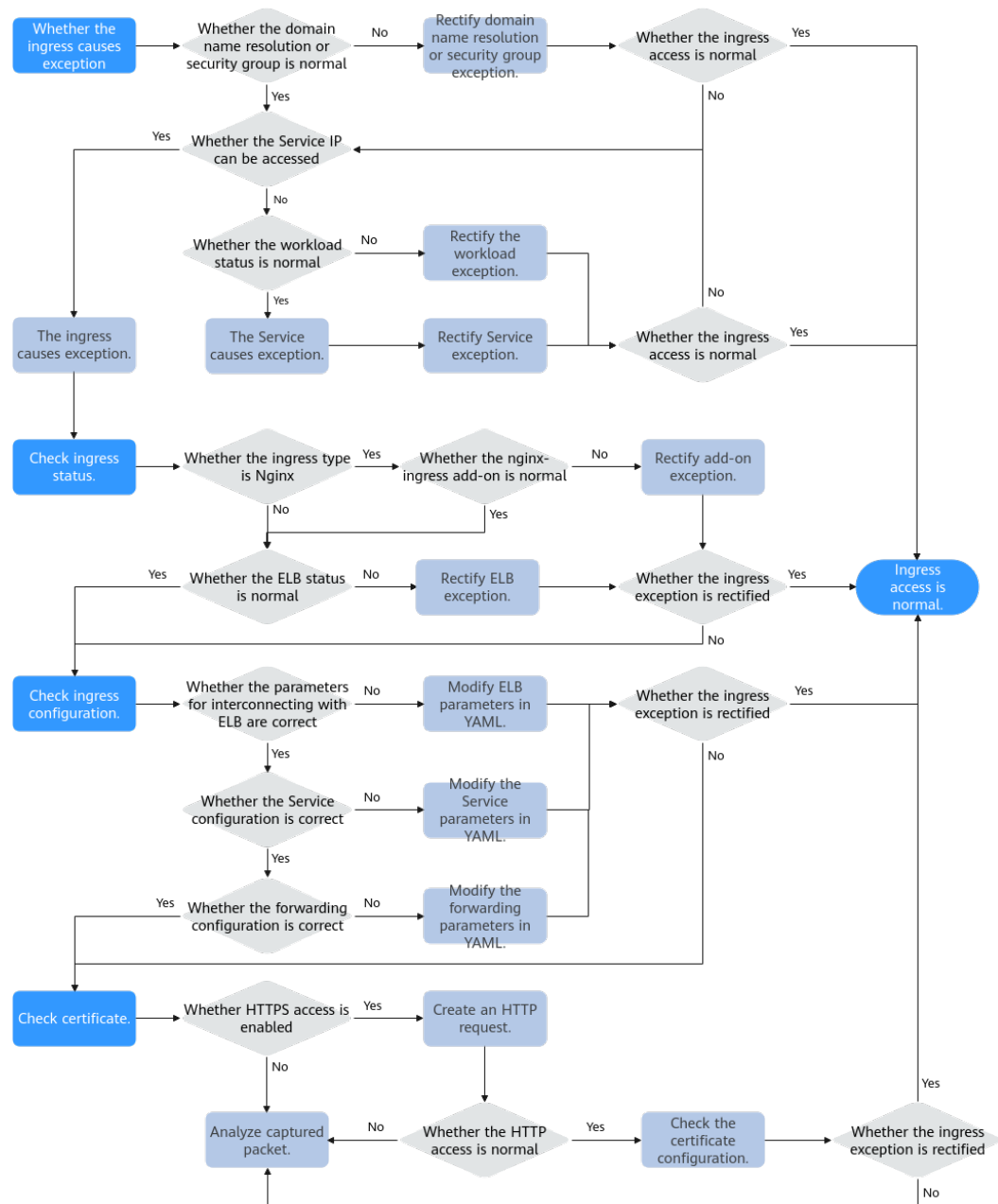
AVISO

- Si la dirección de host se especifica en la entrada, la dirección IP no se puede utilizar para el acceso.
 - Compruebe el grupo de seguridad de nodo del clúster y asegúrese de que los puertos de servicio en el rango de 30000 a 32767 son accesibles para todos los segmentos de red para el tráfico entrante.
-

Proceso de solución de problemas

Esta sección proporciona una descripción general de la solución de problemas de las excepciones de acceso externo de ingreso, como se muestra en [Figura 7-8](#).

Figura 7-8 Descripción de la solución de problemas de las excepciones de acceso externo de ingreso



1. **Compruebe si la excepción es causada por el ingreso.**

Compruebe si el problema es causado por la entrada. Asegúrese de que la resolución del nombre de dominio externo sea normal, que las reglas del grupo de seguridad sean correctas y que el servicio y la carga de trabajo correspondientes a la entrada funcionen correctamente.

2. **Comprobación del estado de ingreso.**

Cuando el servicio y la carga de trabajo son normales, asegúrese de que el balanceador de carga del que depende la entrada es normal. Si la entrada es del tipo Nginx, asegúrese de que el complemento nginx-ingress es normal.

3. **Compruebe si el ingreso está configurado correctamente.**

Si los resultados de la comprobación anterior son normales, la configuración de ingreso puede ser incorrecta.

- Compruebe si los parámetros de interconexión con el balanceador de carga son correctos.
- Compruebe si la configuración del servicio es correcta.
- Compruebe si la configuración de reenvío es correcta.

4. **Comprobación del certificado.**

Si el acceso HTTPS está habilitado en el ingreso, también debe comprobar si el error está causado por una configuración incorrecta del certificado. Puede utilizar el mismo balanceador de carga para crear una entrada HTTP. Si el acceso es normal, el certificado HTTPS puede ser defectuoso.

5. Si el error persiste, capture los paquetes para su análisis o envíe un ticket de servicio para obtener ayuda.

Compruebe si la excepción es causada por el ingreso

Compruebe si la excepción de acceso es causada por el ingreso. Si se produce la excepción de resolución de nombre de dominio, error de regla de grupo de seguridad, excepción de servicio o excepción de carga de trabajo, el acceso de entrada puede fallar.

La siguiente secuencia de comprobación cumple con las reglas de exterior a interior:

Paso 1 Compruebe si la resolución del nombre de dominio o las reglas de grupo de seguridad son normales.

1. Ejecute el siguiente comando para comprobar si los conjuntos de registros del nombre de dominio tienen efecto en el servidor de DNS autoritativo:

```
nslookup -qt= Type Domain name Authoritative DNS address
```

2. Verifique las reglas de grupo de seguridad de los nodos de clúster y asegúrese de que los puertos de servicio en el rango 30000 - 32767 son accesibles para todos los segmentos de red para el tráfico entrante. Para obtener más información acerca de cómo reforzar el grupo de seguridad, consulte [Configuración de reglas de grupo de seguridad de clúster](#).

Priority	Action	Protocol & Port	Type	Source	Description	Last Modified	Operation
1	Allow	TCP: All	IPv4	192.168.0.0/16	-	Nov 15, 2022 15:04:16 GMT+08...	Modify Replicate Delete
1	Allow	TCP: 30000-32767	IPv4	0.0.0.0	-	Nov 15, 2022 15:04:16 GMT+08...	Modify Replicate Delete
1	Allow	UDP: 30000-32767	IPv4	0.0.0.0	-	Nov 15, 2022 15:04:16 GMT+08...	Modify Replicate Delete

Paso 2 Compruebe si el Service puede acceder a los servicios del contenedor.

Puede crear un pod en el clúster y utilizar la dirección IP del clúster para acceder al servicio. Si el tipo Service es NodePort, también puede usar **EIP:Port** para acceder al servicio a través de Internet.

1. Utilice kubectl para conectarse al clúster y consultar el servicio en el clúster.

```
# kubectl get svc
NAME          TYPE          CLUSTER-IP      EXTERNAL-IP      PORT(S)          AGE
kubernetes   ClusterIP     10.247.0.1      <none>           443/TCP         34m
nginx        ClusterIP     10.247.138.227 <none>           80/TCP          30m
```

2. Cree un pod e inicie sesión en el contenedor.

```
kubectl run -i --tty --image nginx:alpine test --rm /bin/sh
```

3. Ejecute el comando **curl** para acceder al **ClusterIP address:Port** del Service para comprobar si el Service del clúster es accesible.

```
curl 10.247.138.227:80
```

Si se puede acceder al Service, el estado de la carga de trabajo de backend es normal. Se puede determinar preliminarmente que la excepción es causada por la entrada. Para obtener más información, véase [Comprobación del estado de ingreso](#).

Si el acceso al Service es anormal, compruebe el estado de la carga de trabajo para determinar la causa.

Paso 3 Compruebe si el estado de la carga de trabajo es normal.

Si la carga de trabajo es normal pero no se puede acceder al Service, la excepción puede ser causada por el Service. Compruebe la configuración del Service. Por ejemplo, compruebe si el puerto de contenedor está configurado correctamente en un puerto de servicio abierto del contenedor.

Si la carga de trabajo es normal pero el resultado de acceso no es el esperado, compruebe el código de servicio que se ejecuta en el contenedor.

----Fin

Comprobación del estado de ingreso

CCE admite dos tipos de entradas. El Nginx Ingress Controller es proporcionado por la comunidad de código abierto y necesita ser mantenido mediante la instalación del complemento en el clúster. El controlador de ingreso ELB se ejecuta en el nodo principal y es mantenido por un equipo dedicado de Huawei Cloud.

Paso 1 Si utiliza una entrada de Nginx, debe instalar el complemento nginx-ingress en el clúster. Si utiliza una entrada de ELB, omita este paso.

Vaya a **Add-ons > Add-ons Installed** y compruebe si el complemento nginx-ingress se está ejecutando. Asegúrese de que los recursos de nodo sean suficientes en el clúster. Si no es así, la instancia del complemento no se puede programar.

Paso 2 Vaya a la consola de ELB para comprobar el estado del ELB.

- Entrada de ELB

El puerto de acceso se puede personalizar. Compruebe si el oyente y el grupo de servidores backend creados en el ELB no se eliminan o modifican.

Al crear una entrada de ELB, puede elegir **Auto Create** en la consola para crear automáticamente un balanceador de carga. No modifique el balanceador de carga. De lo contrario, pueden producirse excepciones de ingreso.

- Entrada de Nginx

Los puertos de acceso están fijados a 80 y 443. No se admiten los puertos personalizados. La instalación del complemento nginx-ingress ocupa ambos puertos 80 y 443. No los elimine. De lo contrario, debe volver a instalar el complemento.

También puede determinar si la falla es causada por el balanceador de carga basado en el código de error. Si se muestra el siguiente código de error, hay una alta probabilidad de que la falla es causada por el balanceador de carga. En este caso, debe prestar especial atención al balanceador de carga.

404 Not Found

ELB

---Fin

Compruebe si el ingreso está configurado correctamente

Si los elementos de comprobación anteriores son normales, compruebe si la excepción se debe a la configuración de los parámetros. Cuando se usa kubectl para crear una entrada, es necesario establecer un gran número de parámetros, lo que es propenso a errores. Se recomienda utilizar la consola para crear entradas y establecer parámetros según sea necesario para filtrar automáticamente balanceadores de carga y Service que no cumplan con los requisitos. Esto evita eficazmente los formatos incorrectos o la falta de parámetros clave.

Compruebe la configuración de ingreso de acuerdo con los siguientes pasos:

- **Compruebe si los parámetros de interconexión con el balanceador de carga son correctos.**

Los balanceadores de carga se definen mediante parámetros en el campo **annotations**. Kubernetes no verifica los parámetros del campo **annotations** al crear recursos. Si los parámetros clave son incorrectos o faltan, se puede crear una entrada, pero no se puede acceder a ella.

Con frecuencia se presentan los siguientes problemas:

- El balanceador de carga de ELB interconectado no está en la **misma VPC** como el clúster.
- Faltan los campos clave **kubernetes.io/elb.id**, **kubernetes.io/elb.ip**, **kubernetes.io/ingress.class** y **kubernetes.io/elb.port** de **annotations** cuando se agrega una entrada de ELB para conectarse a un balanceador de carga de ELB existente.
- Cuando se agrega una entrada Nginx, el complemento nginx-ingress no está instalado. Como resultado, la conexión de ELB no está disponible.
- Cuando se agrega una entrada Nginx, faltan los campos clave **kubernetes.io/ingress.class** y **kubernetes.io/elb.port** en **annotations**.
- Cuando se agrega una entrada de Nginx, el campo **kubernetes.io/elb.port** no admite los puertos personalizados. Si se utiliza HTTP, el valor se fija a **80**. Si se utiliza HTTPS, el valor se fija a **443**.
- **Compruebe si la configuración de Service es correcta.**
 - Compruebe si el tipo Service conectado a la entrada es correcto. Para obtener más información acerca de los tipos de servicio admitidos por el ingreso, consulte [Tabla 7-6](#).

Tabla 7-6 Tipos Service soportados por la entrada

Tipo de ingreso	Tipo de acceso	ClusterIP	NodePort
Entrada de ELB	Enrutamiento de balanceo de carga	No se admite	Se admite
	Enrutamiento de balanceo de carga ENI	Se admite	No se admite
Entrada de Nginx	Enrutamiento de balanceo de carga	Se admite	Se admite
	Enrutamiento de balanceo de carga ENI	Se admite	No se admite

- Compruebe si el número de puerto de acceso del Service es correcto. El número de puerto de acceso (campo **port**) del Service debe ser diferente del número de puerto de contenedor (campo **targetPort**).
- **Compruebe si la configuración de reenvío es correcta.**
 - La URL de reenvío agregada debe existir en la aplicación de backend. De lo contrario, el reenvío falla.

Por ejemplo, el URL de acceso predeterminado de la aplicación Nginx es **/usr/share/nginx/html**. Al agregar **/test** a la política de reenvío de ingreso, asegúrese de que su aplicación de Nginx contiene el mismo URL, es decir, **/usr/share/nginx/html/test**; de lo contrario, se devuelve 404.

 **NOTA**

Cuando utilice Nginx Ingress Controller, puede agregar el comentario **rewrite** al campo **annotations** para redireccionar y reescribir la ruta de acceso que no existe en el Service para evitar el error de que la ruta de acceso no existe. Para obtener más información, consulte [Reescritura](#).

- Si el nombre de dominio (host) se especifica cuando se crea una entrada, no se puede acceder a la entrada utilizando una dirección IP.

Comprobación del certificado

El tipo de certificado secreto de ingreso de CCE es **IngressTLS**. Si el tipo de certificado es incorrecto, el ingreso no puede crear un oyente en el balanceador de carga. Como resultado, el acceso de entrada se vuelve anormal.

Paso 1 Quite los parámetros HTTPS de YAML y cree un ingreso de HTTP para comprobar si se puede acceder al ingreso.

Si el acceso HTTP es normal, compruebe si el certificado secreto HTTPS es correcto.

Paso 2 Compruebe si el tipo secreto es correcto. Comprueba si el tipo secreto es **IngressTLS**.

```
# kubectl get secret
NAME          TYPE          DATA  AGE
ingress      IngressTLS    2      36m
```

Paso 3 Cree certificados de prueba para corregir el error del certificado.

```
# openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout tls.key -out
tls.crt -subj "/CN={YOUR_HOST}/O={YOUR_HOST}"
```

Paso 4 Utilice los certificados de prueba **tls.key** y **tls.crt** para crear un secreto del tipo IngressTLS y comprobar si se puede acceder al secreto normalmente.

El siguiente es un archivo YAML de ejemplo cuando se crea un secreto usando kubectl:

```
kind: Secret
apiVersion: v1
type: IngressTLS
metadata:
  name: ingress
  namespace: default
data:
  tls.crt: LS0tLS1CRU*****FURS0tLS0t
  tls.key: LS0tLS1CRU*****VZLS0tLS0=
```

NOTA

En la información anterior, las **tls.crt** y **tls.key** solo son ejemplos. Reemplácelos con los archivos reales. Los valores de **tls.crt** y **tls.key** son el contenido cifrado usando Base64.

----Fin

7.2.4 ¿Por qué el navegador devuelve el código de error 404 cuando accedo a una aplicación desplegada?

CCE no devuelve ningún código de error cuando no puede acceder a sus aplicaciones mediante un navegador. Revise sus servicios primero.

404 Not Found

Si se devuelve el código de error que se muestra en la siguiente figura, indica que el ELB no puede encontrar la política de reenvío correspondiente. Compruebe las políticas de reenvío.

Figura 7-9 404:ALB

404 Not Found

ALB

Si se devuelve el código de error que se muestra en la siguiente figura, indica que se producen errores en Nginx (sus servicios). En este caso, compruebe sus servicios.

Figura 7-10 404:nginx/1.**.*

404 Not Found

nginx/1.14.0

7.2.5 ¿Qué debo hacer si un contenedor no se conecta a Internet?

Si un contenedor no puede conectarse a Internet, compruebe si el nodo donde se encuentra el contenedor puede conectarse a Internet.

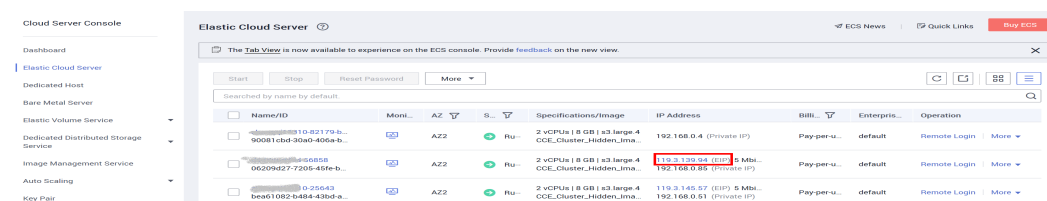
Concepto de comprobación 1: Si el nodo puede conectarse a Internet

Paso 1 Inicie sesión en la consola de ECS.

Paso 2 Compruebe si el ECS correspondiente al nodo se ha vinculado a una EIP o tiene un gateway de NAT configurado.

Una EIP ha sido unido, como se muestra en [Figura 7-11](#). Si no se muestra ninguna EIP, vincule una EIP al ECS.

Figura 7-11 Nodo con una EIP vinculada



----Fin

Concepto de comprobación 2: Si se ha configurado una ACL de red para el nodo

Paso 1 Inicie sesión en la consola de VPC.

Paso 2 En el panel de navegación de la izquierda, elija **Access Control > Network ACLs**.

Paso 3 Compruebe si se ha configurado una ACL de red para la subred donde se encuentra el nodo y si el acceso externo está restringido.

----Fin

7.2.6 ¿Qué puedo hacer si no se puede eliminar una subred de VPC?

Es posible que no se elimine una subred de VPC si ha utilizado la subred de VPC en el clúster de CCE. Por lo tanto, debe eliminar el clúster correspondiente en la consola de CCE antes de eliminar la subred de VPC.

AVISO

- Si elimina un clúster, se eliminarán todos los nodos, aplicaciones y servicios del clúster. Tenga cuidado al eliminar un clúster.
- No se recomienda eliminar nodos en un clúster de CCE en la página de ECS.

7.2.7 ¿Cómo puedo restaurar una NIC de contenedor defectuosa?

Si una NIC de contenedor está defectuosa, el contenedor se reinicia repetidamente y no puede proporcionar servicios para los sistemas externos. Para corregir la falla, realice los siguientes pasos:

Procedimiento

Paso 1 Ejecute el siguiente comando para eliminar el pod del contenedor defectuoso:

```
kubectl delete pod {podName} -n {podNamespace}
```

Donde,

- **{podName}**: Ingrese el nombre del pod del contenedor defectuoso.
- **{podNamespace}**: Ingrese el espacio de nombres donde se encuentra el pod.

Paso 2 Después de eliminar el pod del contenedor defectuoso, el sistema vuelve a crear automáticamente un pod para el contenedor. De esta manera, se restaura la NIC del contenedor.

----Fin

7.2.8 ¿Qué debo hacer si un nodo no se conecta a Internet (red pública)?

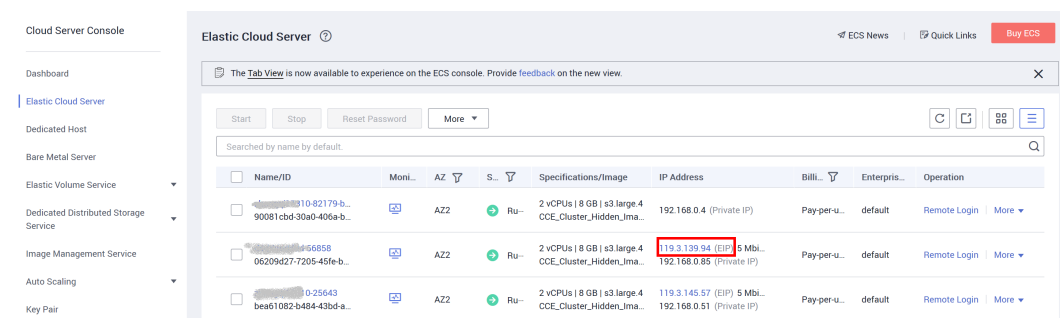
Si un nodo no se conecta a Internet, realice las siguientes operaciones:

Concepto de comprobación 1: Si una EIP ha sido vinculada al nodo

Inicie sesión en la consola de ECS y compruebe si una EIP ha sido vinculada al ECS correspondiente al nodo.

Como se muestra en la siguiente figura, si hay una dirección IP en la columna de dirección IP elástica, se ha enlazado una dirección IP elástica. Si no hay una dirección IP en esa columna, vincule una.

Figura 7-12 Nodo con una EIP vinculada



Concepto de comprobación 2: Si se ha configurado una ACL de red para el nodo

Inicie sesión en la consola de la VPC y elija **Access Control > Network ACLs**. Compruebe si se ha configurado una ACL de red para la subred donde se encuentra el nodo y si el acceso externo está restringido.

7.2.9 ¿Cómo resuelvo un conflicto entre el bloque CIDR de VPC y el bloque CIDR de contenedores?

Cuando crea un clúster, si el bloque CIDR de contenedor entra en conflicto con el bloque CIDR de VPC, se mostrará un mensaje de error. En este caso, cambie el bloque CIDR del contenedor.

Figura 7-13 Mensaje de error de conflicto

Network Settings Select the VPC and CIDR blocks for creating nodes and containers in the cluster.

Network Model **VPC network** Tunnel network [? Network Model Overview](#)
Model used for container networking in a cluster. Not editable after creation

Number of container IP addresses reserved for each node (cannot be changed after creation): 128 [Learn more](#)

VPC vpc-uc-paas-beta (10.10.0.0/16) [C Create VPC](#)
CIDR block used by master nodes and worker nodes in the cluster. Not editable after creation

Master Node Subnet uc-paas-beta-sb-1 (10.10.0.0/20) [C Create Subnet](#) Available Subnet IP Addresses: 4,089
Subnet used by the master node in the cluster. At least 4 IP addresses are required. Not editable after creation

Container CIDR Block **Manually set** Auto select [? How to plan CIDR blocks?](#)

10 . 0 . 0 . 0 / 8

X The pod CIDR block conflicts with the subnet CIDR block. Select another one.

! Max. nodes supported by the current networking configuration: 131,069

7.2.10 ¿Qué debo hacer si se reporta el error de Java "Connection reset by peer" durante la comprobación de estado de la capa 4 de ELB?

Información de error completa

```
java.io.IOException: Connection reset by peer
at sun.nio.ch.FileDispatcherImpl.read0(Native Method)
at sun.nio.ch.SocketDispatcher.read(SocketDispatcher.java:39)
at sun.nio.ch.IOUtil.readIntoNativeBuffer(IOUtil.java:223)
at sun.nio.ch.IOUtil.read(IOUtil.java:197)
at sun.nio.ch.SocketChannelImpl.read(SocketChannelImpl.java:380)
at
com.wanyu.smarthome.gateway.EquipmentSocketServer.handleReadEx(EquipmentSocketServer.java:245)
at
com.wanyu.smarthome.gateway.EquipmentSocketServer.run(EquipmentSocketServer.java:115)
```

Resultado del análisis

Se establece un servidor de socket utilizando Java Non-blocking I/O (NIO). Cuando el cliente se cierra inesperadamente en lugar de enviar una notificación especificada para indicar al servidor que salga, se informa de un error.

Proceso de comprobación de estado TCP

1. El nodo de ELB que realiza comprobaciones de estado envía un paquete SYN al servidor backend (dirección IP privada + puerto de comprobación de estado) basado en la configuración de comprobación de estado.
2. Después de recibir el paquete, el servidor backend devuelve un paquete SYN-ACK a través de su puerto.
3. Si el nodo de ELB no recibe el paquete SYN-ACK dentro de la duración del tiempo de espera, el servidor backend se declara insalubre. A continuación, el nodo de ELB envía un paquete RST al servidor back-end para terminar la conexión de TCP.
4. Si el nodo de ELB recibe el paquete SYN-ACK desde el servidor backend dentro de la duración del tiempo de espera, envía un paquete de ACK al servidor backend y declara que el servidor backend está en buen estado. A continuación, el nodo de ELB envía un paquete RST al servidor back-end para terminar la conexión de TCP.

Nota

Después de un handshake de tres vías de TCP normal, habrá transferencia de datos. Sin embargo, se enviará un paquete de RST para terminar la conexión de TCP durante la comprobación de estado. Las aplicaciones en el servidor backend pueden determinar un error de conexión e informar de un mensaje, por ejemplo, "Connection reset by peer".

Este error está justificado e inevitable. Puede ignorarlo.

7.2.11 ¿Cómo localizo el evento de servicio que indica que ningún nodo está disponible para el enlace?

Paso 1 Inicie sesión en la consola de CCE, haga clic en el clúster y elija **Networking** en el panel de navegación.

Paso 2 Compruebe si el Service tiene una carga de trabajo asociada o si los pods de la carga de trabajo asociada son normales.

---Fin

7.2.12 ¿Por qué se produce el "Dead loop on virtual device gw_11cbf51a, fix it urgently" cuando inicio sesión en una máquina virtual usando VNC?

Síntoma

En un clúster que utiliza el modelo de red de VPC, se muestra el mensaje "Dead loop on virtual device gw_11cbf51a, fix it urgently" después de iniciar sesión en la máquina virtual.

```
[7520230.908741] Dead loop on virtual device gw_11cbf51a, fix it urgently!  
[7764908.323899] Dead loop on virtual device gw_11cbf51a, fix it urgently!  
[7876345.412678] Dead loop on virtual device gw_11cbf51a, fix it urgently!  
[7886952.430199] Dead loop on virtual device gw_11cbf51a, fix it urgently!  
[8053806.787694] Dead loop on virtual device gw_11cbf51a, fix it urgently!
```

Causa

El modelo de red VPC utiliza el módulo IPvlan de Linux de código abierto para las redes de contenedores. En el modo L2E de IPvlan, se realiza preferentemente el reenvío de capa 2, y luego el reenvío de capa 3.

Reproducción de escenas

Supongamos que hay un pod A de servicio, que proporciona servicios externamente y al que accede constantemente el nodo en el que inicia sesión a través del puerto de gateway de contenedor a través del servicio Kubernetes host. Otro escenario puede ser que los pods en este nodo accedan directamente entre sí. Cuando el pod A sale debido a una actualización, escalado u otras razones, y se reclaman los recursos de red correspondientes, si el nodo todavía intenta enviar paquetes a la dirección IP del pod A, El módulo IPvlan en el núcleo primero intenta reenviar estos paquetes en la Capa 2 basándose en la dirección IP de destino. Sin embargo, como la NIC a la que pertenece la dirección IP de pod A ya no se puede encontrar, el módulo IPvlan determina que el paquete puede ser un paquete externo. Por lo tanto, el módulo intenta reenviar el paquete en la Capa 3 y hace coincidir el puerto de gateway basándose en la regla de encaminamiento. Después de que el puerto de gateway recibe el paquete de nuevo, reenvía el paquete a través del módulo IPvlan, y este proceso se repite. La función `dev_queue_xmit` en el núcleo detecta que el paquete se envía repetidamente 10 veces. Como resultado, se descarta el paquete y se generó este log.

Después de perder un paquete, el iniciador de acceso realiza generalmente reintentos de retroceso varias veces. Por lo tanto, se imprimen varios registros hasta que el ARP en el contenedor del iniciador de acceso envejezca o el servicio termine el acceso.

Para la comunicación entre contenedores en diferentes nodos, las direcciones IP de destino y origen no pertenecen a la misma subred dedicada a nivel de nodo (tenga en cuenta que esta subred es diferente de la subred de VPC). Por lo tanto, los paquetes no se enviarán repetidamente, y este problema no se producirá.

Se puede acceder a los pods de diferentes nodos del mismo clúster con un servicio de NodePort. Sin embargo, la dirección IP del servicio NodePort se traduce en la dirección IP de la interfaz de gateway del contenedor accedido por SNAT, que puede generar los registros que ve anteriormente.

Impacto

El funcionamiento normal del recipiente al que se accede no se ve afectado. Cuando se destruye un contenedor, hay un ligero impacto de que los paquetes se envían repetidamente 10 veces y luego se descartan. Este proceso es rápido en el kernel y tiene poco impacto en el rendimiento.

Si el ARP envejece, el servicio no vuelve a intentarlo o se inicia un nuevo contenedor, los paquetes de servicio de contenedor se redirigen al nuevo servicio con kube-proxy.

Manejo en la comunidad de código abierto

Actualmente, este problema todavía existe en la comunidad cuando se utiliza el modo L2E IPvlan. El problema ha sido reportado a la comunidad para una mejor solución.

Solución

El problema del bucle muerto no necesita ser resuelto.

Sin embargo, se recomienda que el pod de servicio salga correctamente. Antes de que finalice el servicio, configure el pod en el estado de eliminación. Después de completar el procesamiento del servicio, el pod sale.

7.2.13 ¿Por qué ocurre un pánico ocasionalmente cuando uso políticas de red en un nodo de clúster?

Escenario

Versión del clúster: v1.15.6-r1

Tipo de clúster: clúster de CCE

Modelo de red: red de túneles de contenedores

Sistema operativo del nodo: CentOS 7.6

Después de configurar una política de red para el clúster, el componente de red canal-agent en el nodo es incompatible con el núcleo de CentOS 7.6. Como resultado, puede producirse un pánico en el núcleo.

Condiciones

Si no se cumple alguna de las siguientes condiciones, este problema no se producirá:

- La versión del clúster es v1.15.6-r1 y se utiliza el modelo de red de túnel de contenedor.
- El nodo de CentOS 7.6 utiliza el componente canal-agent cuya versión es 1.0.RC10.1230.B005 o anterior. (Los nodos de CentOS 7.6 creados en o antes del 23 de febrero de 2021 usan dicho componente.)
- Tiene previsto utilizar o ha utilizado políticas de red.

Localización de fallas

Localización rápida (para nodos de pago por uso)

Compruebe si su nodo de CentOS 7.6 se creó después del 24 de febrero de 2021 en la consola de CCE.

Localización precisa (General)

Si la versión del clúster es v1.15.6-r1, el modelo de red es red de túnel de contenedor, el sistema operativo del nodo es CentOS 7.6, y la versión del componente del canal-agent es 1.0.RC10.1230.B005.sp1 o posterior, el problema no ocurrirá. Si se utiliza una versión anterior (por ejemplo, 1.0.RC10.1230.B002), se recomienda restablecer o eliminar el nodo antes de configurar las políticas de red.

Realice los siguientes pasos para consultar la versión del componente de red en el nodo:

Paso 1 Prepare un nodo donde se pueda usar kubectl.

Paso 2 Ejecute el siguiente comando para consultar la lista de nodos de CentOS:

```
for node_item in $(kubectl get nodes --no-headers | awk '{print $1}'); do  
  kubectl get node ${node_item} -o yaml | grep CentOS >/dev/null; if [[ "$?" ==  
  "0" ]];then echo "${node_item} is CentOS node";fi;done
```

La salida de comandos es la siguiente:

```
10.0.50.187 is CentOS node
10.0.50.220 is CentOS node
10.0.50.43 is CentOS node
```

Paso 3 Suponga que la dirección IP del nodo CentOS de destino es 10.0.50.187. Ejecute el siguiente comando para comprobar la versión canal-agent:

```
kubectl get packageversions.version.cce.io 10.0.50.187 -o yaml | grep -A 1 canal-agent
```

La salida de comandos es la siguiente:

```
- name: canal-agent
  version: 1.0.RC10.1230.B005.sp1
```

----Fin

Solución

Si aún desea utilizar el nodo, restablezca los nodos de CentOS 7.6 en el clúster para actualizar los componentes de red a la versión más reciente. Para obtener más información, consulte [Restablecimiento de un nodo](#).

Si desea eliminar el nodo riesgoso y comprar uno nuevo, consulte [Eliminar un nodo](#) y [Comprar un nodo](#).

7.2.14 ¿Por qué se generan muchos logs de origen ip_type en el VNC?

Escenario

Versión del clúster: v1.15.6-r1

Tipo de clúster: clúster de CCE

Modelo de red: red de VPC

Sistema operativo del nodo: CentOS 7.6

Cuando los contenedores en los nodos anteriores se comunican entre sí, el componente de red de contenedores informa de un gran número de fuentes ip_types o "no ipvlan sino en registros de host propios" en el VNC. Como resultado, la página de VNC en el nodo y el rendimiento de la red de contenedores en escenarios de alta carga se ven afectados. Los síntomas de este problema son los siguientes:

```
[ 3840.916433] =====source ip_type 2, ipv4 10.0.0.128, mac fa:16:3e:57:f2:8f
[ 3840.916527] =====source ip_type 2, ipv4 10.0.0.129, mac fa:16:3e:57:f2:8f
[ 3840.916736] =====source ip_type 2, ipv4 10.0.0.129, mac fa:16:3e:57:f2:8f
```

```
[16739.000551] =====not ipvlan but in own host, mac_src=fa:16:3e:34:23:93 mac_dst=ff:ff:ff:ff:ff:ff
[16740.000968] =====not ipvlan but in own host, mac_src=fa:16:3e:34:23:93 mac_dst=ff:ff:ff:ff:ff:ff
```

Localización de fallas

1. Comprobación rápida

Este método se aplica a los nodos de pago por uso. Compruebe el tiempo de creación del nodo en la consola de CCE. Los nodos CentOS 7.6 creados a partir del 24 de febrero de 2021 no tienen este problema.

2. Comprobación precisa (General)

Puede realizar los siguientes pasos para comprobar si un nodo está afectado:

Paso 1 Inicie sesión en cada nodo de CCE como el usuario **root**.

Paso 2 Ejecute el siguiente comando para comprobar si el nodo es arriesgado:

```
ETH0_IP=$(ip addr show eth0 | grep "inet " | head -n 1 | awk '{print $2}' | awk -F '/' '{print $1}') ;arping -w 0.2 -c 1 -I gw_11cbf51a 1.1.1.1 >/dev/null 2>&1 ; echo ;dmesg -T | grep -E "!==not ipvlan but in own host!=="source ip_type" 1>/dev/null 2>&1 ; if [[ "$?" == "0" ]];then echo "WARNING, node ${ETH0_IP} is affected"; else echo "node ${ETH0_IP} works well"; fi;
```

NOTA

En este comando, el *1.1.1.1* es una dirección IP de ejemplo, que solo se usa para activar el envío de paquetes ARP. Puede usarlo o reemplazarlo con una dirección IP válida.

Paso 3 Si se muestra la siguiente información, el nodo tiene los riesgos potenciales. *10.2.0.35* es la dirección IP de la NIC eth0 en el nodo. La dirección IP real se mostrará en su consulta.

```
WARNING, node 10.2.0.35 is affected
```

Si se muestra la siguiente información, el nodo no tiene este problema:

```
node 10.2.0.35 works well
```

---Fin

Procedimiento

Si aún desea utilizar el nodo, restablezca los nodos de CentOS 7.6 en el clúster para actualizar los componentes de red a la versión más reciente. Para obtener más información, consulte [Restablecimiento de un nodo](#).

Si desea eliminar el nodo riesgoso y comprar uno nuevo, consulte [Eliminar un nodo](#) y [Comprar un nodo](#).

7.3 Resguardo de la seguridad

7.3.1 ¿Cómo puedo evitar que los nodos de clúster se expongan a las redes públicas?

- Si no se requiere acceso al puerto 22 de un nodo de clúster, puede definir una regla de grupo de seguridad que inhabilite el acceso al puerto 22.
- No vincule una EIP a un nodo de clúster a menos que sea necesario.

Si se requiere el inicio de sesión remoto en un nodo de clúster, se recomienda utilizar Cloud Bastion Host (CBH) como nodo de tránsito para conectarse al nodo de clúster.

7.4 Configuración de la red

7.4.1 ¿Cómo se comunica CCE con otros servicios de Huawei Cloud por una intranet?

Los servicios comunes de Huawei Cloud que se comunican con CCE por la intranet incluyen RDS, DMS, Kafka, RabbitMQ, VPN y ModelArts. Se trata de los dos escenarios siguientes:

- En la misma red de VPC, los nodos de CCE pueden comunicarse con todos los servicios. Cuando los nodos de CCE se comunican con otros servicios, compruebe si la regla de grupo de seguridad en la dirección de entrada del bloque CIDR del contenedor está habilitada en el extremo del par. (Esta restricción solo se aplica a los clústeres de CCE que utilizan el modelo de red de VPC.)
- Si los nodos de CCE y otros servicios están en las VPC diferentes, puede usar una interconexión o la VPN para conectar dos VPC. Obsérvese que los dos bloques de CIDR de VPC no pueden solaparse con el bloque de CIDR de contenedor. Además, debe configurar una ruta de retorno para la VPC del mismo nivel o la red privada. (Esta restricción solo se aplica a los clústeres de CCE que utilizan el modelo de red de VPC.) Para obtener más información, consulte [Interconexión de VPC](#).

AVISO

- Esta lógica funciona para todos los servicios de Huawei Cloud.
- Los clústeres que utilizan la red de túneles de contenedores admiten la comunicación interna de Services sin necesidad de configuración adicional.
- Preste atención a los siguientes puntos al configurar un clúster mediante la red de VPC:
 1. La dirección IP de origen que se muestra en el extremo del par es la dirección IP del contenedor.
 2. Las reglas de enrutamiento personalizadas agregadas en CCE permiten que los contenedores se comuniquen entre sí en los nodos de una VPC.
 3. Cuando un contenedor de CCE accede a otros Servicios, haga clic en **check whether the inbound security group rule or firewall of the container CIDR block is configured on the peer end (destination end)**. Para obtener más información, consulte los [Ejemplos de configuración de grupo de seguridad](#).
 4. Si se utiliza una interconexión de VPC o VPN para habilitar la comunicación entre las redes privadas, debe configurar **una ruta de la interconexión de VPC que apunta al bloque CIDR del contenedor** en la ruta y el destino.

7.4.2 ¿Cómo configuro el puerto al configurar el modo de acceso a la carga de trabajo en CCE?

CCE es compatible con el acceso interno y externo.

Al configurar el modo de acceso a la carga de trabajo, debe configurar dos puertos: el **Container Port** y el **Access Port**.

Container Port indica el puerto de escucha de una carga de trabajo en el contenedor. El número de puerto varía según el tipo de servicio y normalmente se especifica en una imagen de contenedor.

Access Port se especifica en función del tipo de acceso.

- Para el acceso interno, el tipo de acceso puede ser **Dirección IP virtual del clúster** o **Dirección IP privada del nodo**.

Tabla 7-7 Descripción del tipo de acceso interno

Tipo de acceso interno	Descripción	Guía
Dirección IP virtual del clúster	<p>Se utiliza para el acceso mutuo entre cargas de trabajo de un clúster. Por ejemplo, si una carga de trabajo de backend necesita comunicarse con una carga de trabajo de frontend, utilice este tipo de acceso.</p> <p>Cuando se selecciona este tipo de acceso, se asigna automáticamente una dirección IP de clúster.</p>	<p>Access port: cuando una carga de trabajo de un contenedor se libera como un servicio, el puerto de acceso es el número de puerto de servicio. El valor es un número entero entre 1 y 65535. Las cargas de trabajo se acceden entre sí con cluster IP:access port.</p>
Dirección IP privada del nodo	<p>Se puede acceder a una carga de trabajo con node IP:access port. Si una dirección IP elástica está vinculada al nodo, se puede acceder a las cargas de trabajo del nodo desde redes externas.</p>	<p>Access port: Puerto (en el nodo) al que se asigna un contenedor. Cuando se completa la configuración, el sistema habilita un puerto real en todos los nodos del proyecto donde se encuentra el usuario. Se puede acceder a una carga de trabajo con node IP:access port.</p> <p>Si no hay requisitos especiales, seleccione Automatically generated para que el sistema asigne automáticamente un puerto de acceso. Si selecciona Specified port, escriba un entero que va de 30000 a 32767 y asegúrese de que el valor es único en el clúster.</p>

- Para el acceso externo, el tipo de acceso puede ser **EIP** o **ELB**.

Tabla 7-8 Descripción del tipo de acceso externo

Tipo de acceso externo	Descripción	Guía
EIP	<p>La dirección IP elástica vinculada a un nodo. Se puede acceder a una carga de trabajo con elastic node IP:node port. Se puede acceder a la carga de trabajo desde Internet.</p>	<p>Access port: Puerto (en el nodo) al que se asigna un contenedor. Cuando se completa la configuración, el sistema habilita un puerto real en todos los nodos del proyecto donde se encuentra el usuario. Se puede acceder a una carga de trabajo con node IP:access port.</p> <p>Si no hay requisitos especiales, seleccione Automatically generated para que el sistema asigne automáticamente un puerto de acceso. Si selecciona Specified port, escriba un entero que va de 30000 a 32767 y asegúrese de que el valor es único en el clúster.</p>
ELB	<p>ELB distribuye automáticamente el tráfico de acceso a múltiples nodos para equilibrar su carga de servicio. Admite niveles más altos de tolerancia a fallos para cargas de trabajo y amplía las capacidades de servicio de cargas de trabajo.</p> <p>Debe crear una instancia de ELB por adelantado y seleccionar ELB como tipo de acceso CCE.</p>	<p>Access port: puerto externo registrado en el ELB. La dirección IP virtual y el puerto de servicio del ELB se utilizan para el acceso externo.</p>

7.4.3 ¿Cómo puedo lograr la compatibilidad entre la propiedad de entrada y el client-go de Kubernetes?

Escenario

La estructura de entrada de Kubernetes no contiene el atributo **property**. Por lo tanto, la entrada creada por la invocación a la API client-go no contiene el atributo **property**. CCE proporciona una solución para garantizar la compatibilidad con Kubernetes client-go.

Solución

Quando utilice client-go para crear una instancia de ingreso, realice la siguiente declaración en el **annotation**:

```
kubernetes.io/ingress.property: '[{"host":"test.com","path":"/
test","matchmode":"STARTS_WITH"}, {"host":"test.com","path":"/
dw","matchmode":"EQUAL_TO}]'
```

Matching rule: Cuando un usuario llama a la interfaz de Kubernetes de CCE para crear una instancia de ingreso, CCE intenta hacer coincidir los campos **host** y **path** en las reglas de ingreso. Si los campos **host** y **path** de las reglas de ingreso son los mismos que los de la anotación, CCE inyecta el atributo **property** en la ruta de acceso. A continuación se presenta un ejemplo:

```
kind: Ingress
apiVersion: extensions/v1beta1
metadata:
  name: test
  namespace: default
  resourceVersion: '2904229'
  generation: 1
  labels:
    isExternal: 'true'
    zone: data
  annotations:
    kubernetes.io/ingress.class: cce
    kubernetes.io/ingress.property: '[{"host":"test.com","path":"/
test","matchmode":"STARTS_WITH"}, {"Path":"/dw","MatchMode":"EQUAL_TO}]'
```

```
spec:
  rules:
    - host: test.com
      http:
        paths:
          - path: /ss
            backend:
              serviceName: zlh-test
              servicePort: 80
          - path: /dw
            backend:
              serviceName: zlh-test
              servicePort: 80
```

El formato después de la conversión es el siguiente:

```
kind: Ingress
apiVersion: extensions/v1beta1
metadata:
  name: test
  namespace: default
  resourceVersion: '2904229'
  generation: 1
  labels:
    isExternal: 'true'
    zone: data
  annotations:
    kubernetes.io/ingress.class: cce
    kubernetes.io/ingress.property: '[{"host":"test.com","path":"/
ss","matchmode":"STARTS_WITH"}, {"host":"","path":"/dw","matchmode":"EQUAL_TO}]'
```

```
spec:
  rules:
    - host: test.com
      http:
        paths:
          - path: /ss
            backend:
              serviceName: zlh-test
              servicePort: 80
            property:
              ingress.beta.kubernetes.io/url-match-mode: STARTS_WITH
          - path: /dw
            backend:
              serviceName: zlh-test
              servicePort: 80
```

Tabla 7-9 Descripciones de parámetros clave

Parámetro	Tipo	Descripción
host	String	Configuración del nombre de dominio. Si este parámetro no está definido, se hace coincidir automáticamente path .
path	String	Camino coincidente.
ingress.beta.kubernetes.io/url-match-mode	String	Política de coincidencia de rutas. Los valores son los siguientes: <ul style="list-style-type: none"> ● REGEX: indica coincidencia de expresiones regulares. ● STARTS_WITH: indica coincidencia de prefijo. ● EQUAL_TO: indica la coincidencia exacta.

Enlaces útiles

[Balanceo de carga de Capa-7 \(Ingreso\)](#)

7.5 Otros

7.5.1 ¿Cómo obtengo un certificado de clave TLS?

Escenario

Si su ingreso necesita usar HTTPS, debe configurar un secreto del tipo IngressTLS o kubernetes.io/tls al crear un ingreso.

Cree un certificado de clave de IngressTLS, como se muestra en [Figura 7-14](#).

Figura 7-14 Creación de un secreto

El archivo de certificado que se va a cargar debe coincidir con el archivo de clave privada. De lo contrario, el archivo de certificado no será válido.

Solución

Por lo general, debe obtener un certificado válido del proveedor del certificado. Si desea usarlo en el entorno de prueba, puede crear un certificado y una clave privada realizando los siguientes pasos.

NOTA

Los certificados de creación automática solo se aplican a los escenarios de prueba. Dichos certificados no son válidos y afectarán al acceso al navegador. Suba manualmente uno válido para garantizar conexiones seguras.

1. Genere un `tls.key`.

```
openssl genrsa -out tls.key 2048
```

El comando generará un `tls.key` privado en el directorio donde se ejecuta el comando.

2. Genere un certificado usando la `tls.key` privada.

```
openssl req -new -x509 -key tls.key -out tls.crt -subj /C=CN/ST=Beijing/O=Devops/CN=example.com -days 3650
```

La clave generada debe tener el siguiente formato:

```
-----BEGIN RSA PRIVATE KEY-----
.....
-----END RSA PRIVATE KEY-----
```

El certificado generado debe tener el siguiente formato:

```
-----BEGIN CERTIFICATE-----
.....
-----END CERTIFICATE-----
```

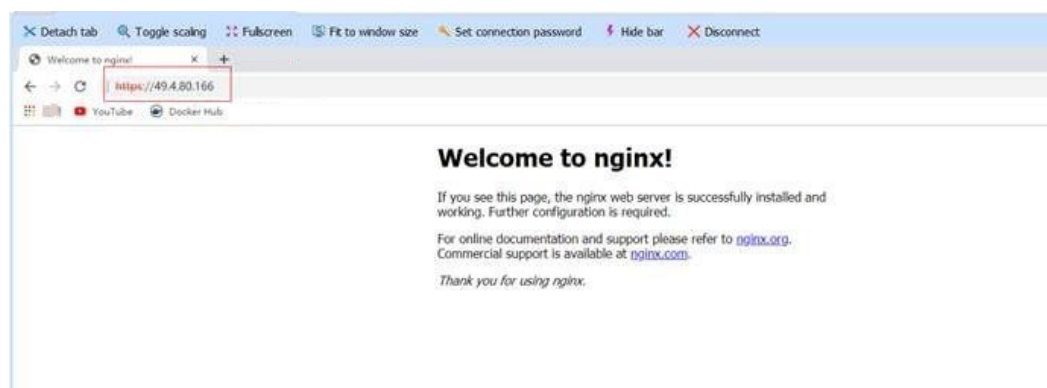
3. Importe el certificado.

Cuando cree un secreto de TLS, importe el archivo de certificado y clave privada a la ubicación correspondiente.

Verificación

El uso de un navegador para acceder a la entrada es exitoso. Sin embargo, el certificado y el secreto no son emitidos por CA y la barra de direcciones muestra que la conexión a nginx no es segura.

Figura 7-15 Resultado de la verificación



7.5.2 ¿Se pueden vincular varias NIC a un nodo en un clúster de CCE?

Se admite multi-NIC.

Sin embargo, no se recomienda vincular manualmente varias NIC a un nodo en un clúster de CCE porque las reglas configuradas después de vincular varias NIC pueden afectar el acceso al clúster de CCE Turbo.

7.5.3 ¿Por qué se elimina automáticamente el grupo de servidores backend de un ELB después de publicar un servicio en el ELB?

Síntomas

Después de publicar un Service en ELB, la carga de trabajo es normal, pero el puerto pod del servicio no se publica a tiempo. Como resultado, el grupo de servidores backend del ELB se elimina automáticamente.

Respuesta

1. Si la comprobación de supervisión de ELB falla durante la creación de ELB, el grupo de servidores backend se eliminará y no se agregará después de que el servicio se vuelva normal. Si se actualiza un SVC existente, el grupo de servidores backend no se elimina.
2. Cuando se agrega o elimina un nodo, el modo de acceso al nodo en el clúster puede cambiar debido al cambio de estado del clúster. Para garantizar el funcionamiento

normal del servicio, el ELB realiza una operación de actualización. El proceso es similar al de actualizar el ELB.

Consejos

Optimice la aplicación para acelerar el inicio.

7.5.4 ¿Por qué no se puede crear una entrada después de cambiar el espacio de nombres?

Síntoma

Una entrada se puede crear en el espacio de nombres predeterminado, pero no se puede crear en otros espacios de nombres.

Análisis de las causas

Después de crear un balanceador de carga, se crea un oyente de HTTP en el espacio de nombres predeterminado para el puerto 80. En CCE, solo se pueden crear entradas del mismo puerto en el mismo espacio de nombres (las políticas de reenvío reales se pueden distinguir en función de nombres de dominio y servicios). Por lo tanto, no se pueden crear entradas del mismo puerto en otros espacios de nombres (se muestra un mensaje de conflicto de puerto).

Solución

Puede usar archivos YAML para crear entradas. Los conflictos de puertos se producen al crear entradas en la consola de CCE, pero no cuando lo hace en el backend.

7.5.5 ¿Cómo obtengo la dirección IP de origen real de un cliente después de agregar un servicio a Istio?

Síntoma

Después de habilitar Istio, la dirección IP de origen del cliente no se puede obtener de los logs de acceso.

Solución

Esta sección utiliza la aplicación de Nginx vinculada a un Service de ELB como ejemplo. El procedimiento es el siguiente:

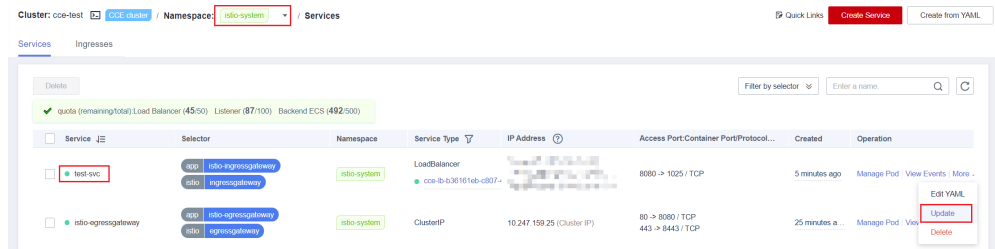
Paso 1 Habilitar la función de obtener la dirección IP del cliente en el balanceador de carga

NOTA

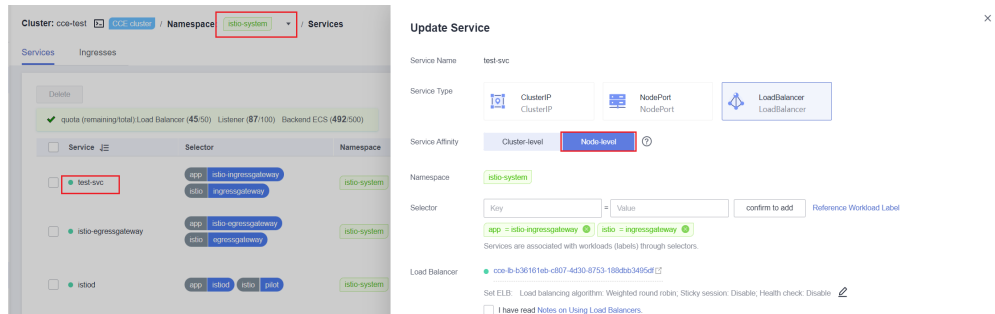
La transmisión transparente de direcciones IP de origen está habilitada por defecto para los balanceadores de carga dedicados. No es necesario activar manualmente esta función.

Paso 2 Actualizar el gateway asociado a un Service

1. Inicie sesión en la consola de CCE y haga clic en el nombre del clúster para acceder a la consola del clúster. En el panel de navegación, elija **Networking**.
2. En la página mostrada, cambie al espacio de nombres **istio-system** y actualice el gateway asociado al Service.



3. Cambie el nivel del Service generado automáticamente en el espacio de nombres **istio-system** al nivel de nodo.



Paso 3 Verificar la dirección IP de origen obtenida

1. Utilice `kubectl` para conectarse al clúster.
2. Consulte los logs de la aplicación de Nginx.
`kubectl logs <pod_name>`

En este ejemplo, la dirección IP de origen obtenida por la aplicación de Nginx es la siguiente:

```
2023/04/11 16:56:18 [notice] 1#1: using the "opssl" event method
2023/04/11 16:56:18 [notice] 1#1: nginx/1.21.6
2023/04/11 16:56:18 [notice] 1#1: built by gcc 10.2.1 20210110 (Debian 10.2.1-6)
2023/04/11 16:56:18 [notice] 1#1: OS: Linux 4.18.0-147.2.1.el8_4.x86_64
2023/04/11 16:56:18 [notice] 1#1: getrlimit(0:1024:1024): 1048576:1048576
2023/04/11 16:56:18 [notice] 1#1: start worker processes
2023/04/11 16:56:18 [notice] 1#1: start worker process 30
2023/04/11 16:56:18 [notice] 1#1: start worker process 31
2023/04/11 16:56:18 [notice] 1#1: start worker process 32
2023/04/11 16:56:18 [notice] 1#1: start worker process 33
127.0.0.6 - - [11/Apr/2023:16:56:31 +0000] "GET / HTTP/1.1" 304 0 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.0.0 Safari/537.36 Edge/112.0.1722.34" "-"
127.0.0.6 - - [11/Apr/2023:16:56:33 +0000] "GET / HTTP/1.1" 304 0 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.0.0 Safari/537.36 Edge/112.0.1722.34" "10.0.0.129"
127.0.0.6 - - [11/Apr/2023:16:56:49 +0000] "GET / HTTP/1.1" 304 0 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.0.0 Safari/537.36 Edge/112.0.1722.34" "-"
127.0.0.6 - - [11/Apr/2023:16:56:58 +0000] "GET / HTTP/1.1" 304 0 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.0.0 Safari/537.36 Edge/112.0.1722.34" "10.0.0.129"
127.0.0.6 - - [11/Apr/2023:16:58:18 +0000] "GET / HTTP/1.1" 304 0 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.0.0 Safari/537.36 Edge/112.0.1722.34" "127.0.0.1"
```

----Fin

7.5.6 ¿Cómo cambio el grupo de seguridad de nodos en un clúster por lotes?

Notas y restricciones

No agregue más de 1000 instancias al mismo grupo de seguridad. De lo contrario, el rendimiento del grupo de seguridad puede deteriorarse. Para obtener más restricciones en los grupos de seguridad, consulte [Restricciones del grupo de seguridad](#).

Procedimiento

- Paso 1** Inicie sesión en la consola de VPC y seleccione la región y el proyecto deseados en la esquina superior izquierda.
- Paso 2** En el panel de navegación de la izquierda, elija **Access Control > Security Groups**.
- Paso 3** En la página **Security Groups**, haga clic en **Manage Instance** en la columna **Operation**.

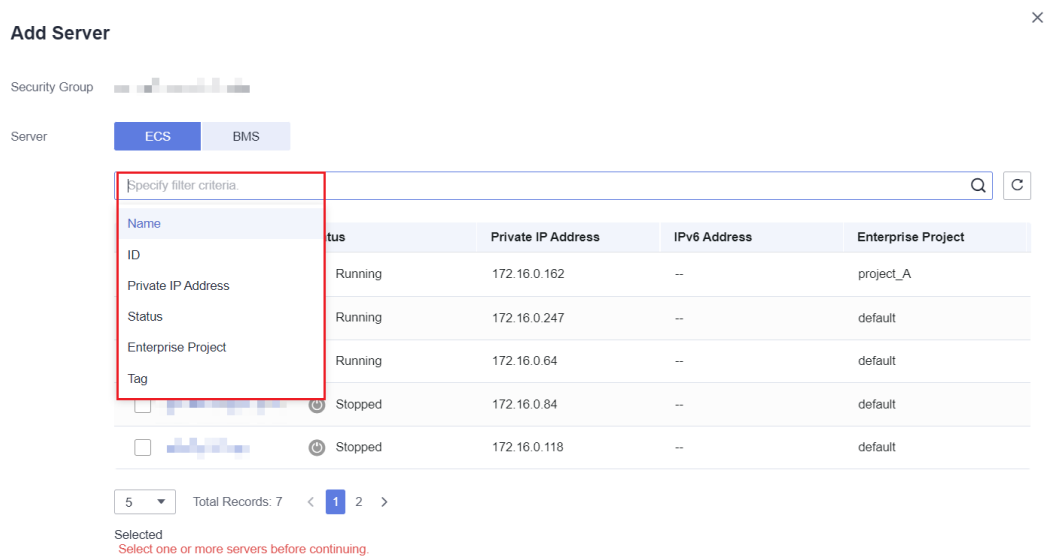
Paso 4 En la página de ficha **Servers**, haga clic en **Add**.

Paso 5 Seleccione los servidores que se agregarán al grupo de seguridad y haga clic en **OK**. También puede filtrar los servidores por nombre, ID, dirección IP privada, estado, proyecto de empresa o etiqueta.

Puede cambiar el número máximo de servidores que se muestran en una página en la esquina inferior izquierda para agregar un máximo de 20 servidores a un grupo de seguridad a la vez.

NOTA

Después de agregar el nodo a un nuevo grupo de seguridad, se conserva el grupo de seguridad original. Para quitar la instancia, haga clic en **Manage Instance** del grupo de seguridad original y seleccione los servidores de nodo que se van a quitar.



Add Server ×

Security Group [Placeholder]

Server ECS BMS

Specify filter criteria. Q C

Name	Status	Private IP Address	IPv6 Address	Enterprise Project
ID	Running	172.16.0.162	--	project_A
Private IP Address	Running	172.16.0.247	--	default
Status	Running	172.16.0.64	--	default
Enterprise Project	Running	172.16.0.64	--	default
Tag	Stopped	172.16.0.84	--	default
	Stopped	172.16.0.118	--	default

5 Total Records: 7 < 1 2 >

Selected
Select one or more servers before continuing.

----Fin

8 Almacenamiento

8.1 ¿Cuáles son las diferencias entre las clases de almacenamiento de CCE en términos de almacenamiento persistente y montaje multinodo?

El almacenamiento de contenedores proporciona almacenamiento para cargas de trabajo de contenedores. Soporta múltiples clases de almacenamiento. Un pod puede usar cualquier cantidad de almacenamiento.

Actualmente, CCE admite volúmenes locales, EVS, SFS, SFS Turbo y OBS.

En la siguiente tabla se enumeran las diferencias entre estas clases de almacenamiento.

Tabla 8-1 Diferencias entre las clases de almacenamiento

Clase de almacenamiento	Almacenamiento persistente	Migración automática con contenedores	Montaje multinodo
Volúmenes locales	Se admite	No se admite	No se admite
Volúmenes de EVS	Se admite	Se admite	No se admite
Volúmenes de OBS	Se admite	Se admite	Se admite. Este tipo de volúmenes se pueden compartir entre múltiples nodos o cargas de trabajo.
Volúmenes de SFS	Se admite	Se admite	Se admite. Este tipo de volúmenes se pueden compartir entre múltiples nodos o cargas de trabajo.

Clase de almacenamiento	Almacenamiento persistente	Migración automática con contenedores	Montaje multinodo
Volúmenes de Turbo de SFS	Se admite	Se admite	Se admite. Este tipo de volúmenes se pueden compartir entre múltiples nodos o cargas de trabajo.

Selección de una clase de almacenamiento

Puede utilizar los siguientes tipos de volúmenes de almacenamiento al crear una carga de trabajo. Se recomienda almacenar datos de carga de trabajo en volúmenes de EVS. Si almacena datos de carga de trabajo en un volumen local, los datos no se pueden restaurar cuando se produce un error en el nodo.

- **Volúmenes locales:** Monte el directorio de archivos del host donde se encuentra un contenedor en una ruta de contenedor especificada (correspondiente a hostPath en Kubernetes). Alternativamente, puede dejar la ruta de origen vacía (correspondiente a emptyDir en Kubernetes). Si la ruta de origen se deja vacía, se montará un directorio temporal del host en el punto de montaje del contenedor. Se utiliza una ruta de origen especificada cuando los datos deben almacenarse de forma persistente en el host, mientras que se utiliza emptyDir cuando se necesita almacenamiento temporal. Un ConfigMap es un tipo de recurso que almacena los datos de configuración requeridos por una carga de trabajo. Sus contenidos son definidos por el usuario. Un secreto es un tipo de recurso que contiene datos confidenciales, como la autenticación y la información clave. Sus contenidos son definidos por el usuario.
- **Volúmenes de EVS:** Monte un volumen EVS en una ruta de contenedor. Cuando se migra el contenedor, el volumen EVS montado se migra conjuntamente. Esta clase de almacenamiento es aplicable cuando los datos deben almacenarse de forma permanente.
- **Volúmenes de SFS:** Cree los volúmenes de SFS y móntelos en una ruta de contenedor. También se pueden utilizar los volúmenes del sistema de archivos creados por el servicio SFS subyacente. Los volúmenes de SFS son aplicables al almacenamiento persistente para lectura/escritura frecuente en múltiples escenarios de carga de trabajo, incluidos procesamiento de medios, gestión de contenido, análisis de big data y análisis de carga de trabajo.
- **Volúmenes de OBS:** Cree los volúmenes de OBS y móntelos en una ruta de contenedor. Los volúmenes de OBS son aplicables a escenarios como carga de trabajo en la nube, análisis de datos, análisis de contenido y objetos de punto de acceso.
- **Volúmenes de SFS Turbo:** Cree los volúmenes de SFS Turbo y móntelos en una ruta de contenedor. Los volúmenes de SFS Turbo son rápidos, bajo demanda y escalables, lo que los hace adecuados para DevOps y aplicaciones de oficina empresarial.

8.2 ¿Puedo agregar un nodo sin un disco de datos de 100 GB?

No. El disco de datos de 100 GB es obligatorio.

Un disco de datos de 100 GB dedicado a Docker está conectado al nuevo nodo. De forma predeterminada, CCE utiliza Logical Volume Manager (LVM) para gestionar discos de datos. Con LVM, puede ajustar la relación de espacio en disco para diferentes recursos en un disco de datos. Para obtener más información, consulte [Descripción general de LVM](#).

Si el disco de datos se desinstala o se daña, el servicio Docker se vuelve anormal y el nodo no está disponible.

8.3 ¿Puedo restaurar un disco de EVS utilizado como volumen persistente en un clúster de CCE después de que el disco se elimine o expire?

Es necesario configurar manualmente las políticas de copia de respaldo para los discos de EVS. Si se elimina o libera un disco de EVS, puede utilizar la copia de respaldo de VBS para restaurar datos.

8.4 ¿Qué debo hacer si no se puede encontrar el host cuando se necesitan cargar archivos en OBS durante el acceso al servicio CCE desde una red pública?

Cuando un Service desplegado en CCE intenta cargar archivos a OBS después de recibir una solicitud de acceso desde una máquina sin conexión, se muestra un mensaje de error que indica que no se puede encontrar el host. La siguiente figura muestra el mensaje de error:

Time	message
February 22nd 2020, 18:50:27.521	com.obs.services.exception.ObsException: OBS service Error Message. Request Error : java.net.UnknownHostException: obs.cn-east-2.myhuaweicloud.com
February 22nd 2020, 18:50:27.521	18:50:27.520 [XNIO-1 task-16] ERROR c.h.f.c.provider.ExceptionProvider - OBS service Error Message. Request Error : java.net.UnknownHostException: obs.cn-east-2.myhuaweicloud.com
February 22nd 2020, 18:50:27.298	18:50:27.298 [XNIO-1 task-9] ERROR c.h.f.c.provider.ExceptionProvider - OBS service Error Message. Request Error : java.net.UnknownHostException: obs.cn-east-2.myhuaweicloud.com
February 22nd 2020, 18:50:27.298	com.obs.services.exception.ObsException: OBS service Error Message. Request Error : java.net.UnknownHostException: obs.cn-east-2.myhuaweicloud.com
February 22nd 2020, 18:50:27.275	18:50:27.274 [XNIO-1 task-9] WARN c.o.s.internal.RestStorageService - com.obs.services.internal.ServiceException: Request Error : java.net.UnknownHostException: obs.cn-east-2.myhuaweicloud.com HEAD 'https://obs.cn-east-2.myhuaweicloud.com/obs-it-problem-management-media-test?apiversion' on Host 'obs.cn-east-2.myhuaweicloud.com'
February 22nd 2020, 18:50:27.275	com.obs.services.internal.ServiceException: Request Error : java.net.UnknownHostException: obs.cn-east-2.myhuaweicloud.com
February 22nd 2020, 18:50:27.275	2020-02-22 18:50:27 274 com.obs.services.internal.RestStorageService handleThrowable 205 com.obs.services.internal.ServiceException: Request Error : java.net.UnknownHostException:

Localización de fallas

Después de recibir la solicitud HTTP, el Service transfiere archivos a OBS a través del proxy.

Si se transfieren demasiados archivos, se consume un gran número de recursos. Actualmente, al proxy se le asigna 128 MB de memoria. De acuerdo con los resultados de la prueba de presión, el consumo de recursos es grande, lo que resulta en una falla de solicitud.

Los resultados de la prueba muestran que todo el tráfico pasa a través del proxy. Por lo tanto, si el volumen de servicio es grande, es necesario asignar más recursos.

Solución

1. La transferencia de archivos implica un gran número de copias de paquetes, que ocupa una gran cantidad de memoria. Se recomienda aumentar la memoria proxy en función del escenario real y luego intentar acceder al Service y cargar archivos de nuevo.
2. Además, puede quitar el Service de la malla porque el proxy solo reenvía paquetes y no realiza ninguna otra operación. Si las solicitudes pasan por la puerta de entrada, la función de liberación en escala de grises del Service no se ve afectada.

8.5 ¿Cuántos nodos (ECS) se puede montar un sistema de archivos SFS?

El número de ECS en los que se puede montar un sistema de archivos SFS no está limitado.

8.6 ¿Cómo puedo lograr la compatibilidad entre ExtendPathMode y Kubernetes client-go?

Escenario

La estructura de pods de Kubernetes no contiene **ExtendPathMode**. Por lo tanto, cuando un usuario invoca a la API para crear un pod o despliegue usando client-go, el pod creado no contiene **ExtendPathMode**. CCE proporciona una solución para garantizar la compatibilidad con Kubernetes client-go.

Solución

AVISO

- Cuando crea un pod, necesita agregar **kubernetes.io/extend-path-mode** al **annotation** del pod.
- Al crear una Deployment, debe agregar **kubernetes.io/extend-path-mode** a **kubernetes.io/extend-path-mode** en la plantilla.

El siguiente es un ejemplo YAML de creación de un pod. Después de agregar la palabra clave **kubernetes.io/extend-path-mode** a **annotation** se hacen coincidir los campos **containername**, **name** y **mountpath** y el **extendpathmode** correspondiente se agrega a **volumeMount**.

```
apiVersion: v1
kind: Pod
metadata:
  name: test-8b59d5884-96vdz
  generateName: test-8b59d5884-
  namespace: default
  selfLink: /api/v1/namespaces/default/pods/test-8b59d5884-96vdz
  labels:
```

```

    app: test
    pod-template-hash: 8b59d5884
    annotations:
      kubernetes.io/extend-path-mode:
' [{"containername": "container-0", "name": "vol-156738843032165499", "mountpath": "/tmp", "extendpathmode": "PodUID"} ]'
      metrics.alpha.kubernetes.io/custom-endpoints:
' [{"api": "", "path": "", "port": "", "names": ""}]'
    ownerReferences:
      - apiVersion: apps/v1
        kind: ReplicaSet
        name: test-8b59d5884
        uid: 2633020b-cd23-11e9-8f83-fal63e592534
        controller: true
        blockOwnerDeletion: true
spec:
  volumes:
    - name: vol-156738843032165499
      hostPath:
        path: /tmp
        type: ''
    - name: default-token-4s959
      secret:
        secretName: default-token-4s959
        defaultMode: 420
  containers:
    - name: container-0
      image: 'nginx:latest'
      env:
        - name: PAAS_APP_NAME
          value: test
        - name: PAAS_NAMESPACE
          value: default
        - name: PAAS_PROJECT_ID
          value: b6315dd3d0ff4be5b31a963256794989
      resources:
        limits:
          cpu: 250m
          memory: 512Mi
        requests:
          cpu: 250m
          memory: 512Mi
      volumeMounts:
        - name: vol-156738843032165499
          mountPath: /tmp
          extendPathMode: PodUID
        - name: default-token-4s959
          readOnly: true
          mountPath: /var/run/secrets/kubernetes.io/serviceaccount
          terminationMessagePath: /dev/termination-log
          terminationMessagePolicy: File
          imagePullPolicy: Always
      restartPolicy: Always
      terminationGracePeriodSeconds: 30
      dnsPolicy: ClusterFirst
      serviceAccountName: default
      serviceAccount: default
      nodeName: 192.168.0.24
      securityContext: {}
      imagePullSecrets:
        - name: default-secret
        - name: default-secret
      affinity: {}
      schedulerName: default-scheduler
      tolerations:
        - key: node.kubernetes.io/not-ready
          operator: Exists
          effect: NoExecute
          tolerationSeconds: 300

```

```
- key: node.kubernetes.io/unreachable
  operator: Exists
  effect: NoExecute
  tolerationSeconds: 300
priority: 0
dnsConfig:
  options:
    - name: timeout
      value: ''
    - name: ndots
      value: '5'
    - name: single-request-reopen
enableServiceLinks: true
```

Tabla 8-2 Descripciones de parámetros clave

Parámetro	Tipo	Descripción
containername	String	Nombre de un contenedor.
name	String	Nombre de un volumen.
mountpath	String	Camino de monte.
extendpathmode	String	<p>Se agrega un directorio de tercer nivel al directorio/subdirectorio de volumen creado para facilitar la obtención de un archivo de salida del pod único.</p> <p>Se admiten los cinco tipos siguientes. Para obtener más información, consulte Logs de contenedores.</p> <ul style="list-style-type: none"> ● None: La ruta extendida no está configurada. ● PodUID: ID de un pod. ● PodName: Nombre de un pod. ● PodUID/ContainerName: ID de un pod o nombre de un contenedor. ● PodName/ContainerName: Nombre de un pod o un contenedor.

8.7 ¿Qué debo hacer si no se crea un volumen de almacenamiento?

Síntoma

No se puede crear el PV o el PVC. En el evento se muestra la siguiente información:

```
{"message": "Your account is suspended and resources can not be used.", "code": 403}
```

Causa posible

La información del evento indica que la cuenta está deshabilitada o no tiene permisos. Comprueba si el estado de la cuenta es normal. Si la cuenta es normal, compruebe los

permisos de espacio de nombres del usuario. Para obtener más información, consulte [Configuración de permisos de espacio de nombres \(en la consola\)](#).

8.8 ¿Pueden los PVC de CCE detectar fallas de almacenamiento subyacentes?

Los PersistentVolumeClaims (PVC) de CCE se despliegan tal como están en Kubernetes. Un PVC se define como una declaración de almacenamiento y se desacopla del almacenamiento subyacente. No es responsable de detectar los detalles de almacenamiento subyacentes. Por lo tanto, los PVC de CCE no pueden detectar fallos de almacenamiento subyacentes.

Cloud Eye permite a los usuarios ver las métricas del servicio en la nube. Estas métricas están integradas en función de los atributos del servicio en la nube. Después de que los usuarios habilitan un servicio en la nube en la plataforma en la nube, Cloud Eye asocia automáticamente sus métricas integradas. Los usuarios pueden realizar un seguimiento del estado del servicio en la nube monitoreando estas métricas.

Se recomienda que los usuarios que tienen requisitos de detección de fallas de almacenamiento usen Cloud Eye para supervisar el almacenamiento subyacente y enviar notificaciones de alarma.

9 Espacio de nombres

9.1 ¿Por qué no puedo eliminar un espacio de nombres debido a un error de acceso a objetos APIService?

Síntoma

El espacio de nombres permanece en el estado de eliminación. El mensaje de error "DiscoveryFailed" aparece en el archivo YAML de **status**.

```
75 - kubeinertes
76 status:
77   phase: Terminating
78   conditions:
79     - type: NamespaceDeletionDiscoveryFailure
80       status: 'True'
81       lastTransitionTime: '2022-07-04T13:44:55Z'
82       reason: DiscoveryFailed
83       message: 'Discovery failed for some groups, 1 failing: unable to retrieve the complete list of server
84         APIs: metrics.k8s.io/v1beta1: the server is currently unable to handle the request'
85     - type: NamespaceDeletionGroupVersionParsingFailure
86       status: 'False'
```

En la figura anterior, el mensaje de error completo es "Discovery failed for some groups, 1 failing: unable to retrieve the complete list of server APIs: metrics.k8s.io/v1beta1: the server is currently unable to handle the request".

Esto indica que la eliminación del espacio de nombres se bloquea cuando kube-apiserver accede al objeto de recurso APIService de la API metrics.k8s.io/v1beta1.

Causa posible

Si existe un objeto APIService en el clúster, al eliminar el espacio de nombres se accederá primero al objeto APIService. Si el acceso falla, se bloqueará la eliminación del espacio de nombres. Además de los objetos APIService creados por usted, algunos complementos en el clúster de CCE también crean automáticamente objetos APIService, como complementos métricas-servidor y prometheus.

📖 NOTA

Para obtener más información sobre APIService, visite <https://kubernetes.io/docs/concepts/extend-kubernetes/api-extension/apiserver-aggregation/>.

Solución

Utiliza alguno de estos métodos:

- Rectifique el objeto APIService en el mensaje de error para que se pueda acceder correctamente. Si el objeto es creado por un complemento, asegúrese de que el pod de la instancia del complemento se está ejecutando correctamente.
- Elimine el objeto APIService en el mensaje de error. Si el objeto es creado por un complemento, desinstale el complemento en la página.

10 Gráfico y complemento

10.1 ¿Qué debo hacer si el complemento nginx-ingress no se instala en un clúster y permanece en el estado de creación?

Contexto

Ha adquirido y configurado un clúster de CCE y desea acceder a las aplicaciones desplegadas desde redes públicas. Actualmente, la forma más eficiente es registrar las rutas de Service de una aplicación en la entrada para permitir el acceso a la red pública.

Sin embargo, después de instalar el complemento nginx-ingress, el complemento siempre está en el estado **Creating** y el **nginx-ingress-controller** pod siempre está en el estado **Pending**.

Solución

Los recursos de memoria para el complemento nginx-ingress son limitados. Como resultado, el complemento nginx-ingress no se puede iniciar. Cancele la limitación de recursos para asegurarse de que el complemento nginx-ingress se puede iniciar correctamente.

Simulación de escena

- Paso 1** Cree un clúster con tres nodos, 2 vCPU y 4 GB de memoria para cada nodo.
- Paso 2** Instale el complemento nginx-ingress y seleccione 2 vCPU y 2 GB de memoria.
- Paso 3** La implementación de nginx-ingress se crea correctamente, pero el complemento nginx-ingress-controller no se puede instalar.

Figura 10-1 nginx-ingress-controller complemento siempre en el estado de creación

<input type="checkbox"/>	Name	Status	⌵
<input type="checkbox"/>	nginx-ingress-controller-7697b9f7...	Creating	
<input type="checkbox"/>	nginx-ingress-default-backend-7697b9f7...	Running	

Figura 10-2 El complemento nginx-ingress-controller no se instala

```
[root@k8s-zwx767800-cluster-33393-1a7ex ~]# kubectl get po -n kube-system | grep nginx
cceaddon-nginx-ingress-controller-577bc9c678-xz17d    0/1    Pending    0    27m
cceaddon-nginx-ingress-default-backend-77f6d77b6f-m5tth  1/1    Running   0    27m
```

Paso 4 Compruebe el mensaje de error. La siguiente información indica que los recursos son insuficientes.

```
status:
  phase: Pending
  conditions:
  - type: PodScheduled
    status: 'False'
    lastProbeTime: '2020-02-13T01:20:57Z'
    lastTransitionTime: '2020-02-12T08:50:21Z'
    reason: Unschedulable
    message: '0/3 nodes are available: 3 Insufficient cpu, 3 Insufficient memory.'
  qosClass: Guaranteed
```

Paso 5 Agregue un nodo con 4 vCPUs y 8 GB de memoria. Después de eso, el complemento nginx-ingress se instala correctamente.

----Fin

Causa posible

Los procesos como kubelet, kube-proxy y Docker en cada nodo están usando recursos del sistema. Como resultado, los recursos disponibles del nodo son menores que los requeridos para que el complemento nginx-ingress se instale con éxito.

Solución sugerida

Adquiera un nodo con al menos 4 vCPU y 8 GB de memoria.

10.2 ¿Qué debo hacer si existen recursos de procesos residuales debido a una versión anterior del complemento npd?

Descripción del problema

Cuando la carga de nodo es pesada, pueden existir recursos de proceso npd residuales.

Síntoma

Después de iniciar sesión con éxito en el nodo de ECS donde se ejecuta el clúster de CCE, se encuentra que existe un gran número de procesos npd.

```

paas 32763 16574 0 Oct13 ? 00:00:00 [sali] <defunct>
root 32764 16574 0 Oct23 ? 00:00:00 [suid] <defunct>
root 32765 16574 0 Oct20 ? 00:00:00 [suid] <defunct>
paas 32766 16574 0 Oct20 ? 00:00:00 [sali] <defunct>
paas 32767 16574 0 Oct13 ? 00:00:00 [grep] <defunct>
Frontend-Request-Queue-Inference-t4-gpu-2-89-44 --JF -c
-bash: fork: retry: No child processes
-bash: fork: retry: No child processes
Frontend-Request-Queue-Inference-t4-gpu-2-89-44 --JF 150f -p 16574
COMMAND PID USER FD TYPE DEVICE SIZE/OFF NODE NAME
node-prob 16574 paas cwd DIR 252,9 4096 2051 /
node-prob 16574 paas rtd DIR 252,9 4096 2051 /
node-prob 16574 paas txt REG 252,9 56274632 25180170 /var/paas/node-problem-detector/node-problem-detector
node-prob 16574 paas men REG 0,20 189651926 199508848 /run/log/Journal/6d14d648-8c64fabab6d8b1b1412959c/system@73d6fe9b5143049e3f8505736d7-000000000100a78-0005b34934459833-Journal
node-prob 16574 paas men REG 0,20 117440512 1359727660 /run/log/Journal/6d14d648-8c64fabab6d8b1b1412959c/system@73d6fe9b5143049e3f8505736d7-000000000e466-0005b27d0d55e3ca-Journal
node-prob 16574 paas men REG 0,20 117440512 1343981821 /run/log/Journal/6d14d648-8c64fabab6d8b1b1412959c/system@73d6fe9b5143049e3f8505736d7-000000000241f-0005b21cc9292123-Journal
node-prob 16574 paas men REG 0,20 117440512 1327784289 /run/log/Journal/6d14d648-8c64fabab6d8b1b1412959c/system@73d6fe9b5143049e3f8505736d7-0000000001e67-0005b33f032c44e-Journal
node-prob 16574 paas men REG 0,20 117440512 1311318304 /run/log/Journal/6d14d648-8c64fabab6d8b1b1412959c/system@73d6fe9b5143049e3f8505736d7-0000000004051f-0005b1c473e8f9c-Journal
node-prob 16574 paas men REG 0,20 189651904 1229454316 /run/log/Journal/6d14d648-8c64fabab6d8b1b1412959c/system@73d6fe9b5143049e3f8505736d7-000000000118d-0005b2c6644584-Journal
node-prob 16574 paas men REG 0,20 117440512 1277802866 /run/log/Journal/6d14d648-8c64fabab6d8b1b1412959c/system@73d6fe9b5143049e3f8505736d7-00000000003576-0005b23f1886cd-Journal
node-prob 16574 paas men REG 0,20 117440512 1261648398 /run/log/Journal/6d14d648-8c64fabab6d8b1b1412959c/system@73d6fe9b5143049e3f8505736d7-00000000007711-0005b233a745454c-Journal
node-prob 16574 paas men REG 0,20 117440512 1246413978 /run/log/Journal/6d14d648-8c64fabab6d8b1b1412959c/system@73d6fe9b5143049e3f8505736d7-0000000000a59-0005b22c8a6533-Journal
node-prob 16574 paas men REG 0,20 117440512 1227498734 /run/log/Journal/6d14d648-8c64fabab6d8b1b1412959c/system@73d6fe9b5143049e3f8505736d7-0000000000d6d-0005b219c6d6f8b0-Journal
node-prob 16574 paas men REG 0,20 189651904 1211842384 /run/log/Journal/6d14d648-8c64fabab6d8b1b1412959c/system@73d6fe9b5143049e3f8505736d7-00000000002701-0005b28d0fcd66e-Journal
node-prob 16574 paas men REG 0,20 117440512 1165718094 /run/log/Journal/6d14d648-8c64fabab6d8b1b1412959c/system@73d6fe9b5143049e3f8505736d7-00000000002687-0005b2818669f6b-Journal
node-prob 16574 paas men REG 0,20 189651904 1180118994 /run/log/Journal/6d14d648-8c64fabab6d8b1b1412959c/system@73d6fe9b5143049e3f8505736d7-0000000000fb76-0005b1f5bde08ca-Journal
node-prob 16574 paas men REG 0,20 117440512 1162470967 /run/log/Journal/6d14d648-8c64fabab6d8b1b1412959c/system@73d6fe9b5143049e3f8505736d7-0000000000ace18-0005b1e281818ab-Journal
node-prob 16574 paas men REG 0,20 189651904 1147391411 /run/log/Journal/6d14d648-8c64fabab6d8b1b1412959c/system@73d6fe9b5143049e3f8505736d7-0000000000316d-0005b1ce1862812-Journal
node-prob 16574 paas men REG 0,20 117440512 1138671264 /run/log/Journal/6d14d648-8c64fabab6d8b1b1412959c/system@73d6fe9b5143049e3f8505736d7-000000000076a5-0005b1a0518571ca-Journal
node-prob 16574 paas men REG 0,20 134217720 1250813909 /run/log/Journal/6d14d648-8c64fabab6d8b1b1412959c/system@73d6fe9b5143049e3f8505736d7-0000000001ca67-0005b33f032c44e-Journal
node-prob 16574 paas men REG 0,20 189651904 1114660888 /run/log/Journal/6d14d648-8c64fabab6d8b1b1412959c/system@73d6fe9b5143049e3f8505736d7-00000000004051f-0005b1c473e8f9c-Journal
node-prob 16574 paas men REG 0,20 134217720 1567372671 /run/log/Journal/6d14d648-8c64fabab6d8b1b1412959c/system@73d6fe9b5143049e3f8505736d7-0000000000b70f-0005b33b0549f976-Journal
node-prob 16574 paas men REG 0,20 117440512 1456897740 /run/log/Journal/6d14d648-8c64fabab6d8b1b1412959c/system@73d6fe9b5143049e3f8505736d7-0000000000202b-0005b2c6644584-Journal
node-prob 16574 paas men REG 0,20 189651904 1513839458 /run/log/Journal/6d14d648-8c64fabab6d8b1b1412959c/system@73d6fe9b5143049e3f8505736d7-0000000000734e7-0005b2f494346375-Journal

```

Solución

Actualice el complemento npd a la última versión.

Paso 1 Inicie sesión en la consola de CCE y haga clic en el clúster. En el panel de navegación, elija **Add-ons**. En la página mostrada, haga clic en **Upgrade en npd**.

NOTA

Si la versión del complemento npd es 1.13.6 o posterior, no es necesario actualizarla.

Paso 2 En la página **Specify Basic Information**, seleccione el clúster y la versión del complemento (por ejemplo, 1.13.6) y haga clic en **Next**.

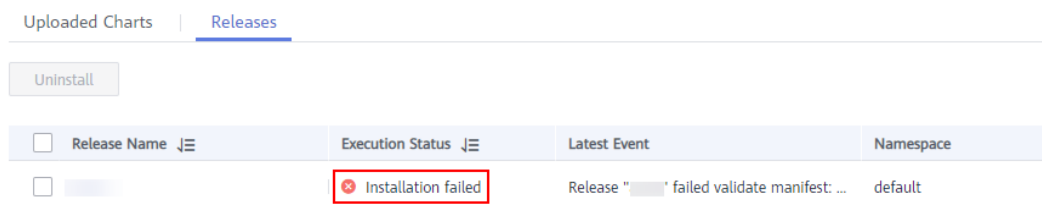
Paso 3 Haga clic en **Upgrade** para actualizar el complemento npd. Tenga en cuenta que el complemento npd no tiene parámetros configurables y puede actualizarse directamente.

----Fin

10.3 ¿Qué debo hacer si no se puede eliminar una versión de gráfico porque el formato del gráfico es incorrecto?

Síntoma

Si un gráfico cargado contiene los recursos incorrectos o incompatibles, el gráfico no se instalará.



En este caso, la versión del gráfico no puede funcionar correctamente. Es posible que no pueda eliminar la versión, se muestra el mensaje de error "deletion failed" y la versión todavía está en la interfaz gráfica de usuario.

Uploaded Charts | Releases

Uninstall

<input type="checkbox"/>	Release Name	Execution Status	Latest Event	Namespace
<input type="checkbox"/>		Installation failed	deletion failed with 1 error(s): unable to d	default

Solución

En este caso, puede ejecutar los comandos kubectl para eliminar la versión.

Durante la instalación del gráfico, es posible que algunos recursos especificados en el gráfico se hayan creado correctamente. Primero debe eliminar manualmente estos recursos. Después de eliminar los recursos residuales, debe eliminar la instancia del gráfico.

Para una versión de gráfico Helm v2, consulte el ConfigMap correspondiente a la versión de gráfico en el espacio de nombres del sistema kube. Por ejemplo:

```
[paas@192-168-0-40 ~]$ kubectl -n kube-system get cm
NAME                               DATA  AGE
9a37566a.cce.io                    0      25d
aosredis.v1                         1      55s
cceaddon-coredns.v1                 1      25d
cceaddon-everest.v1                 1      17d
cceaddon-metrics-server.v1         1      25d
cceaddon-npd-custom-config          0      25d
cceaddon-npd.v1                     1      25d
cceaddon-prometheus.v1              1      25h
cluster-autoscaler-status           1      8d
cluster-versions                    1      25d
coredns                             1      25d
extension-apiserver-authentication  6      25d
ingress-controller-leader-nginx     0      22d
[paas@192-168-0-40 ~]$
```

Después de eliminar el ConfigMap, la versión del gráfico se elimina correctamente.

```
[paas@192-168-0-40 ~]$ kubectl -n kube-system delete cm aosredis.v1
configmap "aosredis.v1" deleted
[paas@192-168-0-40 ~]$
```

Para una versión de gráfico Helm v3, consulte el Secret correspondiente a la versión de gráfico en el espacio de nombres. Por ejemplo:

```
[root@cce-1717-vpc-node2 ~]# kubectl -n default get secret
NAME                               TYPE                               DATA  AGE
default-secret                     kubernetes.io/dockerconfigjson    1      21h
default-token-978pv                kubernetes.io/service-account-token 3      21h
paas.elb                            cfe/secure-opaque                 3      21h
sh.helm.release.v1.test-nginx.v1   helm.sh/release.v1                 1      139m
[root@cce-1717-vpc-node2 ~]#
```

Después de eliminar el Secret, la versión del gráfico se elimina correctamente.

```
[root@cce-1717-vpc-node2 ~]# kubectl -n default delete secret sh.helm.release.v1.test-nginx.v1
secret "sh.helm.release.v1.test-nginx.v1" deleted
[root@cce-1717-vpc-node2 ~]#
```

Nota: Si realiza operaciones en la consola, CCE cambia automáticamente la versión original del gráfico v2 a v3 cuando obtiene o actualiza la versión del gráfico. La información de liberación se almacena en el Secret. La información de la versión en el ConfigMap original no

se elimina. Se recomienda consultar y eliminar la versión del gráfico tanto en ConfigMap como en Secret.

10.4 ¿CCE soporta nginx-ingress?

Introducción a nginx-ingress

nginx-ingress es un controlador de entrada popular. Funciona como un proxy inverso para importar tráfico externo a un clúster y exponer Services en clústeres de Kubernetes a los sistemas externos. En el balanceo de carga de capa 7 (entrada), los nombres de dominio se utilizan para coincidir con los servicios. De esta manera, se puede acceder a los servicios de un clúster con nombres de dominio.

Este gráfico está compuesto por ingress-controller y nginx.

- ingress-controller monitorea las entradas de Kubernetes y actualiza las configuraciones de nginx.

📖 NOTA

Para obtener más información sobre las entradas, consulte <https://kubernetes.io/docs/concepts/services-networking/ingress/>.

- nginx implementa el balanceo de carga para solicitudes y soporta el reenvío de solicitudes de capa 7.

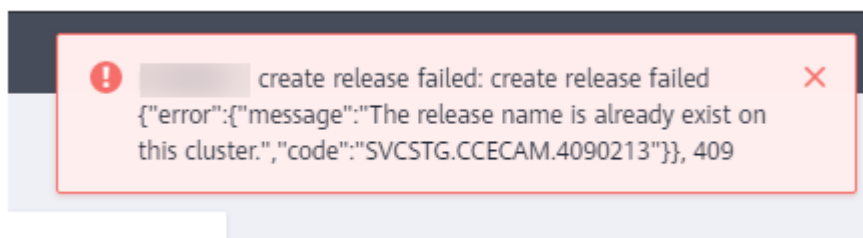
Método de instalación

Puede instalar el complemento nginx-ingress en la página **Add-ons** de la consola de CCE y configurar sus parámetros.

10.5 ¿Por qué falla la instalación del complemento y avisa "The release name is already exist"?

Síntoma

Cuando un complemento no se instala, se devuelve el mensaje de error "The release name is already exist".



Causa posible

El registro de la versión del complemento permanece en el clúster de Kubernetes. Generalmente, se debe a que el clúster etcd ha realizado una copia de respaldo y restaurado el complemento, o no se puede instalar o eliminar el complemento.

Solución

Utilice kubectl para conectarse al clúster y borre manualmente el Secret y Configmap correspondiente a la versión adicional. A continuación se utiliza la versión de complemento de autoescalador como ejemplo.

- Paso 1** Conéctese al clúster mediante kubectl y ejecute el siguiente comando para ver la lista secreta de versiones de complementos:

kubectl get secret -nkube-system |grep cceaddon

```
[root@cce-123-vpc-node2 ~]# kubectl get secret -nkube-system |grep cceaddon
sh.helm.release.v1.cceaddon-autoscaler.v1    helm.sh/release.v1    1    61s
sh.helm.release.v1.cceaddon-autoscaler.v2    helm.sh/release.v1    1    47s
sh.helm.release.v1.cceaddon-coredns.v1      helm.sh/release.v1    1    6h2m
sh.helm.release.v1.cceaddon-everest.v1      helm.sh/release.v1    1    6h2m
[root@cce-123-vpc-node2 ~]#
```

El nombre secreto de una versión adicional tiene el formato de **sh.helm.release.v1.cceaddon-{add-on name}.v***. Si hay varias versiones de lanzamiento, puede eliminar sus secretos al mismo tiempo.

- Paso 2** Ejecute el comando **release secret** para eliminar los secretos.

Por ejemplo:

**kubectl delete secret sh.helm.release.v1.cceaddon-autoscaler.v1
sh.helm.release.v1.cceaddon-autoscaler.v2 -nkube-system**

```
[root@cce-123-vpc-node2 ~]# kubectl delete secret sh.helm.release.v1.cceaddon-autoscaler.v1 sh.helm.release.v1.cceaddon-autoscaler.v2 -nkube-system
secret "sh.helm.release.v1.cceaddon-autoscaler.v1" deleted
secret "sh.helm.release.v1.cceaddon-autoscaler.v2" deleted
[root@cce-123-vpc-node2 ~]#
```

- Paso 3** Si el complemento se crea cuando se utiliza Helm v2, CCE cambia automáticamente la versión v2 en Configmaps a la versión v3 en Secrets al ver los complementos y sus detalles. La versión v2 del Configmap original no se elimina. Ejecute el siguiente comando para ver la lista ConfigMap de versiones de complementos:

kubectl get configmap -nkube-system | grep cceaddon

```
cluster-autoscaler-th-config    1    7d10h
[paas@192-168-0-64 ~]# kubectl get configmap -nkube-system | grep cceaddon
cceaddon-autoscaler.v1          1    7d10h
cceaddon-autoscaler.v2          1    52m
cceaddon-coredns.v1             1    14d
cceaddon-everest.v1             1    14d
[paas@192-168-0-64 ~]#
```

El nombre de ConfigMap de una versión adicional tiene el formato de **cceaddon-{add-on name}.v***. Si hay varias versiones de lanzamiento, puede eliminar sus ConfigMaps al mismo tiempo.

- Paso 4** Ejecute el comando **release configmap** para eliminar el ConfigMaps.

Por ejemplo:

kubectl delete configmap cceaddon-autoscaler.v1 cceaddon-autoscaler.v2 -nkube-system

```
[paas@192-168-0-64 ~]# kubectl delete configmap cceaddon-autoscaler.v1 cceaddon-autoscaler.v2 -nkube-system
configmap "cceaddon-autoscaler.v1" deleted
configmap "cceaddon-autoscaler.v2" deleted
[paas@192-168-0-64 ~]#
```

⚠ ATENCIÓN

Elimine los recursos en kube-system es una operación de alto riesgo. Asegúrese de que el comando es correcto antes de ejecutarlo para evitar que los recursos se eliminen por error.

Paso 5 En la consola de CCE, instale el complemento y, a continuación, desinstálelo. Asegúrese de que los recursos adicionales residuales están borrados. Una vez completada la desinstalación, vuelva a instalar el complemento.

📖 NOTA

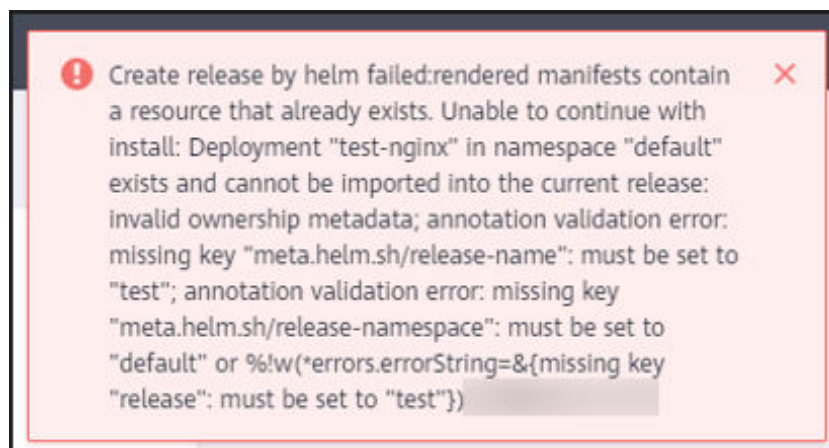
Al instalar el complemento por primera vez, es posible que se encuentre anormal después de la instalación debido a los recursos residuales de la versión anterior del complemento, que es normal. En este caso, puede desinstalar el complemento en la consola para asegurarse de que los recursos residuales se borran y el complemento puede ejecutarse correctamente después de volver a instalarlo.

---Fin

10.6 ¿Por qué falla la creación o la actualización de la versión y avisa "rendered manifests contain a resource that already exists"?

Síntoma

Cuando no se puede crear o actualizar una versión, se muestra el mensaje de error "Create release by helm failed:rendered manifests contain a resource that already exists. Unable to continue with install: ..., label validation error:missing key \"app.kubernetes.io/managed-by\":must be set to\"Helm\" ... Failed to create the release."



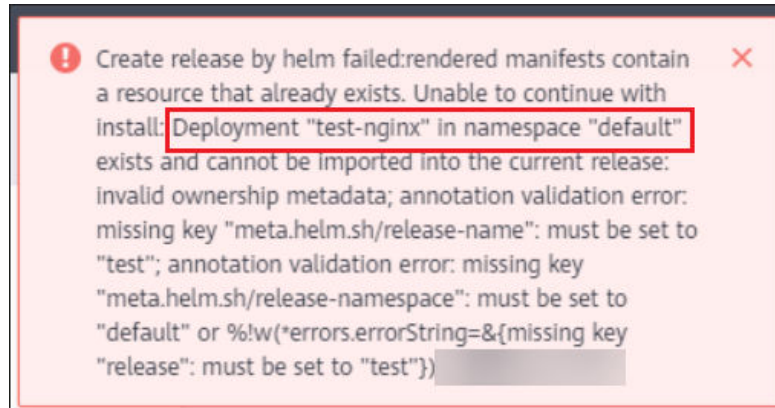
Causa posible

Si se muestra la información de error anterior, la versión no se crea con Helm v3. Si existe una versión con el mismo nombre en el entorno y no tiene la etiqueta de inicio **app.kubernetes.io/managed-by: Helm** de Helm v3, se muestra un mensaje de conflicto.

Solución

Elimine la versión y créela de nuevo usando Helm.

- Paso 1** Compruebe el mensaje de error y busque la versión que causa el conflicto. Preste atención a la información siguiente **Unable to continue with install:**. Por ejemplo, el siguiente mensaje de error indica que se produce un conflicto en la Deployment **test-nginx** en el espacio de nombres **default**.



- Paso 2** Vaya a la consola del clúster o ejecute el siguiente comando kubectl para eliminar la Deployment **test-nginx**. La información anterior es solo un ejemplo. Realice operaciones de acuerdo con la información de error real.

```
kubectl delete deploy test-nginx -n default
```

- Paso 3** Una vez resuelto el conflicto, vuelva a instalar el gráfico.

----Fin

11 API y preguntas frecuentes de kubectl

11.1 ¿Cómo puedo acceder a un clúster de CCE?

Hay dos modos para acceder a un clúster:

- Modo 1: Gateway de la API
Este modo utiliza la autenticación de token. Necesita usar su cuenta para obtener el token.
- Modo 2: API de clúster
Este modo utiliza la autenticación de certificado.

11.2 ¿Se pueden mostrar los recursos creados con las API o kubectl en la consola de CCE?

La consola de CCE no admite la visualización de los siguientes recursos de Kubernetes: DaemonSets, ReplicationControllers, ReplicaSets y puntos de conexión.

Para consultar estos recursos, ejecute los comandos kubectl.

Además, Deployments, StatefulSets, Services solo se pueden mostrar en la consola si se cumplen las siguientes condiciones:

- Deployments y StatefulSets: al menos una etiqueta utiliza **app** como clave.
- Pods: Los pods se muestran en la página de ficha **Pods** en los detalles de la carga de trabajo solo después de que se haya creado una implementación o un StatefulSet.
- Services: Los Services se muestran en la página de ficha **Access Mode** en los detalles de Deployment o StatefulSet.

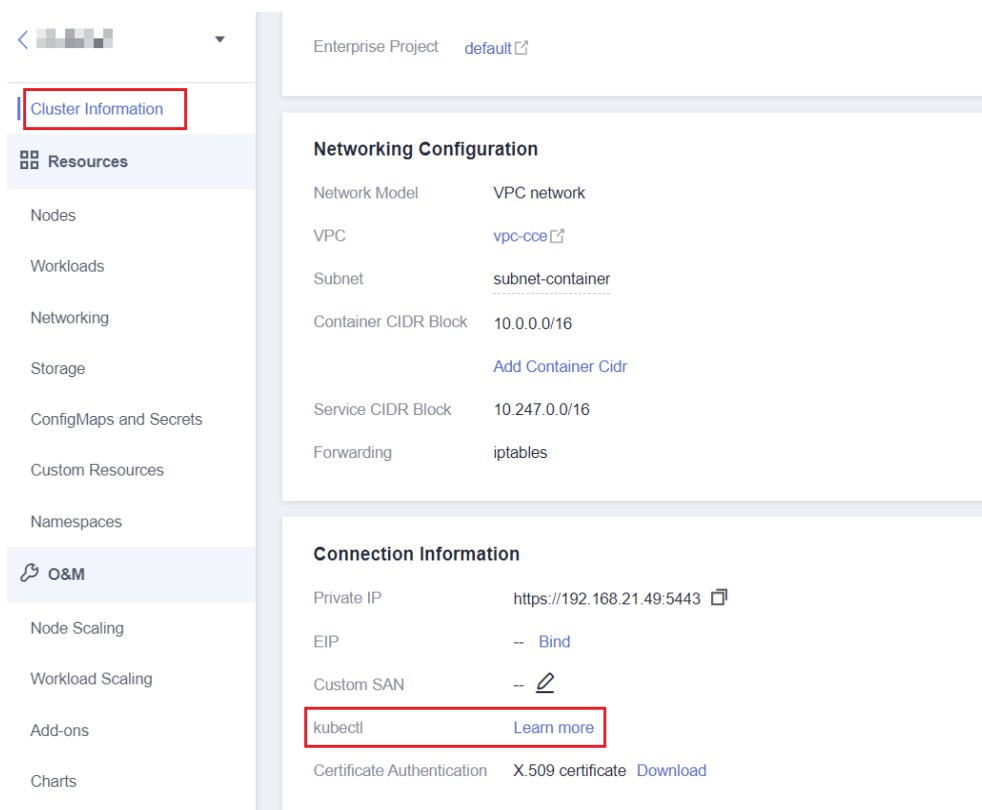
Los Services que se muestran en esta página de fichas están asociados a la carga de trabajo.

- a. Al arrendar, una etiqueta de la carga de trabajo utiliza **app** como clave.
- b. La etiqueta de un Service es la misma que la de la carga de trabajo.

11.3 ¿Cómo descargo kubeconfig para conectarme a un clúster usando kubectl?

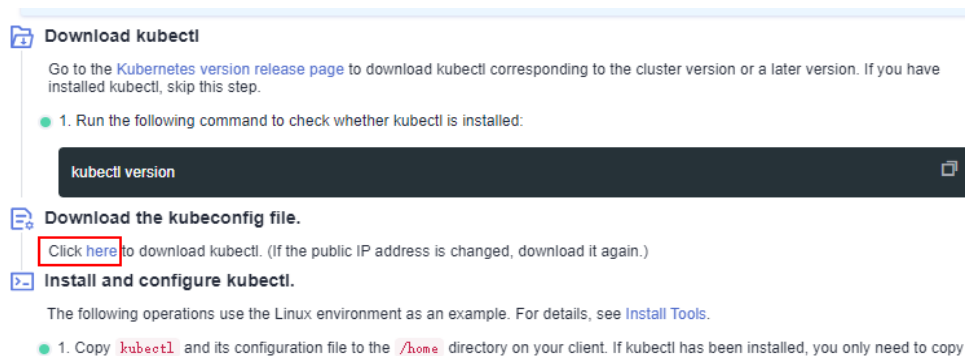
Paso 1 Inicie sesión en la consola de CCE. Haga clic en el clúster de destino para ir a su página de detalles.

Paso 2 En el área **Connection Information**, vea el modo de conexión de kubectl.



Paso 3 En la ventana que se muestra, descargue el archivo de configuración de kubectl (**kubeconfig.json**).

Figura 11-1 Descarga de kubeconfig.json



----Fin

11.4 ¿Cómo puedo rectificar el error notificado al ejecutar el comando kubectl top node?

Síntoma

El mensaje de error "Error from server (ServiceUnavailable): the server is currently unable to handle the request (get nodes.metrics.k8s.io)" aparece después de ejecutar el comando **kubectl top node**.

Causas posibles

"Error from server (ServiceUnavailable)" indica que el clúster no está conectado. En este caso, debe comprobar si la red entre kubectl y el nodo principal en el clúster es normal.

Solución

- Si el comando kubectl se ejecuta fuera del clúster, compruebe si el clúster está enlazado a una EIP. Si es así, descargue el archivo **kubeconfig** y ejecute de nuevo el comando kubectl.
- Si el comando kubectl se ejecuta en un nodo del clúster, compruebe el grupo de seguridad del nodo y compruebe si se permite la comunicación TCP/UDP entre el nodo de trabajo y el nodo principal. Para obtener más información sobre el grupo de seguridad, consulte [Configuración de reglas de grupo de seguridad de clúster](#).

11.5 ¿Por qué se muestra "Error from server (Forbidden)" cuando utilizo kubectl?

Síntoma

Cuando usa kubectl para crear o consultar recursos de Kubernetes, se devuelve el siguiente resultado:

```
# kubectl get deploy Error from server (Forbidden): deployments.apps is forbidden: User "0c97ac3cb280f4d91fa7c0096739e1f8" cannot list resource "deployments" in API group "apps" in the namespace "default"
```

Causa posible

Este usuario no tiene permisos para utilizar los recursos de Kubernetes.

Solución

Asigne permisos al usuario.

Paso 1 Log in to the CCE console. In the navigation pane, choose **Permissions**.

Paso 2 Select a cluster for which you want to add permissions from the drop-down list on the right.

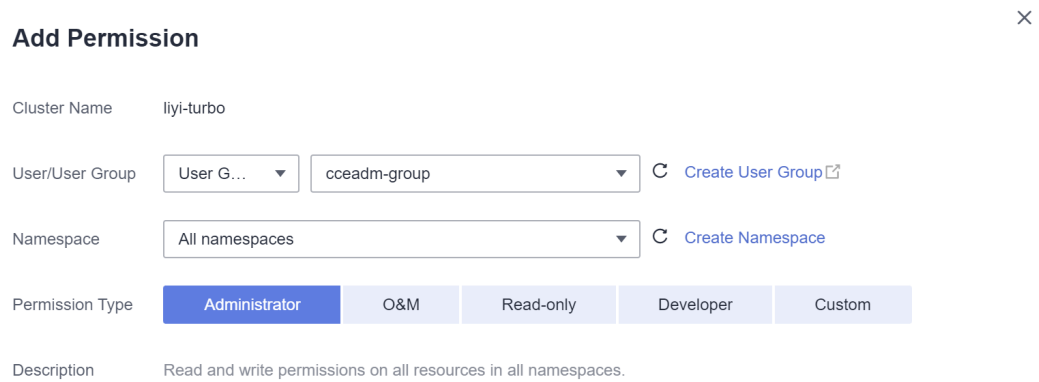
Paso 3 Click **Add Permissions** in the upper right corner.

Paso 4 Confirm the cluster name and select the namespace to assign permissions for. For example, select **All namespaces**, the target user or user group, and select the permissions.

NOTA

If you do not have IAM permissions, you cannot select users or user groups when configuring permissions for other users or user groups. In this case, you can enter a user ID or user group ID.

Figura 11-2 Configuring namespace permissions



Add Permission ×

Cluster Name: liyi-turbo

User/User Group: User G... [Create User Group](#)

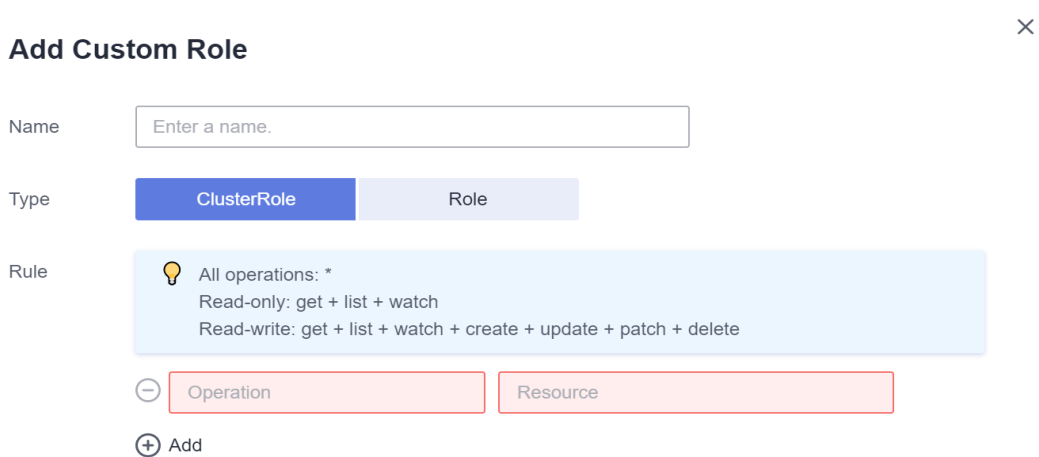
Namespace: All namespaces [Create Namespace](#)

Permission Type: **Administrator** | O&M | Read-only | Developer | Custom

Description: Read and write permissions on all resources in all namespaces.

Permissions can be customized as required. After selecting **Custom** for **Permission Type**, click **Add Custom Role** on the right of the **Custom** parameter. In the dialog box displayed, enter a name and select a rule. After the custom rule is created, you can select a value from the **Custom** drop-down list box.

Figura 11-3 Custom permission



Add Custom Role ×

Name:

Type: **ClusterRole** | Role

Rule: 💡 All operations: *
Read-only: get + list + watch
Read-write: get + list + watch + create + update + patch + delete

Paso 5 Click **Create**.

---Fin

12 Preguntas frecuentes sobre DNS

12.1 ¿Qué debo hacer si falla la resolución de nombres de dominio?

Concepto de comprobación 1: Si el complemento coredns ha sido instalado

- Paso 1** Inicie sesión en la consola de CCE y haga clic en el clúster.
- Paso 2** En el panel de navegación, elija **Add-ons**. En el área **Add-ons Installed**, compruebe si se ha instalado el complemento coredns.
- Paso 3** Si no es así, instale el complemento. Para obtener más información, véase [¿Por qué un contenedor en un clúster de CCE no puede realizar la resolución de DNS?](#).

----Fin

Concepto de comprobación 2: Si la instancia coredns alcanza el límite de rendimiento

CoreDNS QPS se correlaciona positivamente con el uso de la CPU. Si el QPS es alto, ajuste las especificaciones de instancia de coredns basadas en el QPS. Si un clúster tiene más de 100 nodos, se recomienda utilizar NodeLocal DNSCache para mejorar el rendimiento de DNS. Para obtener más información, consulte [Uso de NodeLocal DNSCache para mejorar el rendimiento de DNS](#).

- Paso 1** Inicie sesión en la consola de CCE y acceda a la consola del clúster.
- Paso 2** En el panel de navegación de la izquierda, elija **Add-ons**. En **Add-ons Installed**, busca el complemento coredns correspondiente al clúster y asegúrate de que el estado del complemento sea **Running**.
- Paso 3** Haga clic en el nombre del complemento de coredns para ver la lista de complementos.
- Paso 4** Haga clic en **Monitor** del complemento coredns para ver el uso de CPU y memoria.

Si el rendimiento del complemento alcanza el cuello de botella, ajuste las especificaciones del complemento coredns.

1. En el área **Add-ons Installed**, busque la fila que contiene el complemento coredns y haga clic en **Edit**. Se muestra la página de detalles del complemento.
2. En el área **Specifications**, configure el complemento coredns. Puede utilizar el QPS CoreDNS según sea necesario.
3. También puede seleccionar **Custom qps** y establecer el número de pods, la cuota de CPU y la cuota de memoria.

Specifications

Add-on Specifications

2500 qps	5000 qps	10000 qps	20000 qps	Custom qps
----------	----------	-----------	-----------	-------------------

Pods

— 4 +

Containers

coredns

CPU Quota

Request Limit

Memory Quota

Request Limit

- The request value must be less than or equal to the limit value, otherwise it cannot be created successfully.
- Please ensure that the node resources under the cluster are sufficient, otherwise it cannot be created successfully.

4. Haga clic en **OK**.

----Fin

Concepto de comprobación 3: Si la resolución de nombres de dominio externo es lenta o se agota

Si la tasa de errores de resolución de nombres de dominio es inferior a 1/10000, optimice los parámetros haciendo referencia a [¿Cómo puedo optimizar la configuración si la resolución del nombre de dominio externo es lenta o se agota?](#) o agregue una política de reintento en el servicio.

Concepto de comprobación 4: Si ocurre UnknownHostException

Cuando las solicitudes de servicio en el clúster se envían a un servidor DNS externo, se produce un error de resolución de nombres de dominio debido a UnknownHostException ocasionales. UnknownHostException es una excepción común. Cuando se produzca esta excepción, compruebe si hay algún error relacionado con el nombre de dominio o si ha introducido un nombre de dominio correcto.

Para localizar la falla, efectúe los siguientes pasos:

- Paso 1** Compruebe el nombre del host cuidadosamente (ortografía y espacios adicionales).
- Paso 2** Compruebe la configuración de DNS. Antes de ejecutar la aplicación, ejecute el comando **ping hostname** para asegurarse de que el servidor de DNS se ha iniciado y se ha ejecutado. Si el nombre de host es nuevo, debe esperar un período de tiempo antes de acceder al servidor DNS.
- Paso 3** Compruebe el uso de CPU y memoria del complemento coredns para determinar si se ha alcanzado el cuello de botella de rendimiento. Para obtener más información, véase [Concepto de comprobación 2: Si la instancia coredns alcanza el límite de rendimiento](#).
- Paso 4** Compruebe si la limitación de tráfico se realiza en el complemento coredns. Si se activa la limitación de tráfico, el tiempo de procesamiento de algunas solicitudes puede prolongarse. En este caso, es necesario ajustar las especificaciones del complemento coredns.

Inicie sesión en el nodo donde está instalado el complemento coredns y vea el siguiente contenido:

```
cat /sys/fs/cgroup/cpu/kubepods/pod<pod_uid>/<coredns container ID>/cpu.stat
```

- `<pod uid>` indica el UID de pod del complemento coredns, que se puede obtener ejecutando el siguiente comando:

```
kubectl get po <pod name> -nkube-system -ojsonpath='{.metadata.uid}{"\n"}'
```

En el comando anterior `<pod name>` indica el nombre del complemento coredns que se ejecuta en el nodo actual.

- `<coredns contenedor ID>` debe ser un ID de contenedor completo, que se puede obtener ejecutando el siguiente comando:

```
docker ps --no-trunc | grep k8s_coredns | awk '{print $1}'
```

Ejemplo:

```
cat /sys/fs/cgroup/cpu/kubepods/  
pod27f58662-3979-448e-8f57-09b62bd24ea6/6aa98c323f43d689ac47190bc84cf4fadd23bd8dd2  
5307f773df25003ef0eef0/cpu.stat
```

Preste atención a las siguientes métricas:

- **nr_throttled**: número de veces que el tráfico es limitado.
- **throttled_time**: duración total de la limitación de tráfico, en nanosegundos.

---Fin

Si el nombre de host y la configuración DNS son correctas, puede utilizar las siguientes políticas de optimización.

Políticas de optimización:

1. Cambie el tiempo de caché de coredns.
2. Configure el dominio stub.
3. Modifique el valor de **ndots**.

NOTA

- **Increasing the cache time of coredns** ayuda a resolver el mismo nombre de dominio durante el tiempo N, reduciendo el número de solicitudes DNS en cascada.
- **Configuring the stub domain** puede reducir el número de enlaces de solicitud DNS.

Cómo modificar:

1. Modifique el tiempo de caché de coredns y configure el dominio stub:

Configuración del dominio Stub para CoreDNS

Reinicie el complemento coredns después de modificar las configuraciones.

2. Modificación de **ndots**:

¿Cómo puedo optimizar la configuración si la resolución del nombre de dominio externo es lenta o se agota?

Ejemplo:

```
dnsConfig:  
  options:  
    - name: timeout  
      value: '2'  
    - name: ndots  
      value: '5'  
    - name: single-request-reopen
```

Se recomienda cambiar el valor de **ndots** a **2**.

12.2 ¿Por qué un contenedor en un clúster de CCE no puede realizar la resolución de DNS?

Síntoma

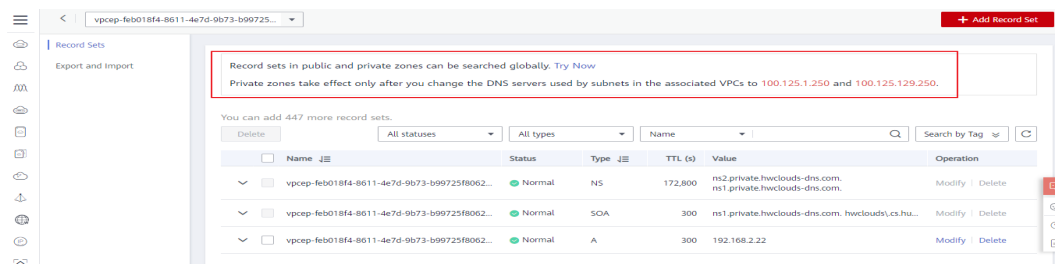
Un cliente vincula su nombre de dominio a los nombres de dominio privados del servicio DNS y también a una VPC específica. Se encuentra que los ECS en la VPC pueden resolver correctamente el nombre de dominio privado, pero los contenedores en la VPC no pueden.

Escenario de aplicación

Los contenedores de una VPC no pueden resolver los nombres de dominio.

Solución

De acuerdo con las reglas de resolución de nombres de dominio privados, el DNS de subred en la VPC debe establecerse en el DNS en la nube. Puede encontrar los detalles del servicio DNS de red privada en su consola.



El cliente puede realizar la resolución de nombres de dominio en los ECS de la subred de VPC, lo que indica que la configuración anterior se ha completado en la subred.

```
bash-4.4# exit
exit
[root@global-skyworth1-vpn ~]# ping [redacted]
PING [redacted] (10.247.11.29) 56(84) bytes of data.
```

Sin embargo, cuando la resolución del nombre de dominio se realiza en un contenedor, se muestra el mensaje "bad address", que indica que el nombre de dominio no se puede resolver.

```
[root@global-skyworth1-vpn ~]#
[root@global-skyworth1-vpn ~]# docker exec -it 86cf062a5ba3 bash
bash-4.4# ping [redacted]
ping: bad address '[redacted]'
bash-4.4#
```

Inicie sesión en la consola de CCE y compruebe los complementos instalados en el clúster.

Si encuentra que el complemento coredns no existe en **Add-ons Installed**, es posible que el complemento coredns se haya desinstalado incorrectamente.

Instálelo y agregue el nombre de dominio correspondiente y la dirección de servicio de DNS para resolver el nombre de dominio.

12.3 ¿Por qué no se puede resolver el nombre de dominio de la zona del tenant después de modificar la configuración de DNS de la subred?

Síntoma

Después de agregar un registro de servidor de DNS, por ejemplo, 114.114.114.114, a la configuración de DNS de la subred del clúster de usuarios, no se puede resolver el nombre de dominio de la zona del tenant.

Análisis de las causas

CCE configura la información DNS de subred del usuario en el nodo, que también es utilizada por el complemento `coredns`. Como resultado, el nombre de dominio no puede ser resuelto por el contenedor de nodo ocasionalmente.

Solución

Se recomienda modificar el dominio `stub` del complemento `coredns` para actualizar la configuración DNS de la subred del clúster de usuarios. Para obtener más información, consulte [Configuración del dominio Stub para CoreDNS](#).

12.4 ¿Cómo puedo optimizar la configuración si la resolución del nombre de dominio externo es lenta o se agota?

A continuación se muestra un archivo `resolv.conf` de ejemplo para un contenedor en una carga de trabajo:

```
root@test-5dffdddf95-vpt4m:/# cat /etc/resolv.conf
nameserver 10.247.3.10
search istio.svc.cluster.local svc.cluster.local cluster.local
options ndots:5 single-request-reopen timeout:2
```

En la información anterior:

- **nameserver**: dirección IP del DNS. Establezca este parámetro en la dirección IP del clúster de CoreDNS.
- **search**: lista de búsqueda de nombres de dominio, que es un sufijo común de Kubernetes.
- **ndots**: Si el número de puntos (.) es menor que el nombre de dominio, se utiliza preferentemente **search** para la resolución.
- **timeout**: intervalo de tiempo de espera.
- **single-request-reopen**: indica que se utilizan diferentes puertos de origen para enviar diferentes tipos de solicitudes.

De forma predeterminada, cuando se crea una carga de trabajo en la consola de CCE, los parámetros anteriores se configuran de la siguiente manera:

```
dnsConfig:
  options:
    - name: timeout
      value: '2'
    - name: ndots
      value: '5'
    - name: single-request-reopen
```

Estos parámetros pueden ser optimizados o modificados en función de los requisitos de servicio.

Escenario 1: Resolución lenta de nombres de dominio externo

Solución de optimización

1. Si la carga de trabajo no necesita acceder al servicio de Kubernetes en el clúster, consulte [¿Cómo configuro una política de DNS para un contenedor?](#).
2. Si el número de puntos (.) en el nombre de dominio utilizado por el servicio en funcionamiento para acceder a otros servicios de Kubernetes es menor que 2, establezca **ndots** en 2.

Escenario 2: Tiempo de espera de resolución de nombres de dominio externos

Solución de optimización

1. Generalmente, el tiempo de espera de un servicio debe ser mayor que el valor de **timeout** multiplicado por **attempts**.
2. Si se necesitan más de 2 segundos para resolver el nombre de dominio, puede establecer **timeout** en un valor mayor.

12.5 ¿Cómo configuro una política de DNS para un contenedor?

CCE utiliza **dnsPolicy** para identificar diferentes políticas de DNS para cada pod. El valor de **dnsPolicy** puede ser uno de los siguientes:

- **None:** No hay ninguna política de DNS configurada. En este modo, puede personalizar la configuración de DNS, y **dnsPolicy** debe usarse junto con **dnsConfig** para personalizar el DNS.
- **Default:** El pod hereda la configuración de resolución de nombres del nodo donde se está ejecutando el pod. El archivo de configuración de DNS del contenedor es el archivo de configuración de DNS al que apunta el indicador **--resolv-conf** del kubelet. En este caso, se utiliza un DNS en la nube para los clústeres de CCE.
- **ClusterFirst:** En este modo, el DNS en el pod utiliza el servicio DNS configurado en el clúster. Es decir, el servicio kube-dns o CoreDNS en Kubernetes se utiliza para la resolución de nombres de dominio. Si la resolución falla, se utiliza la configuración de DNS de la máquina host para la resolución.

Si no se especifica el tipo de **dnsPolicy**, se utiliza **ClusterFirst** de forma predeterminada.

- Si el tipo de **dnsPolicy** se establece en **Default**, la configuración de resolución de nombres se hereda del nodo de trabajo donde se está ejecutando el pod.

- Si el tipo de dnsPolicy se establece en **ClusterFirst**, las consultas de DNS se enviarán al servicio kube-dns.

El servicio kube-dns responde a consultas en los dominios que usan el sufijo de dominio de clúster configurado como raíz. Todas las demás consultas (por ejemplo, www.kubernetes.io) se reenvían al servidor de nombres ascendente heredado del nodo. Antes de que esta característica fuera compatible, los dominios stub eran típicamente introducidos por un resolutor personalizado, en lugar del DNS ascendente. Sin embargo, esto hace que el propio solucionador personalizado sea la ruta clave para la resolución DNS, donde los problemas de escalabilidad y disponibilidad pueden hacer que las funciones DNS no estén disponibles para el clúster. Esta función le permite introducir resolutores personalizados sin tener en cuenta toda la ruta de resolución.

Si una carga de trabajo no necesita usar CoreDNS en el clúster, puede usar kubectl o invocar a las API para establecer dnsPolicy en Default.

13 Preguntas frecuentes sobre el repositorio de imágenes

13.1 ¿Cómo puedo crear una imagen de Docker y resolver el problema de la extracción lenta de imágenes?

Creación de una imagen de Docker

Para obtener más información sobre cómo utilizar Dockerfile a personalizar una imagen Docker para una aplicación web sencilla, consulte [Básicos de Docker](#) o [¿Cómo creo una imagen de Docker?](#).

Acelerar la extracción de la imagen

Las imágenes públicas pueden extraerse lentamente debido a la red portadora. Puede cargar imágenes de uso frecuente en SWR para mejorar la velocidad de extracción de imágenes.

Introducción a SWR

SWR proporciona una gestión de imágenes de contenedores de ciclo de vida completo, que es fácil de usar, segura y confiable. SWR permite a los usuarios desplegar rápidamente servicios en contenedores. SWR se puede utilizar como un repositorio de imágenes para almacenar y gestionar imágenes de Docker.

Preguntas frecuentes de SWR

[Preguntas frecuentes generales](#)

13.2 ¿Cómo subo mis imágenes a CCE?

SoftWare Repository for Container (SWR) gestiona imágenes para CCE. Proporciona las siguientes formas de subir imágenes:

- [Carga de una imagen a través de un cliente de Motor de contenedores](#)
- [Carga de una imagen con la consola de SWR](#)

Para obtener más información sobre cómo migrar sin problemas de Harbor a SWR, consulte [Sincronización de imágenes entre las nubes de Harbor a SWR](#).

14 Permisos

14.1 ¿Puedo configurar solo los permisos de espacio de nombres sin permisos de gestión de clústeres?

Los permisos de espacio de nombres y los permisos de gestión de clústeres son independientes y complementarios entre sí.

- Permisos de espacio de nombres: se aplican a clústeres y se utilizan para gestionar operaciones en recursos de clústeres (como la creación de cargas de trabajo).
- Permisos de gestión de clústeres (IAM): se aplican a servicios en la nube y se utilizan para gestionar clústeres de CCE y recursos periféricos (como VPC, ELB y ECS).

Los administradores del grupo de usuarios de IAM Admin pueden conceder permisos de gestión de clústeres (como CCE Administrator y CCE FullAccess) a los usuarios de IAM o conceder permisos de espacio de nombres en un clúster en la consola de CCE. Sin embargo, los permisos que tiene en la consola de CCE están determinados por la política del sistema de IAM. Si los permisos de gestión del clúster no están configurados, no tiene los permisos para acceder a la consola de CCE.

Si solo ejecuta comandos de kubectl para trabajar en recursos de clúster, solo necesita obtener el archivo de kubeconfig con los permisos de espacio de nombres. Para obtener más información, véase [¿Puedo usar kubectl si los permisos de gestión de clústeres no están configurados?](#). Tenga en cuenta que la fuga de información puede ocurrir cuando se utiliza el archivo kubeconfig.

14.2 ¿Puedo usar las API de CCE si los permisos de gestión de clústeres no están configurados?

CCE tiene las API de servicios en la nube y las API de clúster.

- API de servicios en la nube: puede realizar operaciones en la infraestructura (como la creación de nodos) y recursos de clúster (como la creación de cargas de trabajo).

Cuando se usan API de servicios en la nube, se deben configurar los permisos de gestión de clústeres (IAM).

- API de clúster: puede realizar operaciones en recursos de clúster (como la creación de cargas de trabajo) a través del servidor de API nativo de Kubernetes, pero no en recursos de infraestructura de nube (como la creación de nodos).

Cuando utilice las API de clúster, solo tendrá que agregar el certificado de clúster. Solo los usuarios con los permisos de gestión de clúster (IAM) pueden [descargar](#) el certificado de clúster. Obsérvese que puede producirse una fuga de información durante la transmisión del certificado.

14.3 ¿Puedo usar kubectl si los permisos de gestión de clústeres no están configurados?

No se requiere autenticación de IAM para ejecutar comandos de kubectl. Por lo tanto, puede ejecutar los comandos de kubectl sin configurar los permisos de gestión de clústeres (IAM). Sin embargo, necesita obtener el archivo de configuración de kubectl (kubeconfig) con los permisos de espacio de nombres. En los siguientes escenarios, puede producirse una fuga de información durante la transmisión de archivos.

- Escenario 1
Si un usuario de IAM se ha configurado con los permisos de gestión de clústeres y los permisos de espacio de nombres, descarga el archivo de autenticación de kubeconfig y, a continuación, elimina los permisos de gestión de clústeres (reservando los permisos de espacio de nombres), kubectl aún se puede utilizar para realizar operaciones en clústeres de Kubernetes. Por lo tanto, si desea eliminar permanentemente el permiso de un usuario, también debe eliminar los permisos de gestión de clústeres y los permisos de espacio de nombres del usuario.
- Escenario 2
Un usuario de IAM tiene ciertos permisos de gestión de clúster y espacio de nombres y descarga el archivo de autenticación de kubeconfig. En este caso, CCE determina a qué recursos de Kubernetes puede acceder kubectl basándose en la información del usuario. Es decir, la información de autenticación de un usuario se registra en kubeconfig. Cualquiera puede usar kubeconfig para acceder al clúster.

15 Referencia

15.1 ¿Cómo puedo ampliar la capacidad de almacenamiento de un contenedor?

Escenario

El tamaño de almacenamiento predeterminado de un contenedor es 10 GB. Si se genera un gran volumen de datos en el contenedor, amplíe la capacidad utilizando el método descrito en este tema.

Solución

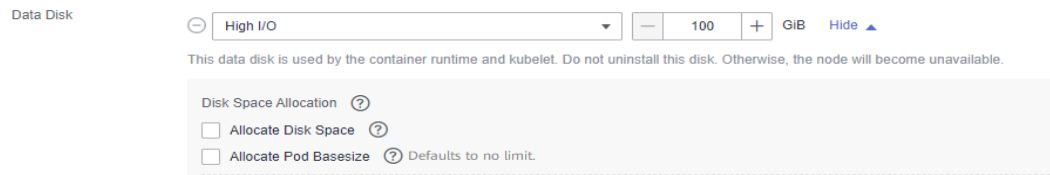
- Paso 1** Inicie sesión en la consola de CCE y haga clic en el nombre del clúster de destino en la lista de clústeres.
- Paso 2** Elija **Nodes** en el panel de navegación.
- Paso 3** Seleccione el nodo de destino y elija **More > Reset Node** en la columna **Operation**.

AVISO

El restablecimiento de un nodo puede hacer que los recursos específicos del nodo no estén disponibles (como el almacenamiento local y las cargas de trabajo programadas para este nodo). Tenga cuidado al realizar esta operación para evitar el impacto en los servicios en ejecución.

- Paso 4** Haga clic en **Yes**.
- Paso 5** Reconfigure los parámetros del nodo.

Si necesita ajustar el espacio de almacenamiento del contenedor, preste atención a las siguientes configuraciones:



Storage Settings: Haga clic en **Expand** junto al disco de datos para establecer los siguientes parámetros:

- **Allocate Disk Space:** espacio de almacenamiento utilizado por el motor de contenedores para almacenar el directorio de trabajo Docker/containerd, los datos de la imagen del contenedor y los metadatos de la imagen. El valor predeterminado es el 90% del disco de datos.
- **Allocate Pod Basesize:** CCE le permite establecer un límite superior para el espacio en el disco ocupado por cada pod de carga de trabajo (incluido el espacio ocupado por imágenes de contenedores). Esta configuración impide que los pods ocupen todo el espacio disponible en disco, lo que puede provocar excepciones de servicio. Se recomienda que el valor sea inferior o igual al 80% del espacio del motor del contenedor.

📖 NOTA

- La capacidad de personalizar el tamaño base de pod está relacionada con el sistema operativo del nodo y los rootfs de almacenamiento de contenedores.
 - Cuando el rootfs utiliza Device Mapper, el nodo admite tamaño base de pod personalizado. El espacio de almacenamiento predeterminado de un solo contenedor es de 10 GiB.
 - Cuando el rootfs utiliza OverlayFS, la mayoría de los nodos no admiten el tamaño base de pod personalizado. El espacio de almacenamiento de un solo contenedor no está limitado y por defecto es el espacio del motor del contenedor.
Solo los nodos de EulerOS 2.9 en clústeres de 1.19.16, 1.21.3, 1.23.3 y versiones posteriores admiten el tamaño básico de pod personalizado.
Para obtener más información acerca de la relación entre los sistemas operativos de nodo y los rootfs de almacenamiento de contenedores, consulte [Asignación entre los SO de nodo y los motores de contenedores](#).
- En el caso de usar Docker en los nodos de EulerOS 2.9, el **basesize** no tendrá efecto si **CAP_SYS_RESOURCE** o **privileged** están configurados para un contenedor.

Para obtener más información acerca de la asignación de espacio de almacenamiento de contenedores, consulte [Asignación de espacio en disco de datos](#).

Paso 6 Después de restablecer el nodo, inicie sesión en el nodo y ejecute el siguiente comando para acceder al contenedor y comprobar si se ha expandido la capacidad de almacenamiento del contenedor:

docker exec -it container_id /bin/sh or **kubectl exec -it container_id /bin/sh**

df -h

```
df -h
Filesystem
/dev/mapper/docker-253:1-787293-631c1bde2cbe82e39f32253b216ba914cb183b168b54708b3e5b9a54ee40a8d1
tmpfs
/dev/mapper/vgpaas-kubernetes
/dev/vda1
shm
tmpfs
tmpfs
tmpfs
tmpfs
tmpfs
tmpfs
Size      Used Avail Use% Mounted on
15G      229M  15G   2% /
32G         0   32G   0% /dev
32G         0   32G   0% /sys/fs/cgroup
9.8G     37M   9.2G  1% /etc/hosts
48G     5.2G   33G  14% /etc/hostname
64M         0   64M   0% /dev/shm
32G     16K   32G   1% /run/secrets/kubernetes.io/serviceaccount
32G         0   32G   0% /proc/acpi
32G         0   32G   0% /sys/firmware
32G         0   32G   0% /proc/scsi
32G         0   32G   0% /proc/kbox
32G         0   32G   0% /proc/oom_extend
```

----Fin

15.2 ¿Cómo pueden las direcciones IP de contenedores sobrevivir a un reinicio de contenedores?

Si los contenedores se ejecutarán en un clúster de nodo único

Agregue **hostNetwork: true** a **spec.spec** en el archivo YAML de la carga de trabajo a la que pertenecerán los contenedores.

Si los contenedores se ejecutarán en un clúster de varios nodos

Configure las políticas de afinidad de nodo, además de realizar las operaciones descritas en "If the Container Runs in a Single-Node Cluster". Sin embargo, después de crear la carga de trabajo, el número de pods en ejecución no puede exceder el número de nodos de afinidad.

Resultado esperado

Una vez completada la configuración anterior y la carga de trabajo se está ejecutando, las direcciones IP de los pods de la carga de trabajo son las mismas que las direcciones IP del nodo. Después de reiniciar la carga de trabajo, estas direcciones IP se mantendrán sin cambios.

15.3 ¿Cuáles son las diferencias entre CCE y CCI?

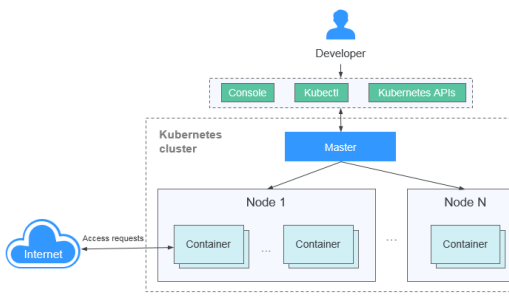
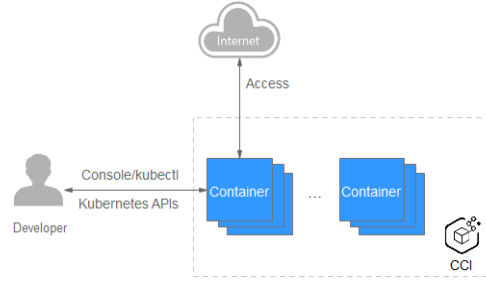
Descripción

Tabla 15-1 Introducción a CCE y CCI

Cloud Container Engine (CCE)	Cloud Container Instance (CCI)
<p>CCE proporciona clústeres de Kubernetes con gran capacidad de escalamiento, de alto rendimiento y de clase empresarial; además es compatible con los contenedores de Docker. CCE es una plataforma de contenedores integral que proporciona servicios de contenedores de pila completa desde la gestión de clústeres de Kubernetes, la gestión del ciclo de vida de aplicaciones en contenedores, la malla de servicios de aplicaciones y los gráficos Helm para la gestión de complementos, la programación de aplicaciones, y monitoreo y O&M. Con CCE, puede desplegar, gestionar y escalar fácilmente aplicaciones en contenedores en Huawei Cloud.</p> <p>Para obtener más información, consulte ¿Qué es Cloud Container Engine?.</p>	<p>Cloud Container Instance (CCI) es un motor de contenedor sin servidor que le permite ejecutar contenedores sin crear ni gestionar clústeres de servidores. Con CCI, solo necesita gestionar los servicios en contenedores que se ejecutan en Kubernetes. Puede crear y ejecutar rápidamente cargas de trabajo contenedor en CCI sin gestionar clústeres y servidores. Debido a la arquitectura sin servidor, CCI le libera de la aplicación contenedorizada O&M y le permite centrarse en los servicios en sí.</p> <p>Con la arquitectura sin servidor, puede centrarse en crear y operar aplicaciones sin tener que crear o gestionar servidores, sin mencionar los problemas causados por un funcionamiento anormal del servidor. Todo lo que tiene que hacer es especificar los requisitos de recursos (en CPU y memoria, por ejemplo). Esto le proporciona un enfoque más centrado en las necesidades empresariales y le ayuda a reducir los costos de gestión y mantenimiento.</p> <p>Tradicionalmente, para ejecutar cargas de trabajo en contenedores con Kubernetes, primero debe crear un clúster de Kubernetes.</p>

Modo de creación

Tabla 15-2 Modos de creación

Cloud Container Engine (CCE)	Cloud Container Instance (CCI)
<p>CCE es un servicio alojado de Kubernetes para la gestión de contenedor. Le permite crear clústeres nativos de Kubernetes con pocos clics.</p> <p>Necesita crear clústeres y nodos para usar CCE. Son fáciles de crear en una consola intuitiva y altamente disponibles. No es necesario gestionar nodos maestros.</p> 	<p>CCI proporciona un motor de contenedor sin servidor. Al desplegar contenedores en Huawei Cloud, no es necesario comprar y gestionar ECS, lo que elimina la necesidad de operación y gestión.</p> <p>No es necesario crear clústeres, nodos maestros o nodos de trabajo, sino iniciar directamente las aplicaciones.</p> 

Facturación

Tabla 15-3 Modos de facturación diferentes

Aspecto	Cloud Container Engine (CCE)	Cloud Container Instance (CCI)
Precios	Cuando se utilice CCE se crearán recursos relacionados (como nodos y ancho de banda). Tiene que pagar por estos recursos.	Los recursos de instancia CCI incluyen CPU, memoria y GPU. Se le facturará según las especificaciones reales de recursos de instancia.
Modo de facturación	Los modos de pago por uso y de facturación anual/mensual son compatibles.	Se admite el modo de facturación de pago por uso.

As pec to	Cloud Container Engine (CCE)	Cloud Container Instance (CCI)
Uni dad de prec io mín ima	Por hora	Facturado por segundo. El período de ejecución de la factura es una hora.

Escenarios de aplicación

Tabla 15-4 Diferentes escenarios de aplicación

Cloud Container Engine (CCE)	Cloud Container Instance (CCI)
<p>Aplicable a todos los escenarios. En general, se están ejecutando aplicaciones estables a gran escala y a largo plazo. Por ejemplo:</p> <ul style="list-style-type: none"> ● Comercio electrónico ● Service mid-end ● Sistema de TI 	<p>Aplicable a escenarios con horas pico y fuera de pico evidentes. Los recursos pueden solicitarse de manera flexible para mejorar la utilización de los recursos. Por ejemplo:</p> <ul style="list-style-type: none"> ● Cómputo por lotes ● Cómputo de alto rendimiento ● Expansión horizontal en ráfagas de tráfico ● Comprueba CI/CD

Creación de clústeres

Tabla 15-5 Modos de creación

Cloud Container Engine (CCE)	Cloud Container Instance (CCI)
<p>Proceso de uso de CCE:</p> <ol style="list-style-type: none"> Crear un clúster Configure la información básica como el nombre, la región y la red. Crear un nodo Especifique las especificaciones del nodo y el tamaño del disco de datos. Configurar el clúster Instale complementos de clúster, como redes, supervisión y registros. Crear una carga de trabajo en el clúster 	<p>Proceso de utilización de CCI:</p> <ol style="list-style-type: none"> Crear un espacio de nombre Configure la información básica como el nombre, la región y la red. Crear una carga de trabajo

Cooperación entre CCE y CCI

Al instalar el complemento virtual-kubelet, puede usar CCI para desplegar pods para sus Deployments, StatefulSets y trabajos en CCE cuando se producen picos de servicio, lo que puede reducir el consumo causado por el ajuste del clúster.

Funciones:

- Crea pods automáticamente en unos segundos. Cuando los recursos del clúster de CCE son insuficientes, no es necesario agregar nodos al clúster. virtual-kubelet crea automáticamente pods en CCI, eliminando la sobrecarga de cambiar el tamaño del clúster de CCE.
- Funciona sin problemas con Huawei Cloud SWR para que utilices imágenes públicas y privadas.
- Soporta sincronización de eventos, supervisión, registro, ejecución de comandos remotos y consulta de estado para los pods CCI.
- Permite ver la información de capacidad de los nodos elásticos virtuales.
- Soporta conectividad entre los pods de CCE y CCI con Services.

Para obtener más información, consulte [Ajuste elástico de pods de CCE a CCI](#).

15.4 ¿Cuáles son las diferencias entre CCE y ServiceStage?

En términos de uso, CCE se centra en el despliegue de pod, y ServiceStage se centra en el uso del servicio.

En términos de implementación técnica, ServiceStage encapsula las capacidades de CCE.

Conceptos básicos

Cloud Container Engine (CCE)

CCE proporciona clústeres de Kubernetes con gran capacidad de escalamiento, de alto rendimiento y de clase empresarial; además es compatible con los contenedores de Docker. CCE es una plataforma de contenedores integral que proporciona servicios de contenedores de pila completa desde la gestión de clústeres de Kubernetes, la gestión del ciclo de vida de aplicaciones en contenedores, la malla de servicios de aplicaciones y los gráficos Helm para la gestión de complementos, la programación de aplicaciones, y monitoreo y O&M. Con CCE, puede desplegar, gestionar y escalar fácilmente aplicaciones en contenedores en Huawei Cloud.

ServiceStage

ServiceStage es una plataforma de gestión de aplicaciones y microservicios que ayuda a las empresas a simplificar la gestión del ciclo de vida de las aplicaciones, desde el despliegue y el monitoreo hasta el gobierno. ServiceStage ofrece una solución de pila completa para que las empresas desarrollen aplicaciones web, móviles y de microservicios. Esta solución ayuda a las empresas a migrar fácilmente varias aplicaciones a la nube, lo que permite a las empresas centrarse en la innovación de servicios para la transformación digital.