## Cloud Backup and Recovery

# Descripción general del servicio

**Edición** 01

**Fecha** 2023-01-12

**HUAWEI TECHNOLOGIES CO., LTD.**

### Marcas y permisos


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

Las funciones, los productos y los servicios adquiridos están estipulados en el contrato celebrado entre Huawei y el cliente. Es posible que la totalidad o parte de los productos, las funciones y los servicios descritos en el presente documento no se encuentren dentro del alcance de compra o de uso. A menos que el contrato especifique lo contrario, ninguna de las afirmaciones, informaciones ni recomendaciones contenidas en este documento constituye garantía alguna, ni expresa ni implícita.

La información contenida en este documento se encuentra sujeta a cambios sin previo aviso. En la preparación de este documento se realizaron todos los esfuerzos para garantizar la precisión de sus contenidos. Sin embargo, ninguna declaración, información ni recomendación contenida en el presente constituye garantía alguna, ni expresa ni implícita.

## Huawei Technologies Co., Ltd.

Dirección: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Sitio web: https://www.huawei.com

Email: support@huawei.com

# Índice



# 1 Infografía de CBR

# 2 Qué es CBR

## Descripción

Cloud Backup and Recovery (CBR) le permite realizar copias de respaldo de Elastic Cloud Servers (ECSs), Bare Metal Servers (BMSs), Elastic Volume Service (EVS) disks, SFS Turbo file systems, archivos y directorios locales y entornos virtuales VMware locales con facilidad. En caso de un ataque de virus, eliminación accidental o fallo de software o hardware, puede restaurar los datos en cualquier momento en el pasado cuando se hizo una copia de respaldo de los datos.

CBR protege sus servicios al garantizar la seguridad y la coherencia de sus datos.

## Arquitectura del producto

CBR consta de copias de respaldo, depósitos y políticas.

**Copia de respaldo**

Una copia de respaldo es una copia de un chunk particular de datos y generalmente se almacena en otro lugar de modo que puede usarse para restaurar los datos originales en caso de pérdida de datos. Los siguientes son los tipos de copias de seguridad de CBR:

- Copia de respaldo en disco en la nube. Este tipo de copia de respaldo proporciona protección de datos basada en instantáneas para discos EVS.
- Copia de respaldo del servidor en la nube. Este tipo de copia de respaldo utiliza la tecnología de instantáneas de consistencia para los discos para proteger los datos de ECSs y BMSs. Las copias de respaldo de servidores sin bases de datos implementadas son copias de respaldo de servidores comunes, y las de servidores con bases de datos implementadas son copias de seguridad compatibles con las aplicaciones.
- Copia de respaldo SFS Turbo. Este tipo de copia de respaldo protege los datos de los sistemas de archivos SFS Turbo.
- Copia de respaldo en la nube híbrida. Este tipo de copia de respaldo protege los datos de los sistemas de almacenamiento OceanStor Dorado locales y las VMs VMware almacenando sus copias de seguridad en la nube. Puede gestionar las copias de seguridad en la consola CBR.
- Copia de respaldo de archivos: Este tipo de copia de respaldo protege los datos de uno o varios archivos en sus servidores en la nube o hosts locales. No es necesario realizar copias de respaldo de todos los servidores o discos.

**Almacén**

CBR utiliza almacenes para almacenar copias de respaldo. Antes de crear una copia de respaldo, debe crear al menos un almacén y asociar el recurso del que desea realizar una copia de respaldo con el almacén. A continuación, las copias de seguridad de recursos generadas se almacenan en el almacén asociado.

Los almacenes pueden ser de copia de respaldo o de replicación. Los almacenes de copia de respaldo almacenan copias de respaldo de recursos, mientras que las de replicación almacenan réplicas de copias de respaldo.

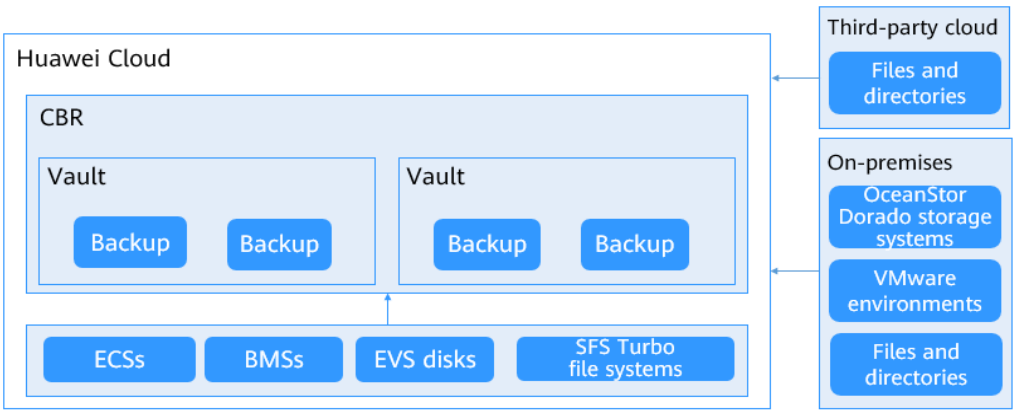
Las copias de seguridad de diferentes tipos de recursos deben almacenarse en diferentes tipos de depósitos.

**Política**

Las políticas se dividen en políticas de backup y políticas de replicación.

- Polóíticas de copia de respaldo: para realizar copias de seguridad automáticas, configure una política de copia de respaldo estableciendo los tiempos de ejecución de las tareas de copia de respaldo, la frecuencia de copia de respaldo y las reglas de retención y, a continuación, aplique la política a un almacén.
- Políticas de replicación: para replicar automáticamente backups o almacenes, configure una política de replicación estableciendo los tiempos de ejecución de las tareas de replicación, la frecuencia de replicación y las reglas de retención y, a continuación, aplique la política a un almacén. Las réplicas de copia de respaldo deben almacenarse en almancenes de replicación.

**Figura 2-1** Arquitectura de CBR



## Diferencias entre los tipos de copia de respaldo

**Tabla 2-1** Diferencias entre los tipos de copia de respaldo

| Artículo | Cloud Server Backup | Cloud Disk Backup | SFS Turbo Backup | Hybrid Cloud Backup | File Backup |
|---|---|---|---|---|---|
| Copia de respaldo y restauración de objetos | Todos los discos (discos de sistema y de datos) en un servidor | Uno o más discos específicos (discos de sistema o de datos) | Sistemas de archivos SFS Turbo | Copias de respaldo sincronizados desde software del local y de máquinas virtuales | Uno o varios archivos en servidores en la nube y hosts locales |
| Escenario recomendado | Es necesario proteger todo un servidor en la nube. | Sólo es necesario realizar una copia de respaldo de los discos de datos, ya que el disco del sistema no contiene los datos de la aplicación de los usuarios. | Es necesario proteger los datos de los sistemas de archivos SFS Turbo. | Las copias de respaldo de los servidores locales deben administrarse y restaurarse en la nube. | Es necesario proteger los datos de uno o varios archivos, y se pueden realizar copias de seguridad y restaurar rápidamente en la nube. |
| Ventajas | Todos los discos de un servidor se realizan copias de seguridad al mismo tiempo, lo que garantiza la coherencia de los datos. | Los costos de copia de respaldo se reducen sin comprometer la seguridad de los datos. | Los datos de copia de respaldo y los sistemas de archivos originales se almacenan por separado. Puede utilizar los datos de copia de respaldo para crear un nuevo sistema de archivos. | Los datos locales pueden respaldarse en la nube y usarse para reconstruir servicios en la nube. | Los datos se pueden hacer copias de seguridad por archivo o directorio. No tiene que realizar copias de seguridad de todos sus servidores o discos, lo que reduce los costos de copia de respaldo. |

## Mecanismo de copia de respaldo

Las copias de seguridad en la nube de CBR ofrecen copias de seguridad a nivel de bloque, y las copias de respaldo de archivos de CBR proporcionan copias de respaldo a nivel de archivo. Una copia de respaldo completa se realiza solo para la primera copia de respaldo y realiza copias de seguridad de todos los bloques de datos usados. Por ejemplo, si el tamaño de un disco es de 100 GB y el espacio utilizado es de 40 GB, se realiza una copia de respaldo de los 40 GB de datos. Una copia de respaldo incremental solo realiza copias de respaldo de los datos cambiados desde la última copia de respaldo, lo que es eficiente en el almacenamiento y en el tiempo. Cuando se elimina una copia de respaldo, solo se eliminan los bloques de datos que no dependen de otras copias de respaldo, de modo que otras copias de seguridad todavía se pueden utilizar para la restauración. Tanto una copia de respaldo completa como una copia de respaldo incremental pueden restaurar los datos al estado en un punto de copia de respaldo determinado.

Al crear una copia de respaldo de un disco, CBR también crea una instantánea para él. Cada vez que se crea una nueva copia de respaldo de disco, CBR elimina la copia de respaldo antigua y solo conserva la última copia de respaldo.

CBR almacena los datos de copia de respaldo en OBS para mejorar la seguridad de los datos de copia de respaldo.

## Opciones de copia de respaldo

CBR admite copias de respaldo únicas y copias de respaldo periódicas. Una tarea de copia de respaldo única es creada manualmente por los usuarios y se ejecuta una sola vez. Las tareas de copia de respaldo periódica se ejecutan automáticamente en función de una política de copia de respaldo definida por el usuario.

**Tabla 2-2** describe las dos opciones de copia de respaldo.

**Tabla 2-2** One-off backup y periodic backup

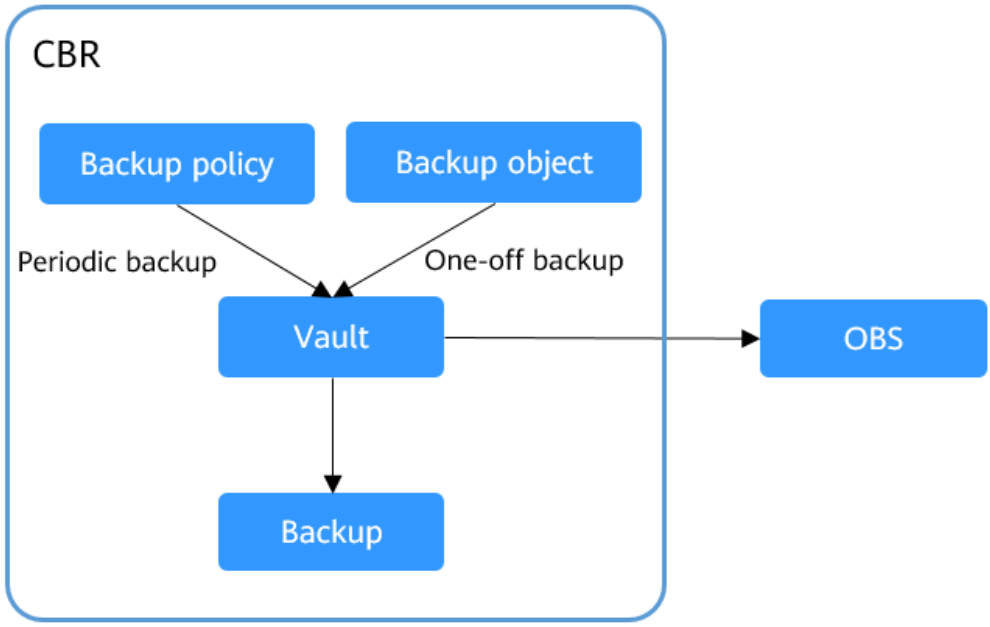
| Artículo | One-Off Backup | Periodic Backup |
| --- | --- | --- |
| Política de copia de respaldo | No requerido | Requerido |
| Número de tareas de copia de respaldo | Una tarea de copia de respaldo manual | Tareas periódicas impulsadas por una política de copia de respaldo |
| Nombre del respaldo | Nombre de copia de respaldo definido por el usuario, que es **manualbk**_*xxxx* de forma predeterminada | Nombre de copia de respaldo asignado al sistema, que es **autobk**_*xxxx* de forma predeterminada |
| Modo de copia de respaldo | Copia de respaldo completa por primera vez y copia de respaldo incremental posteriormente, de forma predeterminada | Copia de respaldo completa por primera vez y copia de respaldo incremental posteriormente, de forma predeterminada |

| Artículo | One-Off Backup | Periodic Backup |
| --- | --- | --- |
| Escenario de aplicación | Se ejecuta antes de aplicar parches o actualizar el sistema operativo o actualizar una aplicación en un recurso. Se puede utilizar una copia de respaldo única para restaurar el recurso al estado original si falla el parche o la actualización. | Ejecutado para el mantenimiento rutinario de un recurso. La última copia de respaldo se puede utilizar para la restauración si se produce un fallo inesperado o una pérdida de datos. |

También puede utilizar las dos opciones de copia de respaldo juntas si es necesario. Por ejemplo, puede asociar recursos a un almacén y aplicar una política de copia de respaldo al almacén para ejecutar copias de respaldo periódicas de todos los recursos del almacén. Además, puede realizar copias de seguridad de los recursos más importantes bajo demanda para mejorar la seguridad de los datos. **Figura 2-2** muestra el uso entremezclado de las dos opciones de copia de respaldo.

**Figura 2-2** Uso entremezclado de las dos opciones de copia de respaldo




## Método de acceso

Puede acceder al servicio CBR a través de la consola o llamando a las API basadas en HTTPS.

- Consola

  Utilice la consola si prefiere una interfaz de usuario basada en web para realizar operaciones. Inicie sesión en la consola y elija **Cloud Backup and Recovery**.
- APIs

Utilice APIs si necesita integrar CBR en un sistema de terceros para el desarrollo secundario. Para obtener más información, consulta la **Referencia de la API de Cloud Backup and Recovery**.

# 3 Ventajas

## Confiabilidad

CBR admite copias de seguridad consistentes en fallos para varios discos en un servidor y copias de seguridad consistentes en aplicaciones para servidores de bases de datos, lo que garantiza la seguridad y fiabilidad de sus datos.

## Eficiente

Las copias de seguridad incrementales para siempre acortan el tiempo necesario para la copia de respaldo en un 95%. Con Instant Restore, CBR admite RPO de tan solo 1 hora y RTO en cuestión de minutos.

NOTA

Recovery Point Objective (RPO) especifica el período máximo aceptable en el que se pueden perder los datos.

Recovery Time Objective (RTO) especifica la cantidad máxima de tiempo aceptable para restaurar todo el sistema después de que se produzca un desastre.

## Fácil de usar

Puede completar la configuración de copia de respaldo en solo tres pasos, y no se requieren conocimientos profesionales de software de copia de respaldo. El CBR es más fácil de usar que los sistemas de respaldo convencionales.

## Seguro

Encripte automáticamente los datos de las copias de respaldo de discos encriptados para garantizar la seguridad de los datos. Puede replicar y restaurar datos de backup en distintas regiones para implementar la recuperación remota ante desastres.

# 4 Escenarios de aplicación

CBR realiza copias de respaldo de los recursos para maximizar la seguridad y consistencia de los datos del usuario y garantizar la continuidad del servicio. CBR es adecuado para backup y restauración de datos.

## Copia de respaldo y restauración de datos

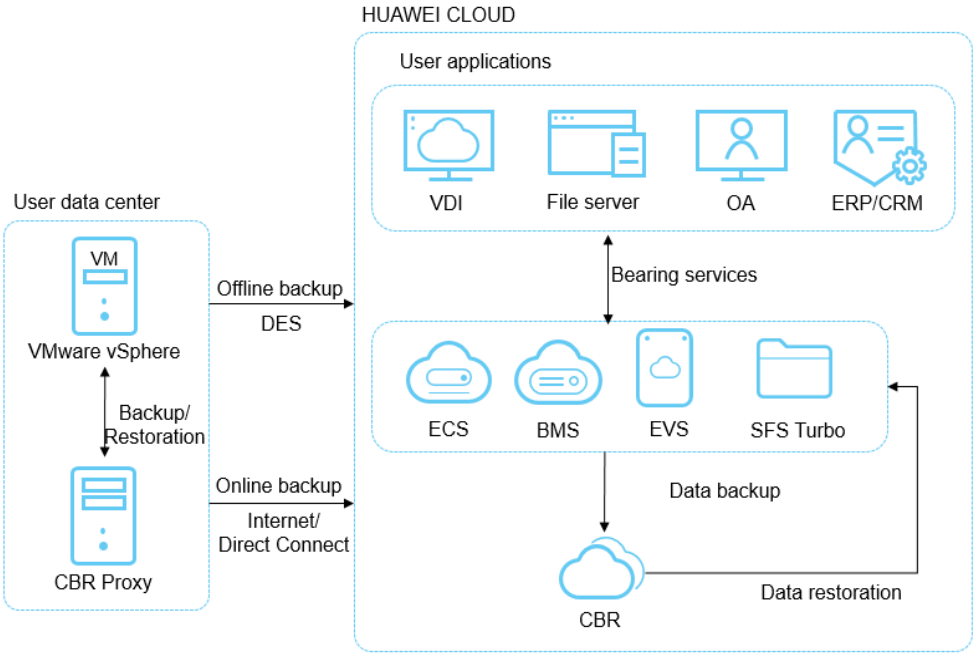
CBR se puede utilizar para restaurar datos rápidamente en los siguientes escenarios:

- Ataques de hackers o virus
- Eliminación accidental
- Errores de actualización de aplicaciones
- Colapso del sistema

  Para cualquiera de los incidentes anteriores, puede usar CBR para restaurar los datos en el último punto de copia de respaldo antes del incidente.

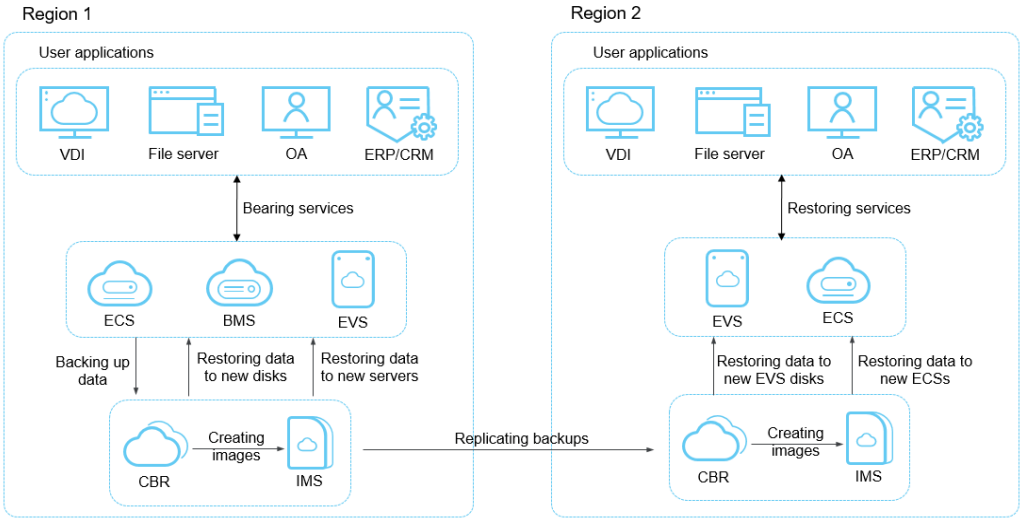
**Figura 4-1** Copia de respaldo y restauración de datos




## Implementación & de migración rápida de servicio

Puede usar copias de respaldo de servidores en la nube para crear imágenes y luego usar dichas imágenes para aprovisionar rápidamente nuevos servidores en la nube con la misma configuración que los existentes. Consulte **Figura 4-2**.

**Figura 4-2** Migración e implementación rápidas de servicios



# 5 Funciones

**Tabla 5-1** enumera las funciones básicas de CBR.

Antes de utilizar este servicio, se recomienda que vaya a **conceptos básicos** para obtener más información sobre CBR, como sobre el almacén y la política de copia de respaldo.

**Tabla 5-1** Funciones básicas de CBR

| Categoría | Función | Descripción |
| --- | --- | --- |
| Cloud disk backup | **Copia de respaldo de discos** | La copia de respaldo de disco en la nube proporciona protección de datos basada en instantáneas para discos EVS. Puede utilizar CBR para realizar una copia de respaldo de un solo disco en un servidor para proteger los datos de ese disco. |
| | **Copia de respaldo de datos basado en políticas** | Una política de copia de respaldo permite que un almacén ejecute automáticamente tareas de copia de respaldo en momentos o intervalos especificados. Las copias de respaldo periódicas se pueden utilizar para restaurar los datos rápidamente contra la corrupción o pérdida de datos. |
| | **Gestión de copia de respaldo** | Cuando se ejecuta o completa una tarea de copia de respaldo, puede establecer criterios de búsqueda para filtrar las copias de respaldo de la lista de copia de respaldo para gestionarlas y ver sus detalles. |
| | **Restauración de datos de disco mediante copias de respaldo** | Cuando un disco está defectuoso o se pierden datos del disco debido a un funcionamiento incorrecto, puede utilizar una copia de respaldo para restaurar el disco. |

| Categoría | Función | Descripción |
| --- | --- | --- |
| | **Creación de discos mediante copias de respaldo** | Puede utilizar una copia de respaldo de disco para crear un disco. Después de crear el disco, los datos en el nuevo disco son los mismos que en la copia de respaldo del disco. |
| | **Compartir copias de respaldo** | Puede compartir una copia de respaldo de un servidor o disco con otras cuentas. Las copias de respaldo compartidas se pueden utilizar para crear discos o servidores. |
| Cloud server backup | **Servidores de copia de respaldo** | La copia de respaldo de servidores en la nube utiliza la tecnología de instantáneas de consistencia para los discos para proteger los datos de ECS y BMS. Puede usar CBR para hacer una copia de respaldo de todo un servidor para proteger los datos en el servidor. Se recomienda utilizar la copia de respaldo del servidor en la nube en escenarios que requieren una alta consistencia de datos, como los clústeres RAID. |
| | **Copia de respaldo de discos en un servidor** | Puede realizar una copia de respaldo de los discos de un servidor en una copia de respaldo para ahorrar espacio en el almacén de copias de respaldo del servidor. |
| | **Copia de respaldo de datos basado en políticas** | Una política de copia de respaldo permite que un almacén ejecute automáticamente tareas de copia de respaldo en momentos o intervalos especificados. Las copias de respaldo periódicas se pueden utilizar para restaurar los datos rápidamente contra la corrupción o pérdida de datos. |
| | **Gestión de copia de respaldo** | Cuando se ejecuta o completa una tarea de copia de respaldo, puede establecer criterios de búsqueda para filtrar las copias de respaldo de la lista de copia de respaldo para gestionarlas y ver sus detalles. |
| | **Restauración de datos del servidor mediante copias de respaldo** | Cuando un servidor está defectuoso o se pierden datos del servidor debido a un mal funcionamiento, puede usar una copia de respaldo para restaurar el servidor. |

| Categoría | Función | Descripción |
| --- | --- | --- |
| | **Compartir copias de respaldo** | Puede compartir una copia de respaldo de un servidor o disco con otras cuentas. Las copias de respaldo compartidas se pueden utilizar para crear discos o servidores. |
| | **Creación de imágenes mediante copias de respaldo** | La copia de respaldo del servidor en la nube le permite crear imágenes usando copias de respaldo de ECS. Puede utilizar las imágenes para aprovisionar ECS para restaurar rápidamente entornos en ejecución de servicios. |
| | **Copia de respaldo de servidores de bases de datos** | La copia de respaldo del servidor en la nube admite copias de respaldo compatibles con las aplicaciones, además de copias de respaldo compatibles con fallos. La copia de respaldo consistente con las aplicaciones garantiza la consistencia de los datos de las aplicaciones al realizar copias de respaldo de archivos y discos al mismo tiempo. Es adecuado para realizar copias de respaldo de ECS, así como las bases de datos MySQL o SAP HANA que se ejecutan en ellos. |
| | **Replicación de copias de respaldo entre regiones** | La copia de respaldo del servidor en la nube le permite replicar las copias de respaldo generadas de una región a otra. Puede utilizar réplicas de copia de respaldo en la región de destino para crear imágenes y aprovisionar servidores. |
| Copia de respaldo SFS Turbo | **Copia de respaldo de sistemas de archivos SFS Turbo** | La copia de respaldo de SFS Turbo le permite realizar copias de respaldo de los sistemas de archivos SFS Turbo. Una copia de respaldo del sistema de archivos SFS Turbo se puede utilizar para crear un nuevo sistema de archivos SFS Turbo, evitando la pérdida de datos importantes. |

| Categoría | Función | Descripción |
| --- | --- | --- |
| | **Copia de respaldo de datos basado en políticas** | Una política de copia de respaldo permite que un almacén ejecute automáticamente tareas de copia de respaldo en momentos o intervalos especificados. Las copias de respaldo periódicas se pueden utilizar para restaurar los datos rápidamente contra la corrupción o pérdida de datos. |
| | **Gestión de copia de respaldo** | Cuando se ejecuta o completa una tarea de copia de respaldo, puede establecer criterios de búsqueda para filtrar las copias de respaldo de la lista de copia de respaldo para gestionarlas y ver sus detalles. |
| | **Creación de sistemas de archivo mediante copia de respaldo** | Puede utilizar una copia de respaldo del sistema de archivos SFS Turbo para crear un nuevo sistema de archivos. Después de crearlo, los datos del nuevo sistema de archivos son los mismos que los de la copia de respaldo. |
| | **Replicación de copias de respaldo entre regiones** | La copia de respaldo de SFS Turbo le permite replicar copias de respaldo de sistemas de archivos SFS Turbo de una región a otra. A continuación, puede utilizar la copia de respaldo replicada para crear un sistema de archivos en la región de destino. |
| Hybrid cloud backup | **Sincronización de datos de copia de respaldo de servidores locales** | Si se ha realizado una copia de respaldo de una máquina virtual de VMware local sin conexión y los datos de copia de respaldo se han cargado en un bucket OBS, puede sincronizar los datos de copia de respaldo en el bucket OBS en un almacén de copia de respaldo en la nube híbrida para operaciones posteriores. |
| | **Restauración de datos en servidores mediante copias de respaldo** | Una vez sincronizadas correctamente las copias de respaldo en un almacén de copia de respaldo en la nube híbrida, puede restaurar los datos de copia de respaldo en servidores en la nube para la recuperación ante desastres, la migración de servicios, el desarrollo y las pruebas. |

| Categoría | Función | Descripción |
| --- | --- | --- |
| File backup | **Copia de respaldo de archivos** | La copia de respaldo de archivos le permite realizar copias de respaldo de archivos y directorios en sus servidores en la nube y hosts locales. No es necesario realizar copias de respaldo de todos los servidores o discos. |
| | **Restauración de datos mediante copias de respaldo** | Si se produjo la pérdida de datos en un archivo local debido a una eliminación accidental o un ataque de virus, puede usar las copias de respaldo creadas en la nube para restaurar los datos. |

# 6 Seguridad



## 6.1 Responsabilidades compartidas

Huawei garantiza que su compromiso con la seguridad cibernética nunca se verá compensado por la consideración de intereses comerciales. Para hacer frente a los desafíos emergentes de seguridad en la nube y a las amenazas y ataques generalizados de seguridad en la nube, Huawei Cloud crea un sistema integral de garantía de seguridad de servicios en la nube para diferentes regiones e industrias basado en las ventajas únicas de software y hardware, las leyes, las regulaciones, los estándares de la industria y el ecosistema de seguridad de Huawei.

**Figura 6-1** ilustra las responsabilidades compartidas por Huawei Cloud y los usuarios.

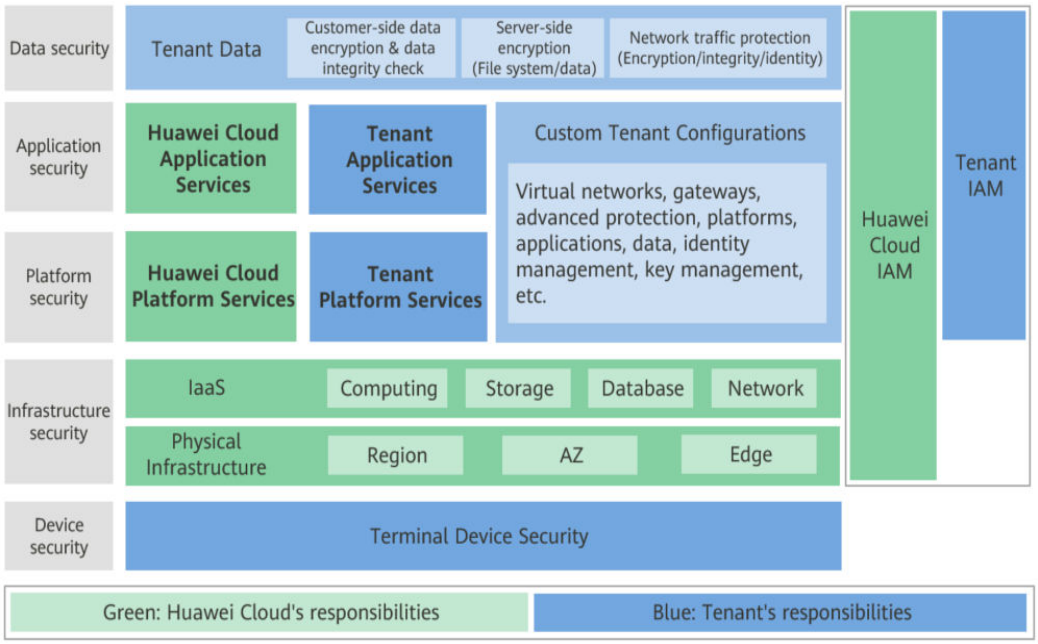
- **Huawei Cloud**: Garantizar la seguridad de los servicios en la nube y proporcionar nubes seguras. Las responsabilidades de seguridad de Huawei Cloud incluyen garantizar la seguridad de nuestros servicios IaaS, PaaS y SaaS, así como los entornos físicos de los centros de datos de Huawei Cloud donde nuestros IaaS, PaaS, y los servicios SaaS operan. Huawei Cloud es responsable no solo de las funciones de seguridad y el rendimiento de nuestra infraestructura, servicios en la nube y tecnologías, sino también de la seguridad general de la nube y, en el sentido más amplio, del cumplimiento de seguridad de nuestra infraestructura y servicios.
- **Tenant**: Utilizar la nube de forma segura. Los inquilinos de Huawei Cloud son responsables de la gestión segura y efectiva de las configuraciones personalizadas por el inquilino de los servicios en la nube, incluidos IaaS, PaaS y SaaS. Esto incluye, entre otros, redes virtuales, el sistema operativo de los hosts e invitados de máquinas virtuales,

firewalls virtuales, API Gateway, servicios de seguridad avanzados, todo tipo de servicios en la nube, datos del inquilino, cuentas de identidad, y gestión de claves.

**Libro blanco de seguridad de Huawei Cloud** elabora las ideas y medidas para construir la seguridad en Huawei Cloud, incluidas las estrategias de seguridad en la nube, el modelo de responsabilidad compartida, el cumplimiento y la privacidad, las organizaciones y el personal de seguridad, la seguridad de la infraestructura, el servicio y la seguridad del inquilino, la seguridad de ingeniería, seguridad de O&M y seguridad del ecosistema.

**Figura 6-1** Modelo de responsabilidad de seguridad compartida de Huawei Cloud




# 6.2 Autenticación de identidad y control de acceso

Puede acceder a CBR a través de la consola CBR, las API y los SDK. No importa el método que elija, en realidad utiliza REST APIs para acceder a CBR.

Las API de CBR solo admiten solicitudes autenticadas. Debe obtener la información de autenticación de Huawei Cloud IAM antes de poder acceder a CBR. Para obtener más información acerca de la autenticación de IAM, consulte **Autenticación**.

# 6.3 Protección de datos

CBR toma muchas medidas para mantener los datos seguros y confiables.

**Tabla 6-1** Protección de datos CBR

| Medida | Descripción |
| --- | --- |
| Transmission encryption (HTTPS) | Para garantizar la seguridad de la transmisión, los datos de copia de respaldo se almacenan en los depósitos de OBS a través de HTTPS. |

| Medida | Descripción |
| --- | --- |
| Backup data encryption | Si un disco del que desea realizar una copia de respaldo está cifrado, las copias de seguridad generadas para este disco también se cifrarán. Cuando se usa una copia de respaldo de este tipo para restaurar datos, los datos cifrados se descifrarán primero y luego se restaurarán en el disco de destino. |
| Cross-region replication | La replicación entre regiones le permite replicar copias de respaldo de forma automática y asincrónica desde una región a un almacén de replicación en una región diferente según una política de replicación. Las capacidades de recuperación ante desastres entre regiones que ofrece pueden satisfacer sus necesidades de copia de respaldo remota. |

# 6.4 Auditoría y registro

## Auditoría

Cloud Trace Service (CTS) registra las operaciones en los recursos de la nube de su cuenta. Puede utilizar los registros generados por CTS para realizar análisis de seguridad, realizar un seguimiento de los cambios de recursos, auditar el cumplimiento y localizar fallos.

Después de habilitar CTS y configurar un rastreador, CTS puede registrar la gestión y las trazas de datos de CBR para su auditoría.

Para obtener más información acerca de cómo habilitar y configurar CTS, consulte **Primeros pasos de CTS**.

Para obtener información sobre la gestión de CBR y las trazas de datos soportadas por CTS, consulte **Auditoría**.

## Registro

CBR muestra tareas de operaciones críticas en la página web. Puede iniciar sesión en la consola CBR, elegir **Tasks** en la página de exploración de la izquierda y ver la lista de tareas en el panel derecho. Alternativamente, puede **consultar la lista de tareas** a través de la API.

# 6.5 Resiliencia

CBR utiliza una arquitectura de confiabilidad de varios niveles y proporciona soluciones técnicas, que incluyen replicación entre regiones, para garantizar la durabilidad y confiabilidad de los datos.

# 6.6 Monitoreo de riesgos

Cloud Eye es una plataforma de monitoreo multidimensional que le permite ver los usos de los recursos y el estado de ejecución del servicio, y responder a las excepciones de manera oportuna para el buen funcionamiento de los servicios.

CBR utiliza Cloud Eye para realizar monitoreo de recursos y operaciones, lo que le ayuda a monitorear sus bóvedas y copias de seguridad y recibir alarmas y notificaciones en tiempo real. Puede obtener el uso de su almacén en tiempo real y recibir notificaciones de eventos, como errores de creación de copias de seguridad o eliminación.

Para obtener más información sobre las métricas CBR compatibles y cómo crear reglas de alarma, consulte **Monitoreo**.

# 6.7 Recuperación de fallas

CBR le permite realizar copias de seguridad y restaurar ciertos recursos en la nube, incluidos ECS, discos EVS, sistemas de archivos SFS Turbo y escritorios Workspace. Si alguno de estos tipos de recursos falla, puede usar copias de seguridad para restaurar en el origen o en los nuevos recursos, restaurando así rápidamente los datos y los servicios. Para obtener más información, consulte **Descripción de función**.

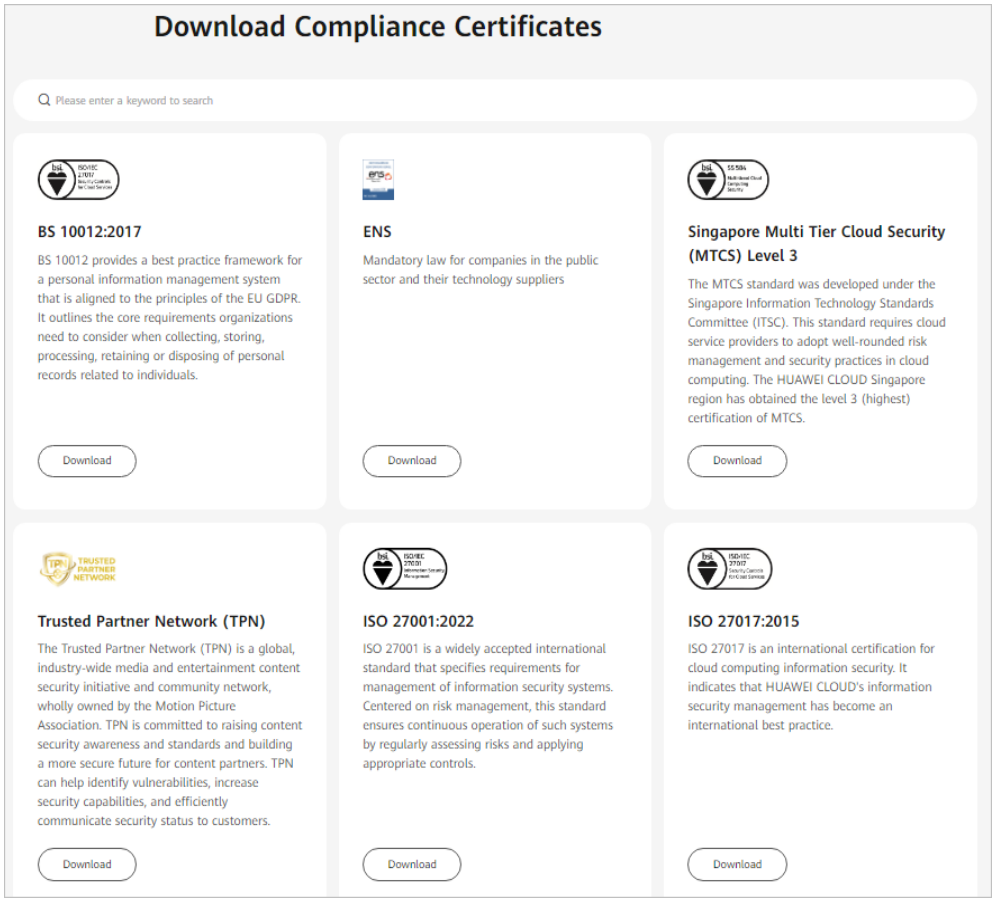
# 6.8 Certificados

## Certificados de Cumplimiento

Los servicios y plataformas de Huawei Cloud han obtenido diversas certificaciones de seguridad y cumplimiento de organizaciones autorizadas, como la Organización Internacional de Normalización (ISO). Puede **descargarlos** desde la consola.

**Figura 6-2** Descarga de certificados de cumplimiento

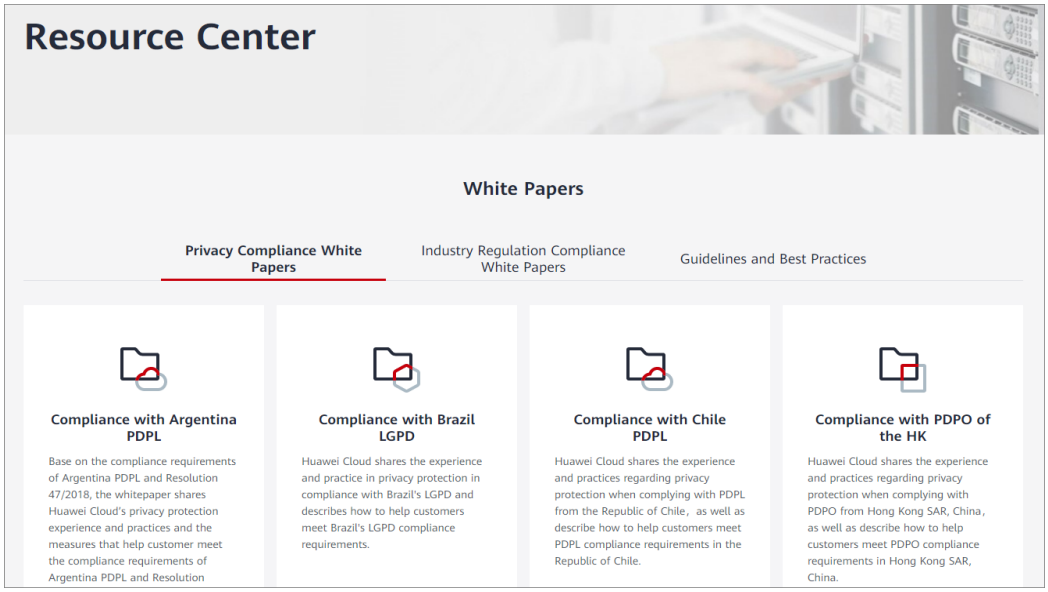



## Centro de recursos

Huawei Cloud también proporciona los siguientes recursos para ayudar a los usuarios a cumplir con los requisitos de cumplimiento. Para obtener más información, consulte **Centro de recursos**.

**Figura 6-3** Centro de recursos



# 7 Facturación

## Artículos de facturación

Se le factura el espacio de almacenamiento y el tráfico de datos generado si se utiliza la replicación de copia de respaldo. El precio del espacio de almacenamiento varía según los tipos de almacén. Vea los detalles en la tabla siguiente.

| Categoría | Artículo de facturación | Descripción | Modo de facturación |
|---|---|---|---|
| Espacio de almacenamiento | Almacén de copias de respaldo de discos | Si es necesario realizar una copia de respaldo de los discos en la nube, compre almacenes de copia de respaldo de disco para almacenar las copias de seguridad generadas. | Pago por uso<br>Anual/Mensual |
| | Almacén de respaldo de servidor | Si es necesario realizar una copia de respaldo de los servidores en la nube (aplicaciones no incluidas), compre almacenes de copia de respaldo del servidor para almacenar las copias de seguridad generadas. | Pago por uso<br>Anual/Mensual |
| | Almacén de copia de respaldo SFS Turbo | Si es necesario realizar una copia de respaldo de los sistemas de archivos SFS Turbo, compre almacenes de copia de respaldo SFS Turbo para almacenar las copias de seguridad generadas. | Pago por uso<br>Anual/Mensual |

| Categoría | Artículo de facturación | Descripción | Modo de facturación |
|---|---|---|---|
| | Almacén de respaldo de servidores de bases de datos | Si es necesario realizar una copia de respaldo de los servidores en la nube (aplicaciones incluidas), compre almacenes de copia de respaldo del servidor de base de datos para almacenar las copias de seguridad generadas.<br>Cómo comprar: Habilite **Application-Consistent Backup** en la página **Buy Server Backup Vault**. Para obtener más información, consulte **Descripción general de copia de respaldo consistente con aplicación**. | Pago por uso<br>Anual/Mensual |
| | Almacén de copia de respaldo de nube híbrida | Si las VMs de VMware locales, y las matrices OceanStor Dorado necesitan ser respaldados, compre almacenes de copia de respaldo en la nube híbrida para almacenar las copias de seguridad generadas. | Pago por uso<br>Anual/Mensual |
| | Almacén de réplica | Si necesita replicar copias de respaldo en otra región, compre almacenes de replicación en la región de destino. | Pago por uso<br>Anual/Mensual |
| Tráfico de datos | Tráfico saliente a través de Internet. | Si se utilizan copias de seguridad de nube híbrida en la nube para restaurar los datos en IDCs locales, se genera tráfico saliente a través de Internet. | Gratis por tiempo limitado |
| | Tráfico de replicaciones entre regiones | Si las copias de seguridad o los almacenes se replican en otra región, el tráfico de replicación entre regiones se genera en la región de origen. | Pago por uso<br>Anual/Mensual |

NOTA

Para obtener más información, consulte **Detalles de precios de CBR**.

## Ejemplos de facturación

Caso 1:

Almacén de pago por uso para servidores en la nube sin bases de datos implementadas:

Un usuario tiene un servidor en la nube de 100 GB y un almacén de respaldo de servidor de 400 GB adquirida en la región CN-Hong Kong, y el servidor en la nube está asociado con el

almacén. Se factura al usuario por el almacén de copia de respaldo del servidor de 400 GB en CBR.

Caso 2:

Almacén de pago por uso para servidores en la nube con bases de datos implementadas:

Un usuario tiene un servidor en la nube de 100 GB que ejecuta bases de datos y un almacén de respaldo de servidor de base de datos de 800 GB adquirida en la región CN-Hong Kong, y el servidor en la nube está asociado con el almacén. Se factura al usuario por el almacén de copia de respaldo del servidor de base de datos de 800 GB en CBR.

Caso 3:

Replicación de una copia de respaldo en otra región, con facturación de pago por uso:

Un usuario compra un almacén A de copia de respaldo de servidor único de 100 GB en la región CN-Hong Kong, y los datos de copia de respaldo utilizan 40 GB de espacio de almacenamiento. Este usuario también compra una almacén de replicación B de 200 GB en la región AP-Bangkok y replica datos de la almacén A al almacén B, sin utilizar el servicio de aceleración. En este caso, se factura al usuario por la almacén de copia de respaldo de 100 GB y el almacén de replicación de 200 GB, así como el tráfico de datos de replicación entre regiones de 40 GB.

## Modos de facturación

Los almacéns CBR tienen dos modos de facturación: pago por uso y anual/mensual. Seleccione el modo de facturación que mejor se adapte a las necesidades de su empresa.

- **Pago por uso**

  Usted paga por la duración de uso de los recursos. Los precios se calculan por hora y no se requiere una tarifa mínima.

- **Anual/Mensual:**

  Puedes elegir la suscripción anual/mensual por un mejor precio.

CBR también proporciona paquetes de tráfico de replicación para replicación de backup entre regiones. Si no se compra ningún paquete, se le facturará el tráfico de replicación según el pago por uso.

Para obtener más información, consulte **Detalles de precios de CBR**.

## Cambio del modo de facturación

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

Si desea cambiar una almacén de pago por uso a un almacén anual/mensual, Consulte **Cambio del modo de facturación de pago por uso a anual/mensual**.

## Caducidad

Para obtener más información, consulte **Suspensión de servicio y versión de recursos**.

## Renovación

Elija **More** > **Renew** en la columna **Operation** del almacén anual/mensual para renovar su suscripción. Para obtener más información acerca de la renovación, incluida la renovación automática, la exportación de la lista de renovación y el cambio de suscripciones, consulte **Gestión de renovación**.

## Pago atrasado

**Causas posibles de pago atrasado:**

- El saldo de la cuenta no es suficiente después de comprar un almacén de pago por uso.
- Las tarifas de tráfico generadas durante la replicación de backup son mayores que el saldo de su cuenta.

**Estado del servicio y restricciones de operación cuando una cuenta está en atraso:**

Durante el período de retención, se conservan sus almacenes y los datos de copia de respaldo. Puede ver las copias de seguridad existentes, pero no puede crear nuevas copias de seguridad ni agregar etiquetas. Si no paga las tarifas pendientes antes de que expire el período de retención, sus datos se liberarán automáticamente y no se podrán restaurar. Para ver cómo pagar los atrasos, vea **Reembolso de los atrasos**.

Para obtener más información sobre el período de retención, consulte **Suspensión de servicio y liberación de recursos**.

# 8 Gestión de permisos

Si necesita asignar diferentes permisos a los empleados de su empresa para acceder a sus recursos de CBR en Huawei Cloud, Identity and Access Management (IAM) es una buena opción para la gestión de permisos detallada. IAM proporciona autenticación de identidad, gestión de permisos y control de acceso, lo que le ayuda a proteger el acceso a sus recursos de Huawei Cloud.

Con IAM, puede usar su cuenta de Huawei Cloud para crear usuarios de IAM para sus empleados y asignar permisos a los usuarios para controlar su acceso a tipos de recursos específicos. Por ejemplo, algunos desarrolladores de software de su empresa necesitan usar recursos CBR, pero no deben poder eliminarlos ni realizar ninguna otra operación de alto riesgo. En este escenario, puede crear usuarios de IAM para los desarrolladores de software y concederles solo los permisos necesarios para usar los recursos de CBR.

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

IAM se puede utilizar de forma gratuita. Solo paga por los recursos de su cuenta. Para obtener más información acerca de IAM, consulte **Descripción general de servicio IAM**.

## Permisos de CBR

De forma predeterminada, los nuevos usuarios de IAM no tienen permisos asignados. Debe agregar un usuario a uno o más grupos y adjuntar directivas o roles de permisos a estos grupos. Los usuarios heredan permisos de los grupos a los que se agregan y pueden realizar operaciones específicas a servicios en la nube según los permisos.

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

Puede conceder permisos a los usuarios mediante roles y políticas.

- Roles: Un tipo de mecanismo de autorización de grano grueso que define permisos relacionados con las responsabilidades de los usuarios. Solo hay disponible un número limitado de funciones de nivel de servicio para la autorización. Al usar roles para conceder permisos, también debe asignar otros roles de los que dependen los permisos

para que surtan efecto. Sin embargo, los roles no son una opción ideal para la autorización detallada y el control de acceso seguro.

- Políticas: Un tipo de mecanismo de autorización detallado que define los permisos necesarios para realizar operaciones en recursos de nube específicos bajo ciertas condiciones. Este mecanismo permite una autorización más flexible basada en políticas, cumpliendo los requisitos para un control de acceso seguro. Por ejemplo, puede conceder a los usuarios de ECS solo los permisos para administrar un determinado tipo de ECS. La mayoría de las políticas definen permisos basados en API. Para ver las acciones de API admitidas por CBR, consulte **Políticas de permisos y acciones admitidas**.

**Tabla 8-1** enumera todas las funciones y políticas definidas por el sistema admitidas por CBR.

**Tabla 8-1** Políticas definidas por el sistema compatibles con CBR

| Nombre de la política | Descripción | Tipo |
| --- | --- | --- |
| CBR FullAccess | Permisos de administrador para CBR. Los usuarios a los que se conceden estos permisos pueden operar y usar todas las bóvedas, copias de seguridad y políticas. | System-defined policy |
| CBR BackupsAndVaults-FullAccess | Permisos de usuario comunes para CBR. Los usuarios a los que se conceden estos permisos pueden crear, ver y eliminar depósitos y copias de seguridad, pero no pueden crear, actualizar ni eliminar políticas. | System-defined policy |
| CBR ReadOnlyAccess | Permisos de sólo lectura para CBR. Los usuarios a los que se han concedido estos permisos solo pueden ver los datos CBR. | System-defined policy |

**Tabla 8-2** enumera las operaciones comunes soportadas por cada política o función definida por el sistema de CBR. Seleccione las políticas según sea necesario.

**Tabla 8-2** Operaciones comunes respaldadas por cada política definida por el sistema o función de CBR

| Operación | CBR FullAccess | CBR BackupsAndVaultsFullAccess | CBR ReadOnlyAccess |
| --- | --- | --- | --- |
| Consulta de almacenes | √ | √ | √ |
| Creación de almacenes | √ | √ | × |
| Listado de almacenes | √ | √ | √ |
| Actualización de almacenes | √ | √ | × |

| Operación | CBR FullAccess | CBR BackupsAndVaultsFullAccess | CBR ReadOnlyAccess |
|---|---|---|---|
| Supresión de almacenes | √ | √ | × |
| Asociación de recursos | √ | √ | × |
| Disociación de recursos | √ | √ | × |
| Creación de políticas | √ | × | × |
| Actualización de políticas | √ | × | × |
| Aplicación de políticas a un almacén | √ | √ | × |
| Eliminación de políticas de un almacén | √ | √ | × |
| Eliminación de políticas | √ | × | × |
| Sincronización de copias de respaldo | √ | √ | × |
| Replicación de almacenes | √ | √ | × |
| Realización de copias de seguridad | √ | √ | × |
| Actualización de suscripciones | √ | √ | × |
| Consulta del estado del agente | √ | √ | × |
| Eliminación de copias de seguridad | √ | √ | × |
| Restauración de datos mediante copias de seguridad | √ | √ | × |
| Replicación de copias de respaldo | √ | √ | × |
| Asociación de almacenes | √ | √ | × |

| Operación | CBR FullAccess | CBR BackupsAndVaultsFullAccess | CBR ReadOnlyAccess |
|---|---|---|---|
| Agregar o eliminar etiquetas de almacén por lotes | √ | √ | × |
| Adición de etiquetas de almacén | √ | √ | × |
| Edición de etiquetas | √ | √ | × |

## Enlaces útiles

- **Descripción general del servicio de IAM**
- **Creación de un grupo de usuarios y usuarios y concesión de permisos CBR**
- **Políticas de permisos y acciones admitidas**

# 9 Restricciones

## General

- Un almacén solo puede asociarse a una política de copia de respaldo.
- Un almacén solo puede asociarse a una política de replicación.
- Un almacén puede asociarse con un máximo de 256 recursos.
- Se puede crear un máximo de 32 políticas de copia de respaldo y 32 políticas de replicación.
- Sólo se pueden utilizar las copias de respaldo de un almacén cuyo estado es **Available** o **Locked** para la restauración de datos.
- Las copias de respaldo de un almacén cuyo estado es **Deleting** no se pueden eliminar.
- Las copias de respaldo no se pueden descargar en un PC local ni subir a OBS.
- Un almacén y sus servidores o discos asociados deben estar en la misma región.
- No se admite la restauración de datos simultánea.

## Copia de respaldo de disco en la nube

- Solo se puede realizar una copia de respaldo de los discos en el estado **Available** o **In-use**.
- No se puede realizar una copia de respaldo de los discos congelados durante el período de retención.
- Un disco nuevo debe ser al menos tan grande como el disco de origen de la copia de respaldo.
- Las copias de respaldo de disco en la nube no se pueden replicar en otras regiones.

## Copia de respaldo de servidor en la nube

- Se puede realizar una copia de respaldo de los discos compartidos en un servidor, pero no puede haber más de 10 discos compartidos.
- Sólo se pueden utilizar las copias de respaldo de un almacén cuyo estado sea **Available** o **Locked** para crear imágenes y replicarse en otra región.
- Los servidores congelados en el período de retención no se pueden realizar copias de respaldo.
- Se admiten copias de respaldo consistentes en bloqueos para varios discos y copias de respaldo consistentes en aplicaciones para servidores de bases de datos.

- Puede optar por hacer una copia de respaldo solo de los discos especificados en un servidor, pero dicha copia de respaldo de los discos debe restaurarse como un todo. No se admite la restauración a nivel de archivo o directorio.
- Las imágenes no se pueden crear mediante copias de respaldo si la cantidad de recursos asociados a un almacén de copias de respaldo del servidor excede la cuota.
- Se recomienda no realizar copias de respaldo de un servidor cuyo tamaño de disco supere los 4 TB.
- Las copias de respaldo se pueden replicar en regiones que admitan la replicación. Las limitaciones de replicación son las siguientes:
  - Una copia de respaldo sólo se puede replicar si cumple todas las condiciones siguientes:
    i. Es una copia de respaldo de ECS.
    ii. Contiene datos del disco del sistema.
    iii. Se encuentra en el estado **Available**.
  - Solo se pueden replicar las copias de respaldo. Las réplicas de copia de respaldo no se pueden replicar de nuevo, pero se pueden utilizar para crear imágenes.
  - Una copia de respaldo se puede replicar en varias regiones de destino, pero solo puede tener una réplica en cada región de destino. La regla de replicación varía con el método de replicación:
    - Replicación manual: se puede replicar una copia de respaldo en la región de destino siempre que no tenga réplica en la región de destino. Una copia de respaldo se puede replicar de nuevo si se ha eliminado su réplica en la región de destino.
    - Replicación basada en políticas: una vez que una copia de respaldo se ha replicado correctamente en la región de destino, no se puede replicar de nuevo en esa región, incluso si se ha eliminado su réplica.
  - Sólo se pueden seleccionar regiones con capacidades de replicación como regiones de destino.

## Copia de respaldo SFS Turbo

- Sólo se pueden realizar copias de respaldo de los sistemas de archivos en el estado **Available**.
- No se puede utilizar una copia de respaldo del sistema de archivos SFS Turbo para restaurar los datos en el sistema de archivos original.
- Las copias de respaldo se pueden replicar en regiones que admitan la replicación. Las limitaciones de replicación son las siguientes:
  - Una copia de respaldo sólo se puede replicar si cumple todas las condiciones siguientes:
    i. Se genera para un sistema de archivos SFS Turbo.
    ii. Se encuentra en el estado **Available**.
  - Solo se pueden replicar las copias de respaldo. Las réplicas de backup no se pueden replicar de nuevo, pero se pueden utilizar para crear sistemas de archivos SFS Turbo.
  - Una copia de respaldo se puede replicar en varias regiones de destino, pero solo puede tener una réplica en cada región de destino. La regla de replicación varía con el método de replicación:

    - Replicación manual: se puede replicar una copia de respaldo en la región de destino siempre que no tenga réplica en la región de destino. Una copia de respaldo se puede replicar de nuevo si se ha eliminado su réplica en la región de destino.
    - Replicación basada en políticas: una vez que una copia de respaldo se ha replicado correctamente en la región de destino, no se puede replicar de nuevo en esa región, incluso si se ha eliminado su réplica.
  - Sólo se pueden seleccionar regiones con capacidades de replicación como regiones de destino.

## Copia de respaldo de nube híbrida

- Las copias de respaldo sincronizadas con la nube no se pueden utilizar para crear servidores en la nube.
- Las copias de respaldo de almacenamiento solo se pueden restaurar en discos de datos en servidores en la nube.

## Copia de respaldo de archivos

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

# 10 CBR y otros servicios

## Servicios relacionados con CBR

**Tabla 10-1** Servicios relacionados con CBR

| Función | Servicios relacionados | Referencia |
| --- | --- | --- |
| CBR realiza copias de respaldo de los datos de los discos en un ECS y restaura los datos de copia de respaldo en los discos de un ECS para restaurar los datos perdidos o dañados. Las copias de respaldo generadas se pueden utilizar para crear imágenes para restaurar rápidamente los entornos en ejecución de servicios. | ECS | **Creación de una copia de respaldo de servidor en la nube**<br>**Creación de una copia de respaldo de disco en nube** |
| CBR realiza copias de respaldo de los datos de los discos en un BMS y restaura los datos de copia de respaldo en los discos de un BMS para restaurar los datos perdidos o dañados. Los procesos de copia de respaldo y gestión para BMS y ECS son los mismos. | BMS | **2 Qué es CBR**<br>**Creación de una copia de respaldo de servidor en la nube** |
| CBR realiza copias de respaldo de los datos de los sistemas de archivos SFS Turbo. Puede utilizar los datos de copia de respaldo para crear nuevos sistemas de archivos para restaurar los datos perdidos o dañados. | SFS | **Creación de una copia de respaldo de SFS Turbo** |
| CBR almacena los datos de copia de respaldo en OBS para mejorar la seguridad de los datos de copia de respaldo. | OBS | **2 Qué es CBR** |
| CBR realiza copias de respaldo de los datos en discos. Puede utilizar los datos de copia de respaldo para crear nuevos discos. | EVS | **Creación de una copia de respaldo de disco en nube** |

| Función | Servicios relacionados | Referencia |
| --- | --- | --- |
| Cloud Trace Service (CTS) registra las operaciones en recursos de CBR, facilitando futuras consultas, auditorías y seguimiento. | CTS | **Auditoría** |
| Data Express Service (DES) le proporciona un servicio de transmisión de datos seguro, rápido y eficiente. Resuelve el problema de la migración masiva de datos a la nube. Después de realizar una copia de respaldo de una máquina virtual de VMware en las instalaciones, puede usar DES para transmitir los datos de copia de respaldo mediante teletransportes o discos a un bucket OBS. A continuación, puede sincronizar los datos de copia de respaldo en el bucket OBS con un almacén CBR en la consola para la gestión basada en la nube. | DES | **Creación de una unidad de almacenamiento** |
| IAM es un sistema de autoservicio para que las empresas administren recursos en la nube. Proporciona funciones de gestión de identidad de usuario y control de acceso. Cuando varios usuarios de una empresa necesitan usar CBR, el administrador de la empresa puede usar IAM para crear usuarios y controlar los permisos de estos usuarios en los recursos de la empresa. | IAM | **8 Gestión de permisos** |
| Tag Management Service (TMS) le permite agregar etiquetas preestablecidas a los almacenes CBR para facilitar el filtrado y la gestión. | TMS | **Gestión de etiquetas de almacén** |

# 11 Conceptos Básicos



## 11.1 Conceptos de CBR

### Almacén

CBR utiliza almacenes para almacenar copias de respaldo. Los almacenes pueden ser almacenes de copia de respaldo o almacenes de replicación.

- Un almacén de copias de respaldo es un contenedor que almacena copias de respaldo de recursos como servidores y discos. Los almacenes de copia de respaldo se clasifican en los siguientes tipos:
  - **Server backup vaults**: incluyen aquellas que solo almacenan copias de respaldo de servidores comunes y aquellas que almacenan copia de respaldos de servidores de bases de datos. Puede asociar servidores a un almacén de copias de respaldo de servidor y aplicar una política de copia de respaldo o replicación al almacén. También puede replicar copias de respaldo de un almacén en una región a un almacén de replicación en otra región. Las copias de respaldo del servidor se pueden utilizar para restaurar los datos del servidor.
  - **Disk backup vaults**: almacene solo copias de respaldo en disco. Puede asociar discos a un almacén de copias de respaldo de disco y aplicar una política de copia de respaldo al almacén.
  - **SFS Turbo backup vaults**: almacene solo copias de respaldo de sistemas de archivos SFS Turbo. Puede asociar sistemas de archivos a un almacén de copias de respaldo SFS Turbo y aplicar una política de copia de respaldo al almacén.
  - **Hybrid cloud backup vaults**: almacene copias de respaldo sincronizadas desde los sistemas de almacenamiento OceanStor Dorado y VMware VMs. Puede replicar copias de respaldo en un almacén de replicación de otra región y restaurar los datos de copia de respaldo en otros servidores. También pueden almacenar las copias de respaldo de archivos y directorios en sus servidores en la nube y hosts locales. No es necesario realizar copias de respaldo de todos los servidores o discos.

- Los almacenes de replicación solo almacenan réplicas de copia de respaldos. Tales réplicas no se pueden replicar de nuevo. Los almacenes de replicación para backups de servidores incluyen aquellos que almacenan sólo réplicas de backups comunes y aquellos que almacenan réplicas de backups compatibles con las aplicaciones.

## Copia de respaldo

Una copia de respaldo es una copia de un chunk particular de datos y generalmente se almacena en otro lugar de modo que puede usarse para restaurar los datos originales en caso de pérdida de datos. Se puede generar manualmente mediante una tarea de copia de respaldo única o automáticamente mediante una tarea periódica.

CBR admite copias de respaldo únicas y copias de respaldo periódicas. Una tarea de copia de respaldo única es creada manualmente por los usuarios y se ejecuta una sola vez. Las tareas de copia de respaldo periódica se ejecutan automáticamente en función de una política de copia de respaldo definida por el usuario.

- El nombre de una copia de respaldo única es **manualbk_***xxxx*. Puede ser definido por el usuario o por el sistema.
- El nombre de una copia de respaldo periódica es **autobk_***xxxx*, que es asignada automáticamente por el sistema.

## Política de copia de respaldo

Una política de copia de respaldo es un conjunto de reglas para realizar copias de respaldo de datos, incluido el nombre de la política, el estado de la política, el tiempo de ejecución de las tareas de copia de respaldo, la frecuencia de copia de respaldo y la regla de retención. Una regla de retención especifica cuánto tiempo se conservan las copias de respaldo o el número de copias de respaldo que se conservan. Las copias de respaldo automáticas se pueden realizar aplicando una política de copias de respaldo a un almacén de copias de respaldo.

## Replicación

La replicación es el proceso de replicación de datos de copia de respaldo de una región de origen a una región de destino. Puede utilizar réplicas de copia de respaldo en la región de destino para crear imágenes y aprovisionar servidores.

Las copias de respaldo de servidores en la nube y las copias de respaldo en la nube híbrida admiten la replicación manual para una sola copia de respaldo. También puede configurar reglas de replicación en una política para replicar periódicamente copias de respaldo, que se generan en función de la política y que no se han replicado o no se han replicado en la región de destino.

Por ejemplo, si desea realizar una copia de respaldo de un servidor, seleccione **Backup** para el tipo de protección del almacén. Si desea replicar copias de respaldo del servidor de la región 1 a la región 2, el almacén de destino de la región 2 debe ser del tipo de protección de **Replication**.

## Restauración instantánea

Restauración instantánea es una función para restaurar datos y crear imágenes a partir de copias de respaldo. La restauración instantánea es mucho más rápida que un proceso de restauración normal.

Las copias de respaldo comunes no admiten restauración instantánea, mientras que las copias de respaldo mejoradas sí. De forma predeterminada, todas las copias de respaldo de CBR son copias de respaldo mejoradas. En comparación con las copias de respaldo comunes, las copias de respaldo mejoradas consumen menos tiempo para restaurar datos del servidor o crear imágenes.

## Copia de respaldo mejorada

Las copias de respaldo mejoradas se pueden utilizar para restaurar rápidamente los datos del servidor o crear imágenes. Este tipo de copias de respaldo depende de Restauración instantánea.

Antes de implementar la restauración instantánea, todas las copias de respaldo de CBR generadas son copias de respaldo comunes. Después de implementar la restauración instantánea, todas las copias de respaldo de CBR generadas son copias de respaldo mejoradas. Esta es una actualización de rendimiento general de CBR, y no se requiere ninguna configuración adicional. Actualmente, todas las copias de respaldo de CBR generadas son copias de respaldo mejoradas.

Se necesita más tiempo para restaurar los datos del servidor o crear imágenes usando copias de respaldo comunes. Las copias de respaldo mejoradas pueden hacer lo mismo con un tiempo significativamente más corto. La única diferencia entre las copias de respaldo comunes y las copias de respaldo mejoradas es la velocidad de restauración.

## Copias de respaldo consistentes con la aplicación

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

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

La copia de respaldo del servidor en la nube CBR admite tanto la copia de respaldo consistente en bloqueos como la copia de respaldo consistente en aplicaciones (también llamada copia de respaldo del servidor de base de datos). Instale el agente antes de habilitar la copia de respaldo compatible con las aplicaciones para evitar que la copia de respaldo del servidor de base de datos falle.

### Copia de respaldo completa periódica

De forma predeterminada, CBR realiza una copia de respaldo completa de un recurso en la copia de respaldo inicial y copias de respaldo incrementales en todas las copias de respaldo posteriores.

CBR ahora le permite implementar copias de respaldo completas periódicas además de la copia de respaldo inicial. Puede configurar una política para realizar una copia de respaldo completa después de cada N copias de respaldo incrementales. Esto mejora aún más la respaldo de los datos de copia de respaldo y cumple con las necesidades periódicas de copia de respaldo completa.

Las copias de respaldo completos periódicos ocupan más espacio de almacenamiento que las copias de respaldo incrementales.

## 11.2 Proyecto y proyecto empresarial

### Proyecto

Un proyecto se utiliza para agrupar y aislar recursos de OpenStack como los recursos de cómputo, almacenamiento y red. Un proyecto puede ser un departamento o un equipo de proyecto. Se pueden crear varios proyectos para una cuenta.

### Proyecto empresarial

Un proyecto de empresa administra varias instancias de recursos por categoría. Los recursos y proyectos en diferentes regiones de servicios en la nube se pueden clasificar en un solo proyecto empresarial. Una empresa puede clasificar los recursos según el departamento o el grupo de proyecto y poner los recursos relevantes en un proyecto empresarial para la gestión. Los recursos se pueden migrar entre proyectos empresariales.

## 11.3 Región y AZ

### Concepto

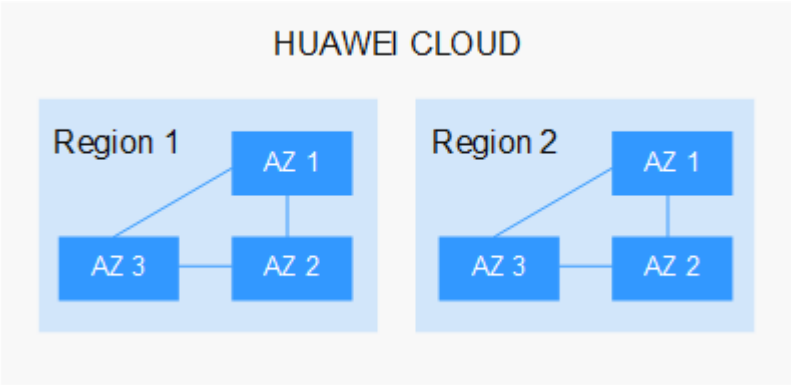
Una región y una zona de disponibilidad (AZ) identifican la ubicación de un centro de datos. Puede crear recursos en una región específica y AZ.

- Las regiones se dividen en función de la ubicación geográfica y la latencia de la red. Los servicios públicos, como Elastic Cloud Server (ECS), Elastic Volume Service (EVS), Object Storage Service (OBS), Virtual Private Cloud (VPC), Elastic IP (EIP) y Image Management Service (IMS), se comparten dentro de la misma región. Las regiones se clasifican en regiones universales y regiones dedicadas. Una región universal proporciona servicios en la nube universales para los tenants estándares. Una región dedicada proporciona servicios específicos para tenants específicos.
- Una AZ contiene uno o más centros de datos físicos. Cada AZ cuenta con instalaciones independientes de electricidad, de refrigeración, de extinción de incendios y a prueba de humedad. Dentro de una AZ, los recursos de computación, red, almacenamiento y otros se dividen de forma lógica en múltiples clústeres. Las AZ dentro de una región están interconectadas usando fibras ópticas de alta velocidad, para soportar sistemas de alta disponibilidad entre las AZ.

**Figura 11-1** muestra la relación entre regiones y AZ.

**Figura 11-1** Las regiones y las AZ




Huawei Cloud ofrece servicios en muchas regiones de todo el mundo. Seleccione una región y AZ según los requisitos. Para obtener más información, consulte **Regiones globales de Huawei Cloud**.

## Selección de una región

Al seleccionar una región, tenga en cuenta los siguientes factores:

- Localización

  Se recomienda seleccionar la región más cercana para una menor latencia de red y un acceso rápido. Las regiones dentro de China continental proporcionan la misma infraestructura, calidad de red BGP, así como operaciones de recursos y configuraciones. Por lo tanto, si sus usuarios objetivo están en China continental, no es necesario tener en cuenta las diferencias de latencia de la red al seleccionar una región.

  – Si sus usuarios objetivo se encuentran en Asia Pacífico (excepto China continental), seleccione la región **CN-Hong Kong**, **AP-Bangkok**, or **AP-Singapore**.

  – Si sus usuarios objetivo se encuentran en África, seleccione la región **AF-Johannesburg**.

  – Si sus usuarios objetivo están en América Latina, seleccione la región **LA-Santiago**.

  NOTA

  La región **LA-Santiago** se encuentra en Chile.

- Precio del recurso

  Los precios de los recursos pueden variar en diferentes regiones. Para obtener más información, consulte **Detalles de precios del producto**.

## Selección de una AZ

Al implementar recursos, tenga en cuenta los requisitos de las aplicaciones en cuanto a la recuperación ante desastres (DR) y la latencia de la red.

- Para una alta capacidad de DR, implemente recursos en diferentes AZ dentro de la misma región.

- Para una menor latencia de red, implemente recursos en la misma AZ.

## Regiones y endpoint

Antes de usar una API para llamar a recursos, especifique su región y endpoint.

# 12 Historial de cambios

| Lanzado en | Descripción |
| --- | --- |
| 2022-07-20 | Esta edición es el sexto lanzamiento oficial.<br>Se ha actualizado el siguiente contenido:<br>Agregó el contenido de la copia de respaldo de archivos. |
| 2021-10-27 | Esta edición es el quinto lanzamiento oficial.<br>Se ha actualizado el siguiente contenido:<br>Agregó el contenido de la gestión de permisos. |
| 2020-08-07 | Esta edición es el cuarto lanzamiento oficial.<br>Se ha actualizado el siguiente contenido:<br>Agregó la descripción del pago atrasado en la sección "Facturación". |
| 2020-04-08 | Esta edición es el tercer lanzamiento oficial.<br>Se ha actualizado el siguiente contenido:<br>Agregó el contenido de la copia de respaldo del sistema de archivos. |
| 2020-03-31 | Esta versión es el segundo lanzamiento oficial.<br>Se ha actualizado el siguiente contenido:<br>Se agregó la sección "Facturación." |
| 2019-07-31 | Esta versión es el primer lanzamiento oficial. |