Cloud Backup and Recovery

Visão geral de serviço

Edição 01

Data 24-02-2023

HUAWEI

HUAWEI TECHNOLOGIES CO., LTD.

Marcas registadas e permissões


e outras marcas registadas da Huawei são marcas registadas da Huawei Technologies Co., Ltd. Todos as outras marcas registadas e os nomes registados mencionados neste documento são propriedade dos seus respectivos detentores.

Aviso

Os produtos, serviços e funcionalidades adquiridos são estipulados pelo contrato feito entre a Huawei e o cliente. Todos ou parte dos produtos, serviços e funcionalidades descritos neste documento pode não estar dentro do âmbito de aquisição ou do âmbito de uso. Salvo especificação em contrário no contrato, todas as declarações, informações e recomendações neste documento são fornecidas "TAL COMO ESTÁ" sem garantias, ou representações de qualquer tipo, seja expressa ou implícita.

As informações contidas neste documento estão sujeitas a alterações sem aviso prévio. Foram feitos todos os esforços na preparação deste documento para assegurar a exatidão do conteúdo, mas todas as declarações, informações e recomendações contidas neste documento não constituem uma garantia de qualquer tipo, expressa ou implícita.

Huawei Technologies Co., Ltd.

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

Site: https://www.huawei.com

Email: support@huawei.com

Índice

1 Infográficos do CBR

2 O que é o CBR?

Visão geral

Cloud Backup and Recovery (CBR) permite que você faça backup de Elastic Cloud Servers (ECSs), Bare Metal Servers (BMSs), discos do Elastic Volume Service (EVS), Sistemas de arquivos SFS Turbo, arquivos e diretórios locais e ambientes virtuais VMware locais com facilidade. No caso de um ataque de vírus, uma exclusão acidental ou uma falha de software/hardware, você poderá restaurar os dados para qualquer ponto no tempo em que um backup dos dados tenha sido feito.

O CBR protege seus serviços, garantindo a segurança e a consistência de seus dados.

Arquitetura do produto

O CBR consiste em backups, cofres e políticas.

Backup

Um backup é uma cópia de um determinado pedaço de dados e geralmente é armazenado em outro lugar para que ele possa ser usado para restaurar os dados originais em caso de perda de dados. A seguir estão os tipos de backups do CBR:

- Backup de disco em nuvem. Esse tipo de backup fornece proteção de dados baseada em snapshot para discos do EVS.
- Backup de servidor em nuvem. Esse tipo de backup usa a tecnologia de snapshot de consistência para discos para proteger dados dos ECS e dos BMSs. Os backups de servidores sem bancos de dados implantados são backups comuns de servidores, e os de servidores com bancos de dados implantados são backups consistentes com a aplicação.
- Backups do SFS Turbo Esse tipo de backup protege os dados dos sistemas de arquivos do SFS Turbo.
- Backup em nuvem híbrida Esse tipo de backup protege os dados dos sistemas de armazenamento locais do OceanStor Dorado e das máquinas virtuais da VMware armazenando seus backups em nuvem. Você pode gerenciar os backups no console do CBR.
- Backup de arquivos: esse tipo de backup protege os dados de um ou vários arquivos dos seus servidores em nuvem ou hosts locais. Você não precisa fazer backup de servidores ou discos inteiros.

Cofre

O CBR usa cofres para armazenar backups. Antes de criar um backup, você precisa de criar pelo menos um cofre e associar o recurso que deseja fazer backup ao cofre. Em seguida, os backups de recursos gerados são armazenados no cofre associado.

Os cofres podem ser cofres de backup ou cofres de replicação. Os cofres de backup armazenam backups, enquanto os cofres de replicação armazenam réplicas de backups.

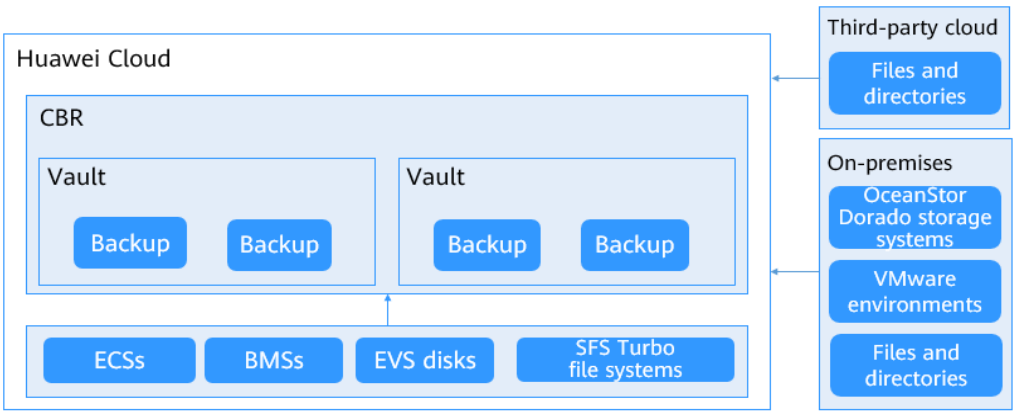
Os backups de diferentes tipos de recursos devem ser armazenados em diferentes tipos de cofres.

Política

As políticas são divididas em políticas de backup e políticas de replicação.

- Políticas de backup: para executar backups automáticos, configure uma política de backup definindo os tempos de execução das tarefas de backup, o ciclo de backup e as regras de retenção e, em seguida, aplique a política a um cofre.
- Políticas de replicação: para replicar automaticamente backups ou cofres, configure uma política de replicação definindo os tempos de execução das tarefas de replicação, o ciclo de replicação e as regras de retenção e, em seguida, aplique a política a um cofre. As réplicas de backup devem ser armazenadas em cofres de replicação.

Figura 2-1 Arquitetura do CBR



Diferenças entre os tipos de backup

Tabela 2-1 Diferenças entre os tipos de backup

Item	Backup de servidor em nuvem	Backup de disco em nuvem	Backups de SFS Turbo	Backup em nuvem híbrida	Backups de arquivos
Objeto de backup e restauração	Todos os discos (discos de sistema e de dados) em um servidor	Um ou mais discos especificados (sistema ou discos de dados)	Sistema de arquivos do SFS Turbo	Backups sincronizados a partir de software de backup local e VMs	Um único ou vários arquivos de servidores em nuvem e hosts locais
Cenário recomendado	Um servidor de nuvem inteiro precisa ser protegido.	Somente os discos de dados precisam ser copiados, porque o disco do sistema não contém dados de aplicativos dos usuários.	Os dados nos sistemas de arquivos do SFS Turbo precisam de ser protegidos.	Backups para servidores locais precisam de ser gerenciados e restaurados em nuvem.	Os dados em um único ou vários arquivos precisam de ser protegidos e podem ser rapidamente copiados e restaurados na nuvem.
Vantagens	Todos os discos em um servidor são copiados ao mesmo tempo, garantindo a consistência dos dados.	O custo de backup é reduzido sem comprometer a segurança dos dados.	Os dados de backup e os sistemas de arquivos originais são armazenados separadamente. Você pode usar os dados de backup para criar um novo sistema de arquivos	Dados locais podem ser copiados para nuvem e usados para recriar serviços em nuvem.	Os dados podem ser copiados por arquivo ou diretório. Você não precisa de fazer backup de seus servidores ou discos inteiros, reduzindo assim os custos de backup.

Mecanismo de backup

Os backups na nuvem do CBR oferecem backup em nível de bloco, e o backup de arquivos do CBR fornece backup em nível de arquivo. Um backup completo é executado apenas para o primeiro backup e faz backup de todos os blocos de dados usados. Por exemplo, se o tamanho de um disco for 100 GB e o espaço usado for 40 GB, o backup de 40 GB de dados será feito. Um backup incremental faz backup apenas dos dados alterados desde o último backup, o que é eficiente em termos de armazenamento e tempo. Quando um backup é excluído, somente os blocos de dados que não dependem de outros backups são excluídos, para que outros backups ainda possam ser usados para restauração. Tanto um backup completo quanto um backup incremental podem restaurar dados para o estado em um determinado ponto de backup no tempo.

Ao criar um backup de um disco, o CBR também cria um snapshot para ele. Sempre que um novo backup em disco é criado, o CBR exclui o snapshot antigo e mantém apenas o snapshot mais recente.

O CBR armazena dados de backup no OBS, aumentando a segurança dos dados de backup.

Opções de backup

O CBR suporta backup único e backup periódico. Uma tarefa de backup única é criada manualmente pelos usuários e é executada apenas uma vez. As tarefas de backup periódico são executadas automaticamente com base em uma política de backup definida pelo usuário.

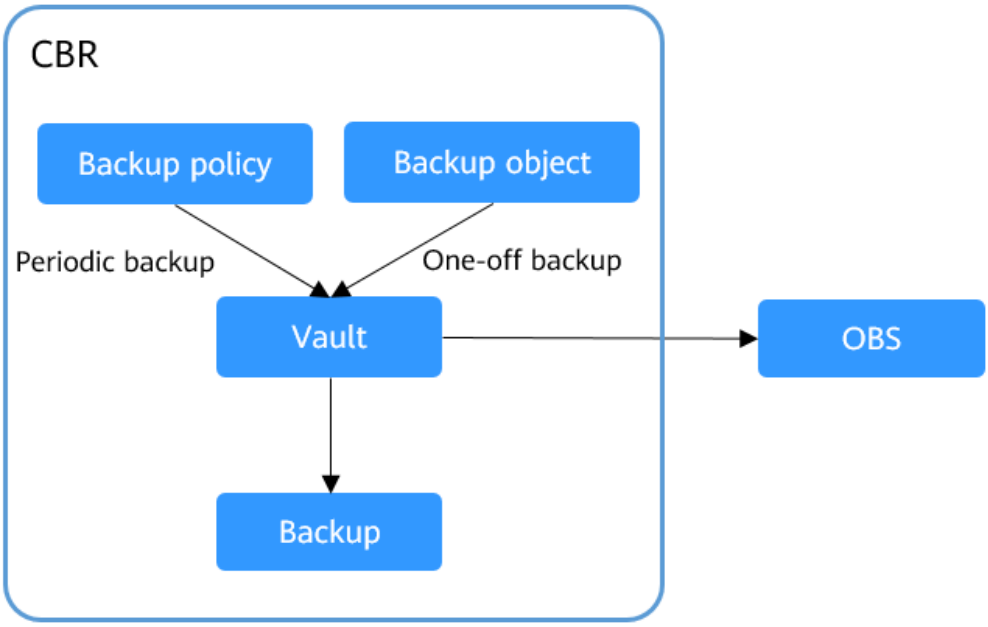
Tabela 2-2 descreve as duas opções de backup.

Tabela 2-2 Backup único e backup periódico

Item	Backup único	Backup periódico
Política de backup	Não necessário	Necessário
Número de tarefas de backup	Uma tarefa de backup manual	Tarefas periódicas orientadas por uma política de backup
Nome do backup	Nome de backup definido pelo usuário, que é **manualbk**_*xxxx* por padrão	Nome de backup atribuído pelo sistema, que é **autobk**_*xxxx* por padrão
Modo de backup	Backup completo pela primeira vez e backup incremental posteriormente, por padrão	Backup completo pela primeira vez e backup incremental posteriormente, por padrão
Cenário de aplicação	Executado antes de corrigir ou atualizar o SO ou atualizar um aplicativo em um recurso. Um backup único pode ser usado para restaurar o recurso para o estado original se a correção ou atualização falhar.	Executado para manutenção de rotina de um recurso. O backup mais recente pode ser usado para restauração se ocorrer uma falha inesperada ou perda de dados.

Você também pode usar as duas opções de backup juntas, se for necessário. Por exemplo, é possível associar recursos a um cofre e aplicar uma política de backup ao cofre para executar backup periódico para todos os recursos no cofre. Além disso, você pode realizar backup para os recursos mais importantes sob demanda para melhorar a segurança dos dados. **Figura 2-2** mostra o uso misto das duas opções de backup.

Figura 2-2 Uso misto das duas opções de backup



Método de acesso

Você pode acessar o serviço do CBR por meio do console ou chamada de APIs baseadas em HTTPS.

- Console

  Use o console se preferir uma IU baseada na Web para executar operações. Faça logon no console e escolha **Cloud Backup and Recovery**.

- APIs

  Use APIs se precisar de integrar o CBR a um sistema de terceiros para desenvolvimento secundário. Para obter detalhes, consulte **Referência de API do Cloud Backup and Recovery**.

3 Vantagens

Confiável

O CBR suporta backup consistente com falhas para vários discos em um servidor e backup consistente com a aplicação para servidores de banco de dados, garantindo a segurança e a confiabilidade dos dados.

Eficiente

Os backups incrementais permanentes reduzem o tempo necessário para o backup em 95%. Com a Restauração instantânea, o CBR oferece suporte a RPOs de até 1 hora e RTO em minutos.

NOTA

O Objetivo de ponto de recuperação (RPO) especifica o período máximo aceitável em que os dados podem ser perdidos.

O Objetivo de tempo de recuperação (RTO) especifica o tempo máximo aceitável para a restauração de todo o sistema após um desastre.

Facilidade de uso

Você pode concluir a configuração de backup em apenas três etapas e não são necessárias habilidades profissionais de software de backup. O CBR é mais fácil de usar do que os sistemas de backup convencionais.

Seguro

Os dados de backup de discos criptografados são criptografados automaticamente para garantir a segurança de dados. Você pode replicar e restaurar dados de backup entre regiões para implementar a recuperação remota de desastres.

4 Cenários de aplicação

O CBR faz backup de recursos para maximizar a segurança e a consistência dos dados do usuário e garantir a continuidade do serviço. O CBR é adequado para backup e restauração de dados.

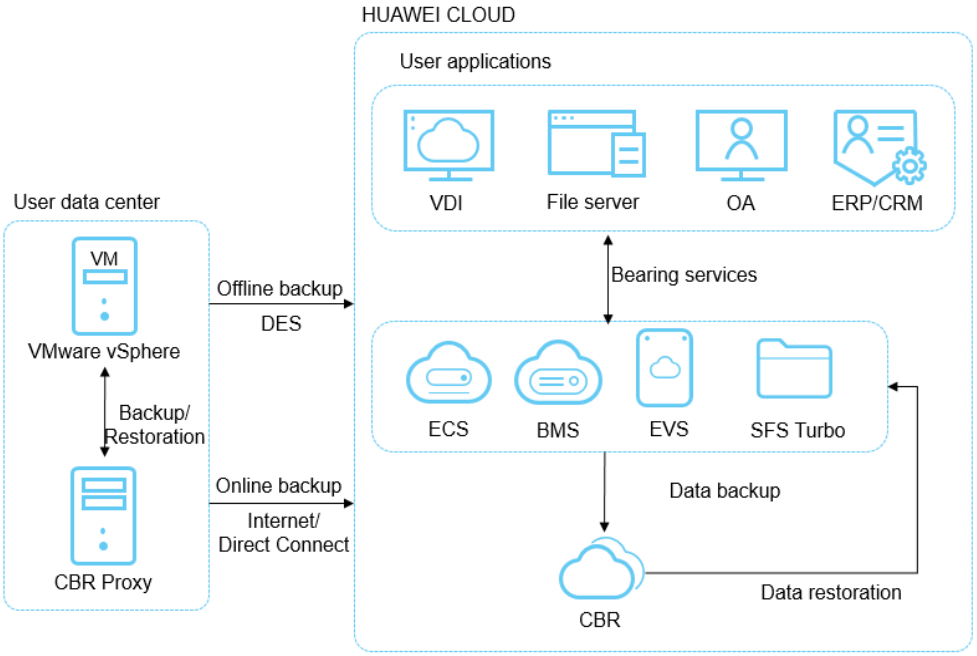
Backup e restauração de dados

O CBR pode ser usado para restaurar dados rapidamente nos seguintes cenários:

- ataques de hackers ou vírus
- eliminação acidental
- erro de atualização do aplicativo
- avarias do sistema

  Para qualquer um dos incidentes acima, você pode usar o CBR para restaurar dados para o ponto de backup mais recente antes do incidente.

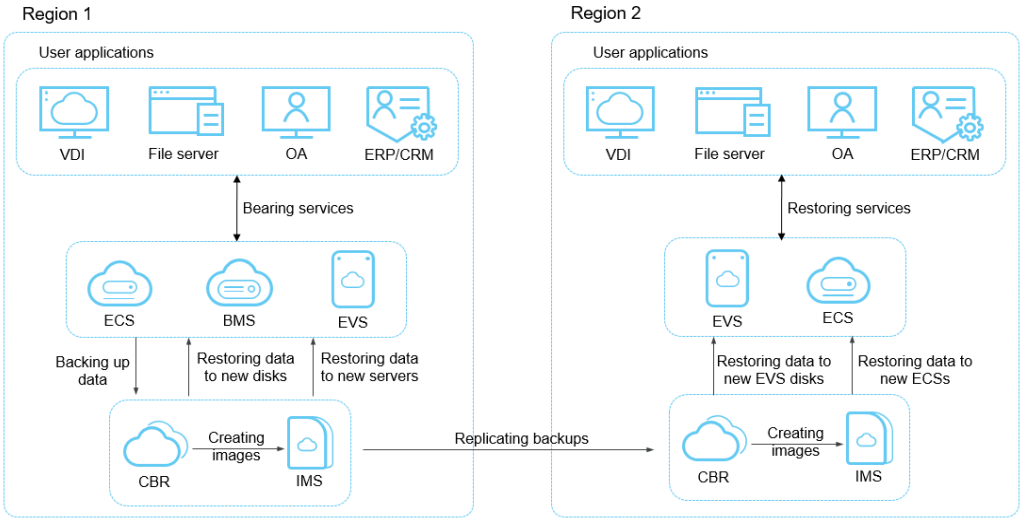
Figura 4-1 Backup e restauração de dados



Migração e implantação rápidas de serviços

Você pode usar backups de servidor em nuvem para criar imagens e, em seguida, usar essas imagens para provisionar rapidamente novos servidores em nuvem com a mesma configuração dos existentes. Consulte **Figura 4-2**.

Figura 4-2 Migração e implantação rápidas de serviços



5 Funções

Tabela 5-1 lista as funções básicas do CBR.

Antes de usar esse serviço, é recomendável que você vá para **conceitos básicos** para aprender mais sobre o CBR, como sobre cofre e política de backup.

Tabela 5-1 Funções básicas do CBR

Categoria	Função	Descrição
Backup de disco em nuvem	**Realização de backup de discos**	O backup de disco em nuvem fornece proteção de dados baseada em instantâneos para discos EVS. Você pode usar o CBR para fazer backup de um único disco em um servidor para proteger os dados nesse disco.
	Backup de dados orientado por políticas	Uma política de backup permite que um cofre execute automaticamente tarefas de backup em horários ou intervalos especificados. Backups periódicos podem ser usados para restaurar dados rapidamente contra corrupção ou perda de dados.
	Gerenciamento de backup	Quando uma tarefa de backup está em execução ou concluída, você pode definir critérios de pesquisa para filtrar backups da lista de backup para gerenciá-los e exibir seus detalhes.
	Restauração de dados de disco usando backups	Quando um disco está com defeito ou os dados do disco são perdidos devido a operações incorretas, você pode usar um backup para restaurar o disco.
	Criação de discos usando backups	Você pode usar um backup de disco para criar um disco. Depois que o disco é criado, os dados no novo disco são os mesmos que no backup em disco.

Categoria	Função	Descrição
	Compartilhamento de backups	Você pode compartilhar um backup de servidor ou disco com outras contas. Backups compartilhados podem ser usados para criar discos ou servidores.
Backup de servidor em nuvem	**Realização de backup de servidores**	Esse tipo de backup usa a tecnologia de snapshot de consistência para discos para proteger dados dos ECSs e dos BMSs. Você pode usar o CBR para fazer backup de um servidor inteiro para proteger os dados no servidor. É aconselhável usar o backup do servidor em nuvem em cenários que exigem alta consistência de dados, como clusters RAID.
	Realização de backup de discos em um servidor	Você pode fazer backup de discos em um servidor em um backup para economizar espaço do cofre de backup do servidor.
	Backup de dados orientado por políticas	Uma política de backup permite que um cofre execute automaticamente tarefas de backup em horários ou intervalos especificados. Backups periódicos podem ser usados para restaurar dados rapidamente contra corrupção ou perda de dados.
	Gerenciamento de backup	Quando uma tarefa de backup está em execução ou concluída, você pode definir critérios de pesquisa para filtrar backups da lista de backup para gerenciá-los e exibir seus detalhes.
	Restauração de dados de servidor usando backups	Quando um servidor está com defeito ou os dados do servidor são perdidos devido a operações incorretas, você pode usar um backup para restaurar o servidor.
	Compartilhamento de backups	Você pode compartilhar um backup de servidor ou disco com outras contas. Backups compartilhados podem ser usados para criar discos ou servidores.
	Criação de imagens usando backups	O backup de servidor em nuvem permite que você crie imagens usando backups do ECS. Você pode usar as imagens para provisionar ECSs para restaurar rapidamente ambientes em execução de serviços.

Categoria	Função	Descrição
	Realização de backup de servidores de banco de dados	O backup de servidor em nuvem oferece suporte ao backup consistente com aplicativos, além do backup consistente com falhas. O backup consistente com aplicativos garante a consistência dos dados do aplicativo fazendo backup de arquivos e discos exatamente ao mesmo tempo. Ele é adequado para fazer backup de ECSs, bem como os bancos de dados MySQL ou SAP HANA em execução neles.
	Replicação de backups entre regiões	O backup de servidor em nuvem permite que você replique backups gerados de uma região para outra. Você pode usar réplicas de backup na região de destino para criar imagens e provisionar servidores.
Backups de SFS Turbo	**Realização de backup de sistemas de arquivos do SFS**	O backup de SFS Turbo permite que você faça backup de sistemas de arquivos SFS Turbo. Um backup do sistema de arquivos do SFS Turbo pode ser usado para criar um novo sistema de arquivos do SFS Turbo, evitando a perda de dados importantes.
	Backup de dados orientado por políticas	Uma política de backup permite que um cofre execute automaticamente tarefas de backup em horários ou intervalos especificados. Backups periódicos podem ser usados para restaurar dados rapidamente contra corrupção ou perda de dados.
	Gerenciamento de backup	Quando uma tarefa de backup está em execução ou concluída, você pode definir critérios de pesquisa para filtrar backups da lista de backup para gerenciá-los e exibir seus detalhes.
	Criação de sistemas de arquivo usando backups	Você pode usar um backup do sistema de arquivos do SFS Turbo para criar um novo sistema de arquivos. Depois que ele é criado, os dados no novo sistema de arquivos são os mesmos que no backup.

Categoria	Função	Descrição
	Replicação de backups entre regiões	O backup do SFS Turbo permite replicar backups do sistema de arquivos do SFS Turbo de uma região para outra. Em seguida, você pode usar o backup replicado para criar um sistema de arquivos na região de destino.
backup na nuvem híbrida	**Sincronização de dados de backup de servidores locais**	Se o backup de VM VMware local tiver sido feito off-line e os dados de backup tiverem sido carregados em um bucket do OBS, você poderá sincronizar os dados de backup no bucket do OBS com um cofre de backup na nuvem híbrida para operações subsequentes.
	Restauração de dados em servidores usando backups	Depois que os backups são sincronizados com sucesso em um cofre de backup em nuvem híbrida, você pode restaurar os dados de backup em servidores em nuvem para recuperação de desastres, migração de serviços, desenvolvimento e testes.
Backups de arquivos	**Backing up files**	O backup de arquivos permite que você faça backup de arquivos e diretórios em seus servidores de nuvem e hosts locais. Você não precisa fazer backup de servidores ou discos inteiros.
	Restauração de dados usando backups	Se a perda de dados ocorreu em um arquivo local devido a exclusão acidental ou ataque de vírus, você pode usar os backups criados na nuvem para restaurar dados.

6 Segurança

6.1 Responsabilidades compartilhadas

Huawei garante que seu compromisso com a segurança cibernética nunca será superado pela consideração de interesses comerciais. Para lidar com os desafios emergentes de segurança na nuvem e ameaças e ataques à segurança na nuvem, a Huawei Cloud constrói um sistema abrangente de garantia de segurança de serviços em nuvem para diferentes regiões e indústrias com base nas vantagens exclusivas de software e hardware da Huawei, leis, regulamentos, padrões da indústria e ecossistema de segurança.

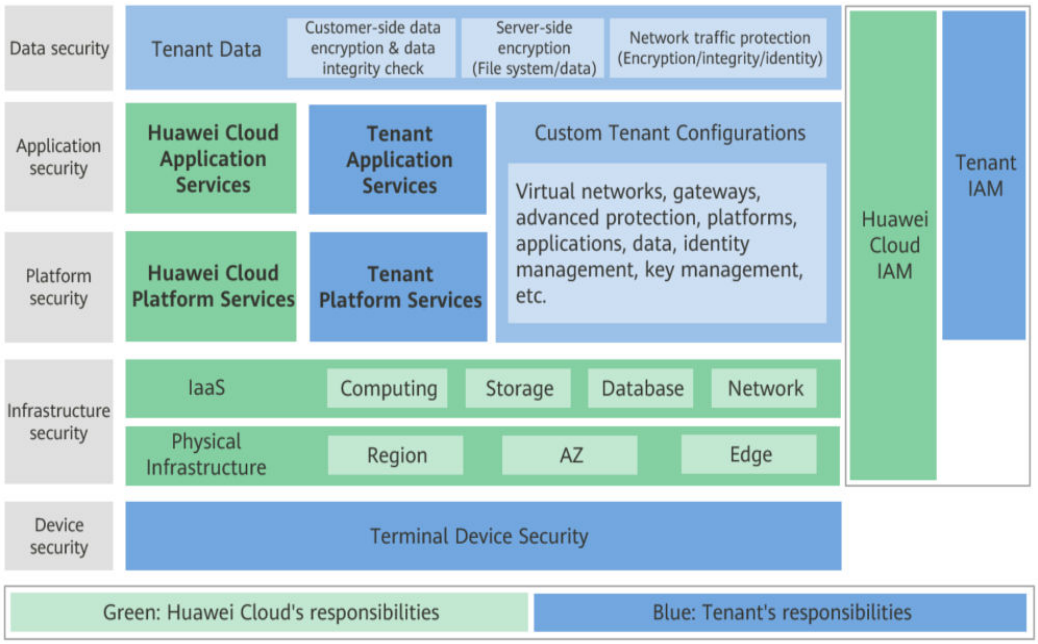
Figura 6-1 ilustra as responsabilidades partilhadas pela Huawei Cloud e pelos usuários.

- **Huawei Cloud**: garante a segurança dos serviços de nuvem e fornece nuvens seguras. As responsabilidades de segurança da Huawei Cloud incluem garantir a segurança de nossos serviços de IaaS, PaaS e SaaS, bem como os ambientes físicos dos data centers da Huawei Cloud onde nossos serviços de IaaS, PaaS e SaaS operam. A Huawei Cloud é responsável não apenas pelas funções de segurança e pelo desempenho de nossa infraestrutura, serviços de nuvem e tecnologias, mas também pela segurança geral de O&M na nuvem e, no sentido mais amplo, pela certificação de segurança de nossa infraestrutura e serviços.
- **Locatário**: usa a nuvem com segurança. Os locatários da Huawei Cloud são responsáveis pelo gerenciamento seguro e eficaz das configurações personalizadas dos serviços em nuvem, incluindo IaaS, PaaS e SaaS. Isso inclui, mas não se limita a, redes virtuais, o SO de hosts e convidados de máquinas virtuais, firewalls virtuais, API

Gateway, serviços avançados de segurança, todos os tipos de serviços em nuvem, dados de locatários, contas de identidade e gerenciamento de chaves.

O livro branco de segurança da Huawei Cloud elabora as ideias e medidas para a construção da segurança da Huawei Cloud, incluindo estratégias de segurança na nuvem, o modelo de responsabilidade compartilhada, conformidade e privacidade, organizações e pessoal de segurança, segurança de infraestrutura, serviço e segurança de locatários, segurança de engenharia, segurança de O&M e segurança do ecossistema.

Figura 6-1 Modelo de responsabilidade de segurança compartilhada da Huawei Cloud



6.2 Autenticação de identidade e controle de acesso

Você pode acessar o CBR por meio do console do CBR, das APIs e dos SDKs. Não importa qual método você escolher, você realmente usa APIs REST para acessar o CBR.

As APIs do CBR suportam apenas solicitações autenticadas. Você deve obter as informações de autenticação do IAM da Huawei Cloud antes de poder acessar o CBR. Para obter detalhes sobre a autenticação do IAM, consulte **Autenticação**.

6.3 Proteção de dados

O CBR toma muitas medidas para manter os dados seguros e confiáveis.

Tabela 6-1 Proteção de dados do CBR

Medida	Descrição
Criptografia de transmissão (HTTPS)	Para garantir a segurança da transmissão, os dados de backup são armazenados em buckets do OBS via HTTPS.

Medida	Descrição
Criptografia de dados de backup	Se um disco que você deseja fazer backup for criptografado, os backups gerados para esse disco também serão criptografados. Quando esse backup é usado para restaurar dados, os dados criptografados serão primeiro descriptografados e depois restaurados no disco de destino.
Replicação de entre regiões	A replicação entre regiões permite replicar backups de forma automática e assíncrona de uma região para um cofre de replicação em uma região diferente com base em uma política de replicação. Os recursos de recuperação de desastres entre regiões que ele oferece podem atender às suas necessidades de backup remoto.

6.4 Auditoria e registro em log

Auditoria

O Cloud Trace Service (CTS) registra as operações nos recursos em nuvem em sua conta. Você pode usar os logs gerados por CTS para realizar análises de segurança, rastrear alterações de recursos, auditar conformidade e localizar falhas.

Depois de ativar o CTS e configurar um rastreador, CTS pode registrar rastreamentos de gerenciamento e dados do CBR para auditoria.

Para obter detalhes sobre como habilitar e configurar o CTS, consulte **Primeiros passos do CTS**.

Para o gerenciamento do CBR e os rastreamentos de dados suportados pelo CTS, consulte **Auditoria**.

Registro em log

O CBR mostra tarefas de operações críticas na página de web. Você pode fazer logon no console do CBR, escolha **Tasks** na página de navegação à esquerda e exibir a lista de tarefas no painel direito. Alternativamente, você pode **consultar a lista de tarefas** por meio da API.

6.5 Resiliência

O CBR usa uma arquitetura de confiabilidade de vários níveis e fornece soluções técnicas, incluindo replicação entre regiões, para garantir durabilidade e confiabilidade dos dados.

6.6 Monitorização de riscos

O Cloud Eye é uma plataforma de monitoramento multidimensional que permite visualizar os usos de recursos e o status de execução do serviço e responder a exceções em tempo hábil para o bom funcionamento dos serviços.

O CBR usa o Cloud Eye para realizar o monitoramento de recursos e operações, ajudando você a monitorar seus cofres e backups e receber alarmes e notificações em tempo real. Você

pode obter o uso do seu cofre em tempo real e ser notificado por eventos, como falhas de criação ou exclusão de backup.

Para obter detalhes sobre as métricas CBR suportadas e como criar regras de alarme, consulte **Monitorização**.

6.7 Recuperação de falhas

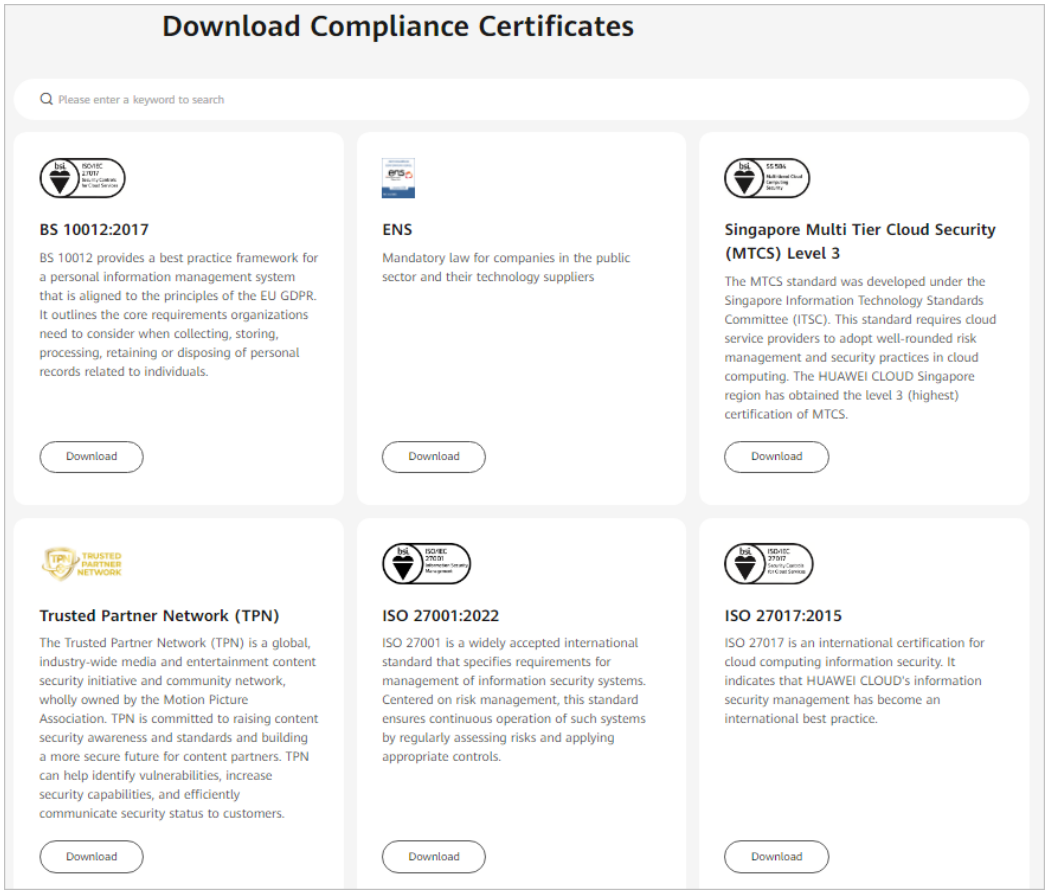
O CBR permite fazer backup e restaurar determinados recursos em nuvem, incluindo ECSs, discos do EVS, sistemas de arquivos do SFS Turbo e desktops de espaço de trabalho. Se algum desses tipos de recursos falhar, você poderá usar backups para restaurar a origem ou novos recursos, restaurando rapidamente dados e serviços. Para obter mais informações, consulte **Visão geral de função**.

6.8 Certificados

Certificados de conformidade

Os serviços e plataformas da Huawei Cloud obtiveram várias certificações de segurança e de conformidade das organizações autorizadas, como a Organização Internacional de Normalização (ISO). Você pode **baixá-los** do console.

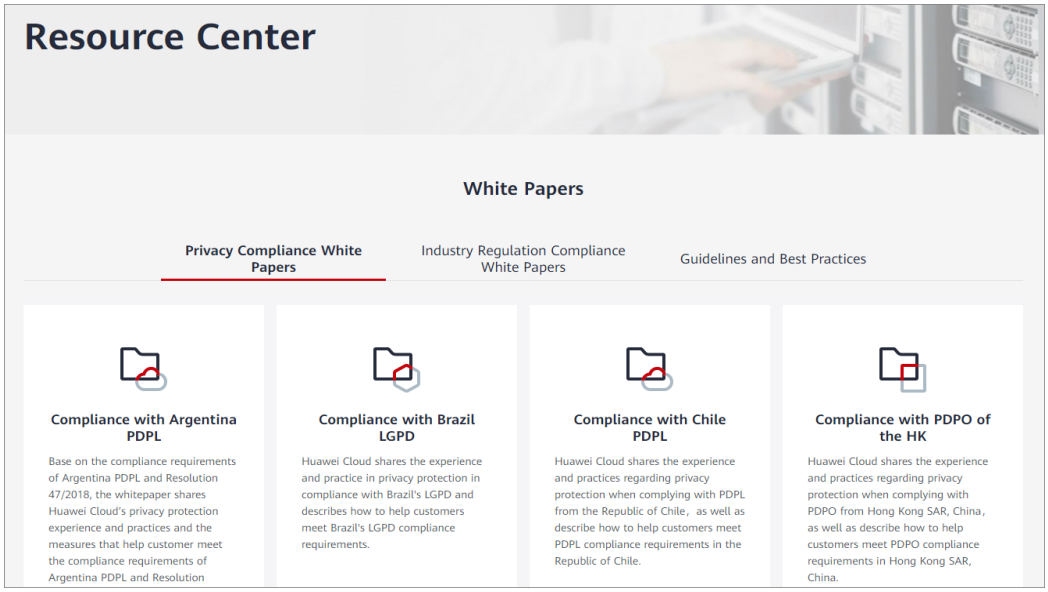
Figura 6-2 Download de certificados de conformidade



Central de recursos

A Huawei Cloud também fornece os seguintes recursos para ajudar os usuários a atender aos requisitos de conformidade. Para obter detalhes, consulte **Central de recursos**.

Figura 6-3 Central de recursos



7 Cobrança

Itens cobrados

Você será cobrado pelo espaço de armazenamento e pelo tráfego de dados gerado se a replicação de backup for usada. O preço do espaço de armazenamento varia de acordo com os tipos de cofre. Veja os detalhes na tabela a seguir.

Categoria	Item cobrado	Descrição	Modo de cobrança
Espaço de armazenamento	Cofre de backup de disco	Se os discos em nuvem precisarem de ser copiados, compre cofres de backup em disco para armazenar os backups gerados.	Pagamento por uso Anual/Mensal
	Cofre de backup de servidor	Se os servidores em nuvem (aplicações não incluídos) precisarem de ser copiados, compre cofres de backup do servidor para armazenar os backups gerados.	Pagamento por uso Anual/Mensal
	Cofres de backup do SFS Turbo	Se for necessário fazer backup dos sistemas de arquivos do SFS Turbo, compre cofres de backup do SFS Turbo para armazenar os backups gerados.	Pagamento por uso Anual/Mensal

Categoria	Item cobrado	Descrição	Modo de cobrança
	Cofre de backup de servidor de banco de dados	Se os servidores em nuvem (aplicações incluídos) precisarem de ser copiados, compre cofres de backup do servidor de banco de dados para armazenar os backups gerados. Como comprar: ative **Application-Consistent Backup** na página **Buy Server Backup Vault**. Para obter mais informações, consulte **Visão geral de backup consistente com a aplicação**.	Pagamento por uso Anual/Mensal
	Cofre de backup em nuvem híbrida	Se for necessário fazer backup de máquinas virtuais de VMware locais e matrizes de Dorado do OceanStor, compre cofres de backup em nuvem híbrida para armazenar os backups gerados.	Pagamento por uso Anual/Mensal
	Cofre de replicação	Se precisar de replicar backups para outra região, compre cofres de replicação na região de destino.	Pagamento por uso Anual/Mensal
Tráfego de dados	Tráfego de saída pela internet	Se os backups em nuvem e em nuvem híbrida forem usados para restaurar os dados em IDCs locais, o tráfego de saída pela Internet será gerado.	Gratuito por tempo limitado
	Tráfego de replicação entre regiões	Se backups ou cofres são replicados para outra região, o tráfego de replicação entre regiões é gerado na região de origem.	Pagamento por uso Anual/Mensal

NOTA

Para obter mais informações, consulte **Detalhes de preços do CBR**.

Exemplos de cobrança

Caso 1:

Cofre de pagamento por uso para servidores em nuvem sem bancos de dados implantados:

um usuário tem um servidor em nuvem de 100 GB e um cofre de backup de servidor de 400 GB comprado na região CN-Hong Kong e o servidor em nuvem está associado ao cofre. O usuário é cobrado pelo cofre de backup do servidor de 400 GB no CBR.

Caso 2:

Cofre de pagamento por uso para servidores em nuvem com bancos de dados implantados:

um usuário tem um servidor de nuvem de 100 GB executando bancos de dados e um cofre de backup de servidor de banco de dados de 800 GB comprado na região CN-Hong Kong e o servidor em nuvem está associado ao cofre. O usuário é cobrado pelo cofre de backup do servidor de banco de dados de 800 GB no CBR.

Caso 3:

Replicação de um backup para outra região, com cobrança de pagamento por uso:

Um usuário compra um cofre de backup A de 100 GB de servidor na região CN-Hong Kong e os dados de backup usam 40 GB do espaço de armazenamento. Esse usuário também compra um cofre de replicação B de 200 GB na região AP-Bangkok e replica dados do cofre A para o cofre B, sem usar o serviço de aceleração. Nesse caso, o usuário é cobrado pelo cofre de backup de 100 GB e pelo cofre de replicação de 200 GB, bem como pelo tráfego de dados de replicação entre regiões de 40 GB.

Modos de cobrança

Os cofres CBR têm dois modos de cobrança: pagamento por uso e anual/mensal. Selecione um modo de cobrança que melhor se adapte às suas necessidades de negócios.

- **pagamento por uso**

  Você paga pelo tempo de uso dos recursos. Os preços são calculados por hora, e nenhuma taxa mínima é necessária.

- **Anual/mensal**

  Você pode escolher a assinatura anual/mensal por um preço melhor.

O CBR também fornece pacotes de tráfego de replicação para replicação de backup entre regiões. Se nenhum pacote for comprado, você será cobrado na base de pagamento por uso pelo tráfego de replicação.

Para obter mais informações, consulte **Detalhes de preços do CBR**.

Alteração do modo de cobrança

- Anual/mensal é um modo de cobrança pré-pago. Você é cobrado com base na duração da assinatura especificada. Este modo oferece preços mais baixos e é ideal quando a duração do uso de recursos é previsível.
- O modo de pagamento por uso é pós-pago. Você é cobrado com base no uso de recursos. Com esse modo, você pode aumentar ou excluir recursos a qualquer momento. As taxas são deduzidas do saldo da sua conta.

Se você quiser mudar um cofre de pagamento por uso para um cofre anual/mensal, consulte **Alteração do modo de cobrança de pagamento por uso para anual/mensal**.

Vencimento

Para obter detalhes, consulte **Suspensão de serviço e liberação de recursos**.

Renovação

Escolha **More** > **Renew** na coluna **Operation** do cofre anual/mensal para renovar sua assinatura. Para obter mais informações sobre renovação, incluindo renovação automática,

exportação da lista de renovação e alteração de assinaturas, consulte **Gerenciamento de renovação**.

Pagamento em atraso

Possíveis causas de pagamento em atraso:

- O saldo da conta não é suficiente depois de comprar um cofre de pagamento por uso.
- As taxas de tráfego geradas durante a replicação do backup são maiores do que o saldo da sua conta.

Status do serviço e restrições de operação quando uma conta está em atraso:

No período de retenção, seus cofres e dados de backup são retidos. Você pode visualizar backups existentes, mas não pode criar novos backups ou adicionar tags. Se você não pagar as taxas pendentes antes que o período de retenção expire, seus dados serão automaticamente liberados e não poderão ser restaurados. Para saber como pagar as dívidas em atraso, consulte **Reembolso de atrasos**.

Para obter detalhes sobre o período de retenção, consulte **Suspensão de serviço e liberação de recursos**.

8 Gerenciamento de permissões

Se você precisar atribuir permissões diferentes a funcionários em sua empresa para acessar seus recursos de CBR na Huawei Cloud, o Identity and Access Management (IAM) é uma boa escolha para o gerenciamento de permissões refinado. O IAM fornece autenticação de identidade, gerenciamento de permissões e controle de acesso, ajudando você a proteger o acesso aos seus recursos da Huawei Cloud.

Com o IAM, você pode usar sua conta da Huawei Cloud para criar usuários do IAM para seus funcionários e atribuir permissões aos usuários para controlar seu acesso a tipos de recursos específicos. Por exemplo, alguns desenvolvedores de software em sua empresa precisam usar recursos de CBR, mas não devem ter permissão para excluí-los ou executar outras operações de alto risco. Nesse cenário, você pode criar usuários do IAM para os desenvolvedores de software e conceder a eles apenas as permissões necessárias para usar os recursos da CBR.

Se sua conta da Huawei Cloud não exigir usuários individuais de IAM para gerenciamento de permissões, pule esta seção.

O IAM pode ser usado gratuitamente. Você paga apenas pelos recursos em sua conta. Para obter mais informações sobre o IAM, consulte **Visão geral de serviço do IAM**.

Permissões de CBR

Por padrão, os novos usuários do IAM não têm permissões atribuídas. Você precisa adicionar um usuário a um ou mais grupos e anexar políticas de permissões ou funções a esses grupos. Os usuários herdam permissões dos grupos aos quais são adicionados e podem executar operações especificadas em serviços de nuvem com base nas permissões.

O CBR é um serviço de nível de projeto implamentado e acessado em regiões físicas específicas. Para atribuir permissões do CBR a um grupo de usuários, especifique o escopo como projetos específicos da região e selecione os projetos para que as permissões entrem em vigor. Se **All projects** estiver selecionado, as permissões entrarão em vigor para o grupo de usuários em todos os projetos específicos da região. Ao acessar o CBR, os usuários precisam alternar para uma região onde foram autorizados a usar esse serviço.

Você pode conceder permissões aos usuários usando funções e políticas.

- Funções: um tipo de mecanismo de autorização grosseira que define permissões relacionadas às responsabilidades dos usuários. Apenas um número limitado de funções de nível de serviço para autorização está disponível. Ao usar funções para conceder permissões, você também precisa atribuir outras funções das quais as permissões

dependem para entrar em vigor. No entanto, as funções não são uma escolha adequada para autorização refinada e controle de acesso seguro.

- Políticas: um tipo de mecanismo de autorização refinado que define as permissões necessárias para realizar operações em recursos de nuvem específicos sob determinadas condições. Esse mecanismo permite uma autorização baseada em políticas mais flexível, atendendo aos requisitos de controle de acesso seguro. Por exemplo, você pode conceder aos usuários do ECS apenas as permissões para gerenciar um determinado tipo dos ECS. A maioria das políticas define permissões com base em APIs. Para as ações de API suportadas pelo CBR, consulte **Políticas de permissões e ações suportadas** .

Tabela 8-1 lista todas as funções e políticas definidas pelo sistema suportadas pelo CBR.

Tabela 8-1 Políticas definidas pelo sistema suportadas pelo CBR

Nome da política	Descrição	Tipo
CBR FullAccess	Permissões de administrador para o CBR. Os usuários com essas permissões podem operar e usar todos os cofres, backups e políticas.	Política definida pelo sistema
CBR BackupsAndVaults-FullAccess	Permissões de usuário comuns para o CBR. Os usuários com essas permissões podem criar, exibir e excluir cofres e backups, mas não podem criar, atualizar ou excluir políticas.	Política definida pelo sistema
CBR ReadOnlyAccess	Permissões somente leitura para o CBR. Os usuários com essas permissões só podem exibir dados do CBR.	Política definida pelo sistema

Tabela 8-2 lista as operações comuns suportadas por cada política definida pelo sistema ou função do CBR. Selecione as políticas ou funções conforme necessário.

Tabela 8-2 Operações comuns suportadas por cada política definida pelo sistema ou função da CBR

Operação	CBR FullAccess	CBR BackupsAndVaultsFullAccess	CBR ReadOnlyAccess
Consultar cofres	√	√	√
Criar cofres	√	√	×
Listar cofres	√	√	√
Atualizar cofres	√	√	×
Excluir cofres	√	√	×
Associar recursos	√	√	×
Dissociar recursos	√	√	×
Criar políticas	√	×	×

Operação	CBR FullAccess	CBR BackupsAndVaultsFullAccess	CBR ReadOnlyAccess
Atualizar políticas	√	×	×
Aplicar políticas a um cofre	√	√	×
Remover políticas de um cofre	√	√	×
Excluir políticas	√	×	×
Sincronizar backups	√	√	×
Replicar cofres	√	√	×
Executar backups	√	√	×
Atualizar assinaturas	√	√	×
Consultar o status do Agente	√	√	×
Excluir backups	√	√	×
Restaurar os dados usando backups.	√	√	×
Replicar backups	√	√	×
Associar cofres	√	√	×
Adicionar ou excluir tags do cofre em lote	√	√	×
Adicionar tags do cofre	√	√	×
Editar tags	√	√	×

Links úteis

- **Visão geral de serviço do IAM**
- **Criação de um grupo de usuários e usuários e concessão de permissões do CBR**
- **Políticas de permissões e ações suportadas**

9 Restrições

Parâmetros

- Um cofre pode ser associado a apenas uma política de backup.
- Um cofre pode ser associado a apenas uma política de replicação.
- Um cofre pode ser associado a um máximo de 256 recursos.
- Um máximo de 32 políticas de backup e 32 políticas de replicação podem ser criadas.
- Somente os backups em um cofre cujo status é **Available** ou **Locked** podem ser usados para restauração de dados.
- Os backups em um cofre cujo status é **Deleting** não podem ser excluídos.
- Os backups não podem ser baixados para um PC local ou carregados no OBS.
- Um cofre e seus servidores ou discos associados devem estar na mesma região.
- A restauração simultânea de dados não é suportada.

Backup de disco em nuvem

- Somente os discos no estado **Available** ou **In-use** podem ser copiados.
- Discos congelados no período de retenção não podem ser copiados.
- Um novo disco deve ser pelo menos tão grande quanto o disco de origem do backup.
- Os backups em disco em nuvem não podem ser replicados para outras regiões.

Backup de servidor em nuvem

- É possível fazer backup de discos compartilhados em um servidor, mas não pode haver mais de 10 discos compartilhados.
- Somente os backups em um cofre cujo status é **Available** ou **Locked** podem ser usados para criar imagens e serem replicados para outra região.
- Servidores congelados no período de retenção não podem ser copiados.
- O backup consistente com falhas para vários discos e o backup consistente com a aplicação para servidores de banco de dados são suportados.
- Você pode optar por fazer backup apenas de discos especificados em um servidor, mas esse backup de discos deve ser restaurado como um todo. Restauração em nível de arquivo ou diretório não é suportada.
- As imagens não podem ser criadas usando backups se a quantidade de recursos associada a um cofre de backup do servidor exceder a cota.

- É aconselhável não fazer backup de um servidor cujo tamanho de disco exceda 4 TB.
- Os backups podem ser replicados para regiões que oferecem suporte à replicação. As limitações de replicação são as seguintes:
  - um backup pode ser replicado somente quando atende a todas as seguintes condições:
    i. é um backup do ECS.
    ii. contém dados do disco do sistema.
    iii. está no estado **Available**.
  - somente backups podem ser replicados As réplicas de backup não podem ser replicadas novamente, mas podem ser usadas para criar imagens.
  - um backup pode ser replicado para várias regiões de destino, mas pode ter apenas uma réplica em cada região de destino. A regra de replicação varia com o método de replicação:
    - replicação manual: um backup pode ser replicado para a região de destino, desde que não haja réplica na região de destino. Um backup pode ser replicado novamente se sua réplica na região de destino tiver sido excluída.
    - replicação orientada por políticas: depois que um backup tiver sido replicado com êxito para a região de destino, ele não poderá ser replicado para essa região novamente, mesmo que sua réplica tenha sido excluída.
  - somente regiões com recursos de replicação podem ser selecionadas como regiões de destino.

Backup de SFS Turbo

- O backup pode ser realizado apenas os sistemas de arquivos no estado **Available**.
- Um backup do sistema de arquivos do SFS Turbo não pode ser usado para restaurar dados no sistema de arquivos original.
- Os backups podem ser replicados para regiões que oferecem suporte à replicação. As limitações de replicação são as seguintes:
  - um backup pode ser replicado somente quando atende a todas as seguintes condições:
    i. ele é gerado para um sistema de arquivos do SFS Turbo.
    ii. está no estado **Available**.
  - somente backups podem ser replicados As réplicas de backup não podem ser replicadas novamente, mas podem ser usadas para criar sistemas de arquivos SFS Turbo.
  - um backup pode ser replicado para várias regiões de destino, mas pode ter apenas uma réplica em cada região de destino. A regra de replicação varia com o método de replicação:
    - replicação manual: um backup pode ser replicado para a região de destino, desde que não haja réplica na região de destino. Um backup pode ser replicado novamente se sua réplica na região de destino tiver sido excluída.
    - replicação orientada por políticas: depois que um backup tiver sido replicado com êxito para a região de destino, ele não poderá ser replicado para essa região novamente, mesmo que sua réplica tenha sido excluída.
  - somente regiões com recursos de replicação podem ser selecionadas como regiões de destino.

Backup em nuvem híbrida

- Os backups sincronizados com a nuvem não podem ser usados para criar servidores em nuvem.
- Os backups de armazenamento só podem ser restaurados em discos de dados em servidores em nuvem.

Backup de arquivos

- Durante o backup de arquivos, se um arquivo estiver sendo alterado por um aplicativo e o cliente de backup tiver a permissão de leitura desse arquivo, os dados do backup ficarão incompletos. É aconselhável primeiro parar o aplicativo e, em seguida, executar backup para garantir a integridade dos dados.
- Durante o backup do arquivo, se um arquivo estiver sendo usado por um processo ou o cliente de backup não tiver a permissão de leitura desse arquivo, os dados do backup estarão incompletos.
- É aconselhável não restaurar backups de arquivos para aplicativos em execução. Pare os aplicativos e, em seguida, restaurar os arquivos.
- Um cliente de backup pode ter um máximo de 8 arquivos e diretórios adicionados.
- Cada recurso só pode ter um Agente instalado.
- O número de recursos em que o Agente pode ser instalado não é limitado.
- Recomenda-se que um diretório não contenha mais do que 500.000 arquivos.
- Um caminho de OBS pode conter no máximo de 200 caracteres.
- A largura de banda máxima permitida para a transmissão de dados de backup de arquivos é de 16 Gbit/s. Se a largura de banda máxima for atingida, o controle de fluxo será acionado.
- O backup de arquivos não pode fazer backup dos arquivos armazenados em sistemas de arquivos do SFS montados em servidores em nuvem.
- O backup pode falhar em diretórios com gravações frequentes de arquivos no Windows.

10 CBR e outros serviços

Serviços relacionados ao CBR

Tabela 10-1 Serviços relacionados ao CBR

Função	Serviço relacionado	Referência
O CBR faz backup de dados de discos em um ECS e restaura dados de backup em discos de um ECS para restaurar dados perdidos ou corrompidos. Os backups gerados podem ser usados para criar imagens para restaurar rapidamente ambientes de execução de serviços.	ECS	**Criação de um backup de servidor em nuvem** **Criação de um backup de disco em nuvem**
O CBR faz backup de dados de discos em um BMS e restaura dados de backup em discos de um BMS para restaurar dados perdidos ou corrompidos. Os processos de backup e gerenciamento para BMSs e ECSs são os mesmos.	BMS	**2 O que é o CBR?** **Criação de um backup de servidor em nuvem**
O CBR faz backup dos dados dos sistemas de arquivos SFS Turbo. Você pode usar dados de backup para criar novos sistemas de arquivos para restaurar dados perdidos ou corrompidos.	SFS	**Criação de um backup de SFS Turbo**
O CBR armazena dados de backup no OBS, aumentando a segurança dos dados de backup.	OBS	**2 O que é o CBR?**
O CBR faz backup de dados em discos. Você pode usar dados de backup para criar novos discos.	EVS	**Criação de um backup de disco em nuvem**
O Cloud Trace Service (CTS) registra as operações nos recursos do CBR, facilitando futuras consultas, auditorias e rastreamento inverso.	CTS	**Auditoria**

Função	Serviço relacionado	Referência
O Data Express Service (DES) oferece um serviço de transmissão de dados seguro, rápido e eficiente. Resolve o problema da migração massiva de dados para a nuvem. Após o backup de VM VMware no local, você pode usar o DES para transmitir os dados de backup usando Teleports ou discos para um bucket do OBS. Em seguida, você pode sincronizar os dados de backup no bucket do OBS com um cofre do CBR no console para gerenciamento baseado em nuvem.	DES	**Criação de uma unidade de armazenamento**
O IAM é um sistema de auto atendimento para empresas gerenciarem recursos de nuvem. Ele fornece gerenciamento de identidade do usuário e funções de controle de acesso. Quando vários usuários de uma empresa precisam de usar o CBR, o administrador da empresa pode usar o IAM para criar usuários e controlar as permissões desses usuários em recursos da empresa.	IAM	**8 Gerenciamento de permissões**
O Tag Management Service (TMS) permite adicionar tags predefinidas aos cofres do CBR para facilitar a filtragem e o gerenciamento.	TMS	**Gerenciamento de tags de cofre**

11 Conceitos básicos

11.1 Conceitos do CBR

Cofre

O CBR usa cofres para armazenar backups. Cofres podem ser cofres de backup ou cofres de replicação.

- Um cofre de backup é um contêiner que armazena backups de recursos, como servidores e discos. Os cofres de backup são classificados nos seguintes tipos:
  - **Cofres de backup de servidor**: eles incluem aqueles que armazenam apenas backups de servidores comuns e aqueles que armazenam backups de servidores de banco de dados. Você pode associar servidores a um cofre de backup de servidor e aplicar uma política de backup ou replicação ao cofre. Também pode replicar backups de um cofre em uma região para um cofre de replicação em outra região. Os backups de servidor podem ser usados para restaurar dados do servidor.
  - **Cofres de backup de disco**: armazenam apenas backups de disco. Você pode associar discos a um cofre de backup de disco e aplicar uma política de backup ao cofre.
  - **Cofres de backup do SFS Turbo**: armazenam apenas backups de sistemas de arquivos do SFS Turbo. Você pode associar sistemas de arquivos a um cofre de backup do SFS Turbo e aplicar uma política de backup ao cofre.
  - **Cofres de backup em nuvem híbrida**: armazenam backups sincronizados dos sistemas de armazenamento locais de Dorado OceanStor e máquinas virtuais de VMware. Você pode replicar backups para um cofre de replicação de outra região e restaurar os dados de backup para outros servidores. Eles também podem armazenar os backups de arquivos e diretórios em seus servidores de nuvem e hosts locais. Você não precisa de fazer backup de servidores ou discos inteiros.
- Os cofres de replicação armazenam somente réplicas de backups. Tais réplicas não podem ser replicadas novamente. Os cofres de replicação para backups de servidor

incluem aqueles que armazenam apenas réplicas de backups comuns e aqueles que armazenam réplicas de backups consistentes com a aplicação

Backup

Um backup é uma cópia de um determinado pedaço de dados e geralmente é armazenado em outro lugar para que ele possa ser usado para restaurar os dados originais em caso de perda de dados. Ele pode ser gerado manualmente por uma tarefa de backup única ou automaticamente por uma tarefa periódica.

O CBR suporta backup único e backup periódico. Uma tarefa de backup única é criada manualmente pelos usuários e é executada apenas uma vez. As tarefas de backup periódico são executadas automaticamente com base em uma política de backup definida pelo usuário.

- O nome de um backup único é **manualbk_***xxxx*. Pode ser definido pelo usuário ou pelo sistema.
- O nome de um backup periódico é **autobk_***xxxx*, que é atribuído automaticamente pelo sistema.

Política de backup

Uma política de backup é um conjunto de regras para backup de dados, incluindo o nome da política, o status da política, o tempo de execução das tarefas de backup, a frequência de backup e a regra de retenção. Uma regra de retenção especifica por quanto tempo os backups são retidos ou o número de backups que são retidos. Os backups automáticos podem ser executados aplicando-se uma política de backup a um cofre de backup.

Replicação

Replicação é o processo de replicação de dados de backup de uma região de origem para uma região de destino. Você pode usar réplicas de backup na região de destino para criar imagens e provisionar servidores.

Backup de servidor em nuvem e backup em nuvem híbrida suportam replicação manual para um único backup. Você também pode configurar regras de replicação em uma política para replicar periodicamente backups, que são gerados com base na política e não foram ou não foram replicados para a região de destino.

Por exemplo, se você deseja fazer backup de um servidor, selecione **Backup** para o tipo de proteção do cofre. Se você deseja replicar backups de servidor da região 1 para a região 2, o cofre de destino na região 2 deve ser no tipo de proteção de **Replication**.

Restauração instantânea

Restauração instantânea é uma função para restaurar dados e criar imagens de backups. A Restauração instantânea é muito mais rápida do que um processo de restauração normal.

Backups comuns não suportam restauração instantânea, enquanto backups otimizados sim. Por padrão, todos os backups do CBR são backups otimizados. Em comparação com backups comuns, os backups otimizados usam menos tempo para restaurar dados do servidor ou criar imagens.

Backup otimizado

Os backups otimizados podem ser usados para restaurar rapidamente os dados do servidor ou criar imagens. Esse tipo de backup depende da Restauração instantânea.

Antes da implementação da Restauração instantânea, todos os backups do CBR gerados são backups comuns. Após a implementação da Restauração instantânea, todos os backups do CBR gerados são backups otimizados. Este é um upgrade de desempenho geral do CBR, e nenhuma configuração adicional é necessária. Atualmente, todos os backups do CBR gerados são backups otimizados.

Demora mais tempo para restaurar os dados do servidor ou criar imagens usando backups comuns. Backups otimizados podem fazer a mesma coisa com tempo significativamente reduzido. A única diferença entre backups comuns e backups otimizados é a velocidade de restauração.

Backup consistente com a aplicação

Existem três tipos de backup em termos de consistência de backup:

- backup inconsistente: os arquivos em um backup inconsistente contêm dados obtidos de diferentes pontos no tempo. Isso geralmente ocorre se forem feitas alterações em seus arquivos ou nos dados em seus discos enquanto o backup está em execução.
- backup consistente com falhas: um backup consistente com falhas captura dados que existem em discos no momento do backup, sem fazer backup de dados de memória ou desativar sistemas de aplicativos. A consistência de backup dos sistemas de aplicativos não é garantida. Para concluir isso, os discos são verificados na reinicialização do sistema operacional para restaurar dados danificados, por exemplo, usando **chkdsk**, e a reversão de log é executada em bancos de dados para manter os dados consistentes.
- backup consistente com a aplicação: um backup consistente com a aplicação é um backup de dados de aplicativos que permite que os aplicativos atinjam um estado quiescente e consistente. Esse tipo de backup captura o conteúdo da memória e quaisquer gravações pendentes que ocorreram durante o processo de backup.

O backup do servidor em nuvem do CBR suporta tanto o backup consistente com falhas quanto o backup consistente com a aplicação (também chamado de backup do servidor de banco de dados). Instale o Agente antes de ativar o backup consistente com a aplicação para impedir que o backup do servidor de banco de dados falhe.

Backup completo periódico

Por padrão, o CBR executa um backup completo para um recurso no backup inicial e backups incrementais em todos os backups subsequentes.

O CBR agora permite que você implemente backups completos periódicos além do backup inicial. Você pode configurar uma política para executar um backup completo após cada N backups incrementais. Isso melhora ainda mais a segurança dos dados de backup e atende às necessidades periódicas de backup completo.

Os backups completos periódicos ocupam mais espaço de armazenamento do que os backups incrementais.

11.2 Projeto e projeto empresarial

Projeto

Um projeto é usado para agrupar e isolar recursos do OpenStack, como computação, armazenamento e recursos de rede. Um projeto pode ser um departamento ou uma equipe de projeto. Vários projetos podem ser criados para uma conta.

Projeto empresarial

Um projeto empresarial gerencia várias instâncias de recursos por categoria. Recursos e projetos em diferentes regiões de serviço de nuvem podem ser classificados em um projeto empresarial. Uma empresa pode classificar recursos com base no departamento ou grupo de projeto e colocar recursos relevantes em um projeto empresarial para gerenciamento. Os recursos podem ser migrados entre projetos empresariais.

11.3 Região e AZ

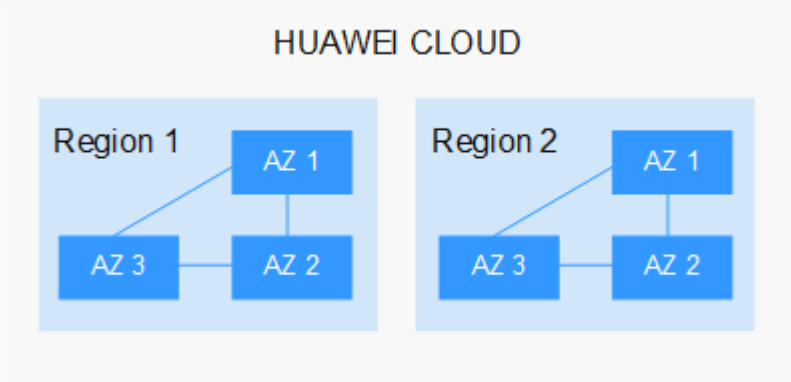
Conceito

Uma região e uma zona de disponibilidade (AZ) identificam a localização de um centro de dados. Você pode criar recursos em uma região e AZ específicas.

- As regiões são divididas com base na localização geográfica e na latência da rede. Serviços públicos, como Elastic Cloud Server (ECS), Elastic Volume Service (EVS), Object Storage Service (OBS), Virtual Private Cloud (VPC), Elastic IP (EIP) e Image Management Service (IMS), são compartilhados na mesma região. As regiões são classificadas em regiões universais e regiões dedicadas. Uma região universal fornece serviços de nuvem universal para locatários comuns. Uma região dedicada fornece serviços específicos para locatários específicos.
- Uma AZ contém um ou mais centros de data físicos. Cada AZ possui resfriamento, sistema de extinção de incêndio, proteção contra umidade e instalações elétricas independentes. Dentro de uma AZ, computação, rede, armazenamento e outros recursos são logicamente divididos em vários clusters. As AZs dentro de uma região são interconectadas usando fibras ópticas de alta velocidade, para suportar sistemas de alta disponibilidade entre AZs.

Figura 11-1 mostra a relação entre regiões e AZs.

Figura 11-1 Regiões e as AZs



HUAWEI CLOUD fornece serviços em muitas regiões do mundo. Selecione uma região e uma AZ com base nos requisitos. Para obter mais informações, consulte **Regiões globais do Huawei Cloud**.

Selecionar uma região

Ao selecionar uma região, considere os seguintes fatores:

- Localização

  É recomendável selecionar a região mais próxima para menor latência de rede e acesso rápido. As regiões dentro do continente chinês fornecem a mesma infraestrutura, qualidade de rede BGP, bem como operações e configurações de recursos. Portanto, se seus usuários-alvo estiverem no continente chinês, você não precisará considerar as diferenças de latência da rede ao selecionar uma região.

  - Se seus usuários-alvo estiverem na Ásia-Pacífico (excluindo o continente chinês), selecione a região **CN-Hong Kong**, **AP-Bangkok**, ou **AP-Singapore**.
  - Se seus usuários-alvo estão na África, selecione a região **AF-Johannesburg**.
  - Se seus usuários de destino estiverem na América Latina, selecione a região **LA-Santiago**.

    NOTA

    A região **LA-Santiago** está localizada no Chile.

- Preço do recurso

  Os preços dos recursos podem variar em diferentes regiões. Para obter detalhes.

Selecionar uma AZ

Ao implantar recursos, considere os requisitos de recuperação de desastres (DR) e latência de rede de seus aplicativos.

- Para alta capacidade de DR, implante recursos nas diferentes AZs dentro da mesma região.
- Para menor latência de rede, implante recursos na mesma AZ.

Regiões e endpoints

Antes de usar uma API para chamar recursos, especifique sua região e endpoint. Para obter mais detalhes, consulte Regions and Endpoints.

12 História de mudanças

Lançado em	Descrição
20/07/2022	Esta edição é o sexto lançamento oficial. Atualização do seguinte conteúdo: adição do conteúdo do backup de arquivo.
27/10/2021	Esta edição é o quinto lançamento oficial. Atualização do seguinte conteúdo: adição do conteúdo do gerenciamento de permissões.
07/08/2020	Esta edição é o quarto lançamento oficial. Atualização do seguinte conteúdo: adição da descrição de pagamento em atraso na seção "Cobrança".
08/04/2020	Esta edição é o terceiro lançamento oficial. Atualização do seguinte conteúdo: adição do conteúdo do backup do sistema de arquivos.
31/03/2020	Esta edição é o segundo lançamento oficial. Atualização do seguinte conteúdo: adição da seção "Cobrança."
31/07/2019	Esta edição é o primeiro lançamento oficial.

