Cloud Backup and Recovery

Guia de usuário

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.

Índice

1 Gerenciamento de permissões

1.1 Criação de um usuário e concessão de permissões do CBR

Este tópico descreve como usar o IAM para implementar o controle de permissões refinado para seus recursos do CBR. Com o IAM, você pode:

- criar usuários do IAM para funcionários com base na estrutura organizacional da sua empresa. Cada usuário do IAM terá suas próprias credenciais de segurança para acessar os recursos do CBR.
- conceder somente as permissões necessárias para que os usuários executem uma tarefa específica.
- confiar uma conta da Huawei Cloud ou serviço de nuvem para executar O&M eficiente em seus recursos de CBR.

Se sua conta da HUAWEI CLOUD não exigir usuários individuais do IAM, pule esta seção.

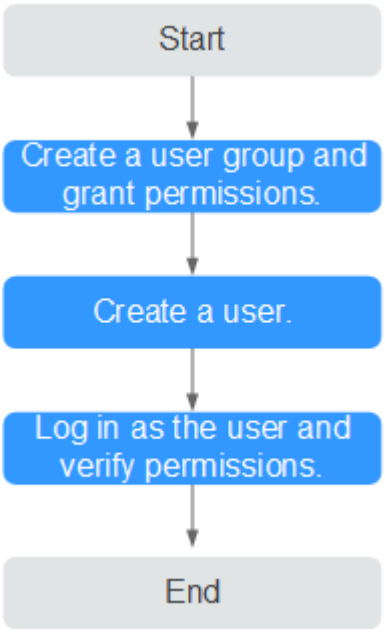
Esta seção descreve o procedimento para conceder permissões (consulte **Figura 1-1**).

Pré-requisitos

Saiba mais sobre as permissões (consulte **Permissões do CBR**) suportadas pelo CBR e escolha políticas ou funções de acordo com suas necessidades. Para as políticas de sistema de outros serviços, veja **Permissões do Sistema**.

Fluxo do processo

Figura 1-1 Processo para concessão de permissões do CBR



1. **Crie um grupo de usuários e atribua permissões** para ele.

   Crie um grupo de usuários no console do IAM, e atribua a política de **CBR ReadOnlyAccess** ao grupo.

2. **Crie um usuário do IAM e adicione-o ao grupo de usuários**.

   Crie um usuário no console do IAM e adicione o usuário ao grupo criado em **1**.

3. **Faça logon** e verifique as permissões.

   Efetue logon no console do CBR usando o usuário criado e verifique se o usuário tem permissões somente leitura para o CBR.

   - Escolha **Service List** > **Cloud Backup and Recovery**. Em seguida, clique em **Buy Server Backup Vault** no console do CBR. Se aparecer uma mensagem indicando que você não tem permissões suficientes para acessar o serviço, a política de **CBR ReadOnlyAccess** já entrou em vigor.
   - Escolha qualquer outro serviço na **Service List**. Se aparecer uma mensagem indicando que você não tem permissões suficientes para acessar o serviço, a política de **CBR ReadOnlyAccess** já entrou em vigor.

1.2 Criação de uma política personalizada

Políticas personalizadas podem ser criadas para complementar as políticas definidas pelo sistema do CBR. Para as ações suportadas para políticas personalizadas, consulte **Políticas de permissões e ações suportadas**.

Você pode criar políticas personalizadas de uma das seguintes maneiras:

- editor visual: selecione serviços de nuvem, ações, recursos e condições de solicitação. Isso não requer conhecimento de sintaxe política.

- JSON: edite políticas JSON do zero ou com base em uma política existente.

Esta seção fornece exemplos de políticas comuns do CBR definidas pelo usuário.

Exemplo de políticas personalizadas

- Exemplo 1: permite que os usuários criem, modifiquem e excluam cofre

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

- Exemplo 2: nega que os usuários excluam cofres e backups

  Uma política com apenas permissões "Deny" deve ser usada em conjunto com outras políticas para entrar em vigor. Se as permissões atribuídas a um usuário contiverem "Allow" e "Deny", as permissões "Deny" terão precedência sobre as permissões "Allow".

  O método a seguir pode ser usado se você precisar atribuir permissões da política de **CBR FullAccess** a um usuário, mas quiser impedir que ele exclua cofres e backups. Crie uma política personalizada para negar a exclusão do cofre e anexe ambas as políticas ao grupo ao qual o usuário pertence. Em seguida, o usuário pode executar todas as operações no CBR, exceto excluir cofres ou backups. O seguinte é um exemplo de uma política de negação:

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

- Exemplo 3: define as permissões para vários serviços em uma política

  Uma política personalizada pode conter as ações de vários serviços que são do tipo global ou de nível de projeto. Veja a seguir um exemplo de política que contém ações de vários serviços:

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



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


2 Gerenciamento de cofre

2.1 Consulta de um cofre

É possível definir critérios de pesquisa para consultar os cofres desejados na lista do cofre.

Pré-requisitos

Um cofre foi criado.

Visualizar detalhes do cofre

Passo 1 Faça logon no console de CBR.

1. **Efetue logon no console de gerenciamento**.
2. Clique em no canto superior esquerdo e selecione sua região e projeto.
3. Escolha **Storage** > **Cloud Backup and Recovery**. Selecione uma guia de backup no painel de navegação esquerdo.

Passo 2 Visualize as informações básicas sobre cofres. Os parâmetros relacionados são descritos na tabela a seguir.

Tabela 2-1 Parâmetros básicos da informação

Parâmetro	Descrição
Name/ID	Nome e identificação do cofre. Clique no nome do cofre para visualizar os detalhes sobre o cofre.
Type	Tipo de cofre, que pode ser cofre de backup e cofre de replicação ● Um cofre de backup armazena backups de servidores, sistemas de arquivos, e discos. ● Um cofre de replicação armazena réplicas de backups.
Status	Status do cofre. **Tabela 2-2** descreve os status do cofre.

Parâmetro	Descrição
Specifications	Especificações do cofre, que podem ser backup do servidor e backup consistente com aplicativos ● Um cofre de backup de servidor armazena backups de servidores comuns. ● Um cofre de backup consistente com aplicativos armazena backups de servidores de banco de dados.
Used/Total Vault Capacity (GB)	Capacidade usada pelos backups no cofre. Ele mostra o espaço usado pelos backups e a capacidade do cofre. Por exemplo: se **20/100** for exibido, 20 GB foram usados fora da capacidade do cofre de 100 GB.
Associated Servers/ File Systems/Disks	Número de servidores, sistemas de arquivos e discos associados ao cofre. Você pode clicar no número para exibir detalhes dos recursos associados. A capacidade associada mostrada na página de detalhes é a capacidade total de todos os recursos que foram associados a este cofre.
Billing Mode	Modo de cobrança do cofre, que pode ser **Yearly/Monthly** e **Pay-per-use**. ● 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. ● Pagamento por uso é um modo de cobrança 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.

Passo 3 Em qualquer página de backup, clique na guia **Vaults** e defina os critérios de filtro para visualizar os cofres.

- Selecione um valor na lista suspensa de status para consultar cofres por status. **Tabela 2-2** descreve os status do cofre.

Tabela 2-2 Status do cofre

Estado	Atributo de status	Descrição
All statuses	--	Todos os cofres são exibidos se este valor for selecionado.
Disponíveis	Um estado estável	Um estado estável após a conclusão de uma tarefa do cofre. Este estado permite a maioria das operações.

Estado	Atributo de status	Descrição
Locked	Um estado intermediário	Um estado intermediário quando uma expansão de capacidade, alteração de modo de cobrança ou alteração de especificações está em andamento. Neste estado, não é possível expandir a capacidade do cofre, alterar o modo de faturamento ou alterar as especificações do cofre. No entanto, você pode executar outras operações, como aplicar uma política e associar servidores, sistemas de arquivos ou discos. Após a expansão da capacidade, a alteração do modo de cobrança ou das especificações está concluída, o status do cofre torna-se **Available**.
Deleting	Um estado intermediário	Um estado intermediário quando um cofre está sendo excluído. Nesse estado, uma barra de progresso é exibida indicando o progresso da exclusão. Se a barra de progresso permanecer inalterada por um período prolongado, ocorreu uma exceção. Entre em contato com atendimento ao cliente.
Frozen	Um estado estável	Se seus recursos inserirem um período de exclusão pendente no caso de sua assinatura ter expirado ou sua conta estar em atraso, ou se os recursos não atenderem aos requisitos de segurança, seu cofre será colocado no estado **Frozen**. Se os recursos forem congelados devido a atrasos, o estado ficará **Available** depois que sua conta for recarregada. Os recursos podem então ser usados normalmente. Se você não recarregar sua conta a tempo, o sistema exclui automaticamente os recursos congelados após o término do período de retenção. Se os recursos estiverem congelados por motivos de segurança, entre em contato com atendimento ao cliente.
Erro	Um estado estável	O cofre entra no estado **Error** quando ocorre uma exceção durante a execução da tarefa. Você pode clicar em **Tasks** no painel de navegação à esquerda para exibir a causa do erro. Se o erro persistir, entre em contato com atendimento ao cliente.

- Pesquise o cofre pelo seu nome ou ID.
- Clique em **Search by Tag** no canto superior direito para procurar cofres por tag.
  - Na página de guia **Search by Tag** exibida, insira uma chave e um valor de tag existentes e clique em  . Os critérios de pesquisa de marca adicionados são exibidos sob as caixas de texto. Clique em **Search** no canto inferior direito.

- Você pode usar mais de uma tag para uma pesquisa combinada. Cada vez que uma chave e um valor forem inseridos, clique em . Os critérios de pesquisa de marca adicionados são exibidos sob as caixas de texto. Quando mais de uma tag for adicionada, as tags serão aplicadas juntas para uma pesquisa de combinação. Um máximo de 10 tags podem ser adicionadas por vez.
- Você pode clicar em **Reset** no canto inferior direito para redefinir os critérios de pesquisa.

Passo 4 Clique no nome do cofre para visualizar os detalhes sobre o cofre.

NOTA

Para os valores de capacidade usada e espaço de backup, somente a parte inteira é mantida e a parte decimal é arredondada. Por exemplo, o espaço de backup usado é exibido como 0 GB, mas o espaço de backup realmente usado pode ser de 0,2 GB.

----Fim

2.2 Exclusão de um cofre

Você pode excluir cofres indesejados para reduzir o uso do espaço de armazenamento e os custos.

Todos os backups armazenados no cofre serão excluídos assim que você excluir um cofre.

Somente cofres de pagamento por uso podem ser excluídos. Os cofre anuais/mensais precisam ser cancelados seguindo as instruções em **Como cancelar a assinatura de um cofre?**

Pré-requisitos

- Existe pelo menos um cofre.
- O cofre está no estado **Available** ou **Error**.
- Um cofre de backup em nuvem híbrida pode ser excluído somente depois que você limpar os backups correspondentes tanto no local quanto na nuvem.

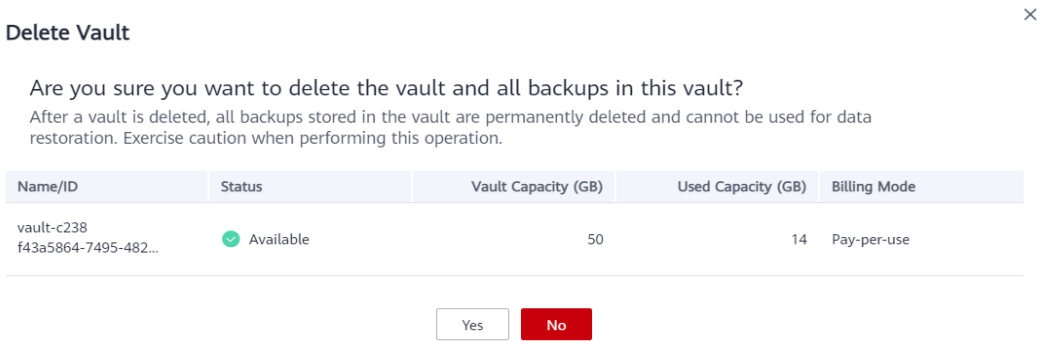
Procedimento

Passo 1 Faça logon no console de CBR.

1. **Efetue logon no console de gerenciamento**.
2. Clique em no canto superior esquerdo e selecione sua região e projeto.
3. Escolha **Storage** > **Cloud Backup and Recovery**. Selecione uma guia de backup no painel de navegação esquerdo.

Passo 2 Em qualquer página de backup, localize o cofre a ser excluído e escolha **More** > **Delete** na coluna **Operation**. Veja **Figura 2-1**. Todos os backups armazenados no cofre serão excluídos assim que você excluir um cofre. Tenha cuidado ao realizar esta operação.

Figura 2-1 Exclusão de um cofre



Passo 3 Clique em **Yes**.

----Fim

2.3 Dissociação de um recurso

Se não for mais necessário fazer backup de um recurso associado, dissocie-o do cofre.

Depois que um recurso é dissociado, a política de backup ou replicação do cofre não tem mais efeito sobre o recurso. Além disso, todos os backups manuais e automáticos do recurso serão excluídos. Backups excluídos não podem ser usados para restauração de dados. Tenha cuidado ao realizar esta operação.

A dissociação de um recurso de um cofre não afeta o desempenho dos serviços no recurso.

Procedimento

Passo 1 Faça logon no console de CBR.

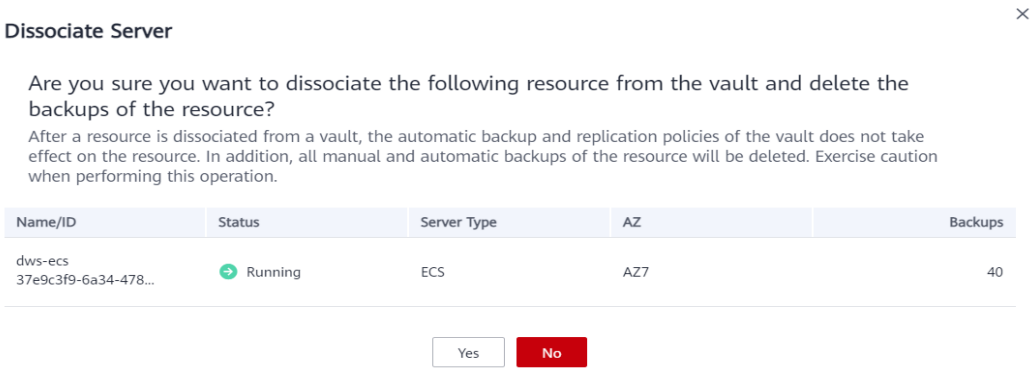
1. **Efetue logon no console de gerenciamento**.
2. Clique em no canto superior esquerdo e selecione sua região e projeto.
3. Escolha **Storage** > **Cloud Backup and Recovery**. Selecione uma guia de backup no painel de navegação esquerdo.

Passo 2 Em qualquer página de backup, localize o cofre de destino e clique no nome do cofre.

Passo 3 Neste exemplo, usaremos a página **Cloud Server Backups** para ilustrar o processo. Clique na guia **Associated Servers**. Localize o servidor de destino e clique em **Dissociate** na coluna **Operation**. Veja **Figura 2-2**.

Depois que um recurso é dissociado, a política de backup ou replicação do cofre não tem mais efeito sobre o recurso. Além disso, todos os backups manuais e automáticos do recurso serão excluídos. Backups excluídos não podem ser usados para restauração de dados. Tenha cuidado ao realizar esta operação.

Figura 2-2 Dissociar um servidor



Passo 4 Confirme as informações e clique em **Yes**.

----Fim

2.4 Migração de um recurso

Migrar um recurso significa dissociar um recurso de um cofre e em seguida associá-lo a outro cofre. Todos os backups do recurso serão migrados para o cofre de destino.

Restrições

- Os recursos podem ser migrados somente quando os cofres de origem e de destino estão no estado **Available** ou **Locked**.
- Os cofres de origem e de destino para migração de recursos devem ter as mesmas especificações.
- A capacidade restante do cofre de destino deve ser maior que o tamanho dos backups de recursos a serem migrados.
- A migração de recursos entre contas não é suportada no momento.

Procedimento

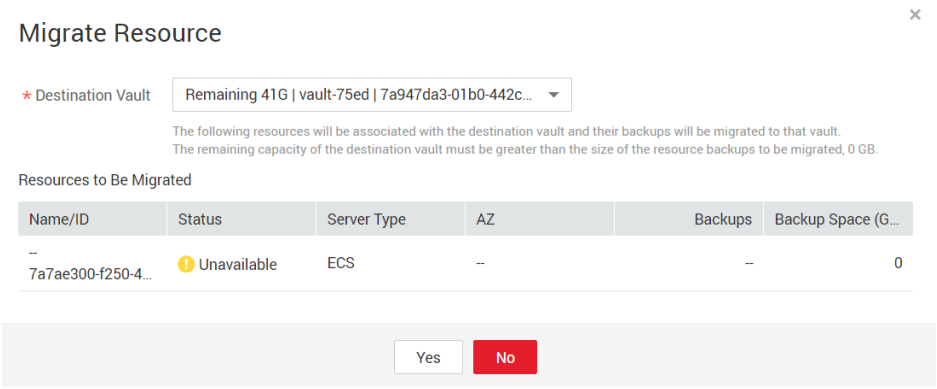
Passo 1 Faça logon no console de CBR.

1. **Efetue logon no console de gerenciamento**.
2. Clique em no canto superior esquerdo e selecione sua região e projeto.
3. Escolha **Storage** > **Cloud Backup and Recovery**. Selecione uma guia de backup no painel de navegação esquerdo.

Passo 2 Em qualquer página de backup, localize o cofre de destino e clique no nome do cofre. Neste exemplo, usaremos a página **Cloud Server Backups** para ilustrar o processo.

Passo 3 Clique na guia **Associated Servers**. Localize o servidor de destino e clique em **Migrate** na coluna **Operation**. Veja **Figura 2-3**.

Figura 2-3 Migrar um recurso



Passo 4 Selecione o cofre de destino e clique em **Yes**.

Passo 5 Exiba o andamento da migração na página **Tasks**. Se **Status** for alterado para **Successful**, o recurso foi migrado.

Passo 6 Vá para o cofre de destino para confirmar que o recurso foi associado ao cofre e que todos os seus backups foram migrados para aquele cofre.

----Fim

2.5 Expansão da capacidade do cofre

Você pode expandir o tamanho de um cofre se sua capacidade total for insuficiente.

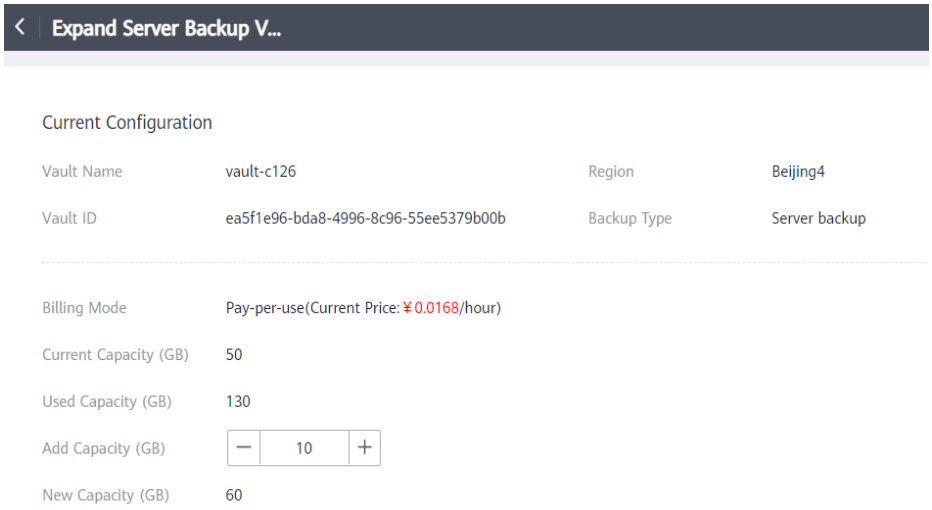
Procedimento

Passo 1 Faça logon no console de CBR.

1. **Efetue logon no console de gerenciamento**.
2. Clique em no canto superior esquerdo e selecione sua região e projeto.
3. Escolha **Storage** > **Cloud Backup and Recovery**. Selecione uma guia de backup no painel de navegação esquerdo.

Passo 2 Em qualquer página de backup, localize o cofre de destino e escolha **More** > **Expand Capacity** na coluna **Operation**. Veja **Figura 2-4**.

Figura 2-4 Expandir a capacidade do cofre



Passo 3 Insira a capacidade a ser adicionada. O valor mínimo é **1**.

Passo 4 Clique em **Next**. Confirme as configurações e clique em **Submit**.

Passo 5 Retorne à lista de cofres e verifique se a capacidade do cofre foi expandida.

----Fim

Expansão de capacidade automática

Se você quiser que um cofre seja expandido automaticamente quando sua capacidade for usada, ative a expansão automática da capacidade.

Se esta função estiver ativada, o tamanho do cofre será automaticamente expandido para 1,25x a capacidade do cofre original quando o limite máximo de tamanho for atingido.

Os cofres anuais/mensais não suportam expansão automática de capacidade.

Passo 1 Faça logon no console de CBR.

1. **Efetue logon no console de gerenciamento**.
2. Clique em no canto superior esquerdo e selecione sua região e projeto.
3. Escolha **Storage** > **Cloud Backup and Recovery**. Selecione uma guia de backup no painel de navegação esquerdo.

Passo 2 Em qualquer página de backup, clique no nome do cofre que deseja expandir.

Passo 3 Na página de detalhes do cofre, ative a **Auto Capacity Expansion**.

Passo 4 (Opcional) Desative a **Auto Capacity Expansion** se não for mais necessário.

----Fim

2.6 Redução da capacidade do cofre

Você pode reduzir o tamanho de um cofre se sua capacidade total for demais para você.

Apenas os cofres de pagamento por uso podem ter sua capacidade reduzida atualmente.

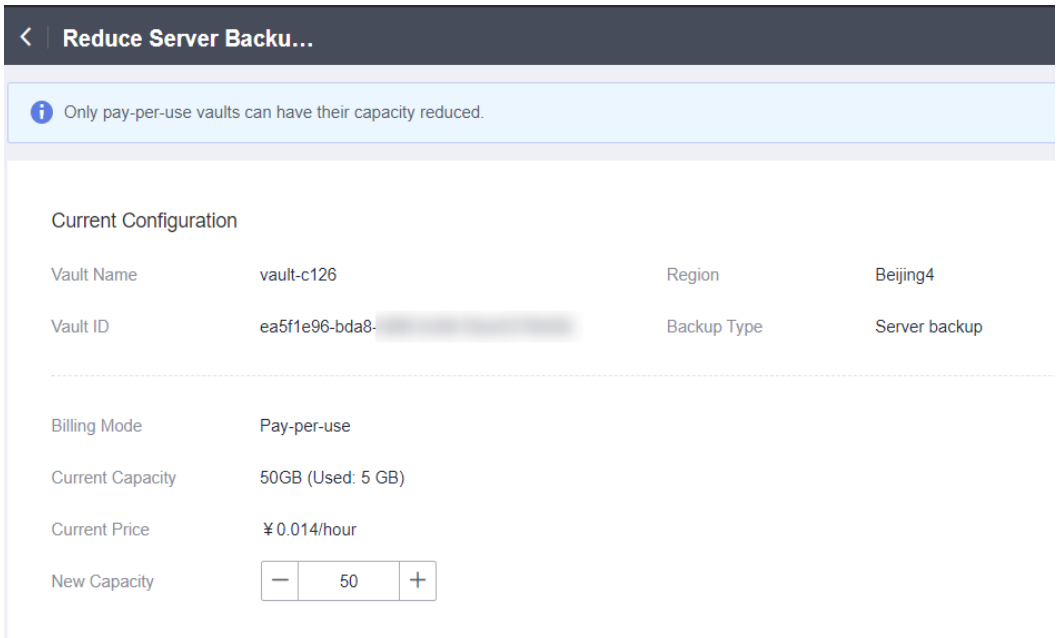
Procedimento

Passo 1 Faça logon no console de CBR.

1. **Efetue logon no console de gerenciamento**.
2. Clique em no canto superior esquerdo e selecione sua região e projeto.
3. Escolha **Storage** > **Cloud Backup and Recovery**. Selecione uma guia de backup no painel de navegação esquerdo.

Passo 2 Em qualquer página de backup, localize o cofre de destino e escolha **More** > **Reduce Capacity** na coluna **Operation**. Veja **Figura 2-5**.

Figura 2-5 Reduzir a capacidade do cofre



Passo 3 Insira a nova capacidade após a redução. Assegure que a nova capacidade seja superior a 125% da capacidade utilizada. Ou, a redução da capacidade falhará.

Passo 4 Clique em **Next**. Confirme as configurações e clique em **Submit**.

Passo 5 Retorne à lista de cofres e verifique se a capacidade do cofre foi reduzida.

----Fim

2.7 Alteração do modo de cobrança de pagamento por uso para anual/mensal

- 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 cobrança por uso é pós-pago. Você é cobrado com base no uso de recursos. Com esse modo, você pode adicionar ou excluir recursos a qualquer momento. As taxas são deduzidas do saldo da sua conta.

Se você quiser usar um cofre por um longo tempo, poderá alterar o modo de cobrança de pagamento por uso para anual/mensal para reduzir o custo. Para obter detalhes sobre as operações, consulte esta seção.

Pré-requisitos

Um cofre está no modo de cobrança de pagamento por uso.

Procedimento

Passo 1 Faça logon no console de CBR.

1. **Efetue logon no console de gerenciamento**.
2. Clique em  no canto superior esquerdo e selecione sua região e projeto.
3. Escolha **Storage** > **Cloud Backup and Recovery**. Selecione uma guia de backup no painel de navegação esquerdo.

Passo 2 Em qualquer página de backup, encontre o cofre de destino e escolha **More** > **Change Billing Mode** na coluna **Operation**.

Passo 3 Selecione a duração necessária para o cofre, confirme as informações e clique em **Pay**.

Passo 4 Retorne à lista do cofre. Você pode ver que o **Billing Mode** do cofre foi alterado para **Yearly/Monthly**.

----Fim

2.8 Alteração de especificações do cofre

Os cofres de backup do servidor e os cofres de replicação do servidor têm duas especificações: os de backups/réplicas do servidor e os de backups/réplicas consistentes com aplicativos.

- Backups de servidor são backups ou de servidores comuns.
- Backups consistentes com aplicativos são backups de servidores com bancos de dados.

Se você precisa fazer backup de um servidor que contém um banco de dados, altere as especificações do cofre associado de backup do servidor para backup consistente com o aplicativo. Esta seção descreve as operações detalhadas.

Você pode alterar as especificações de um cofre de backup do servidor para backup consistente com o aplicativo, mas não o contrário.

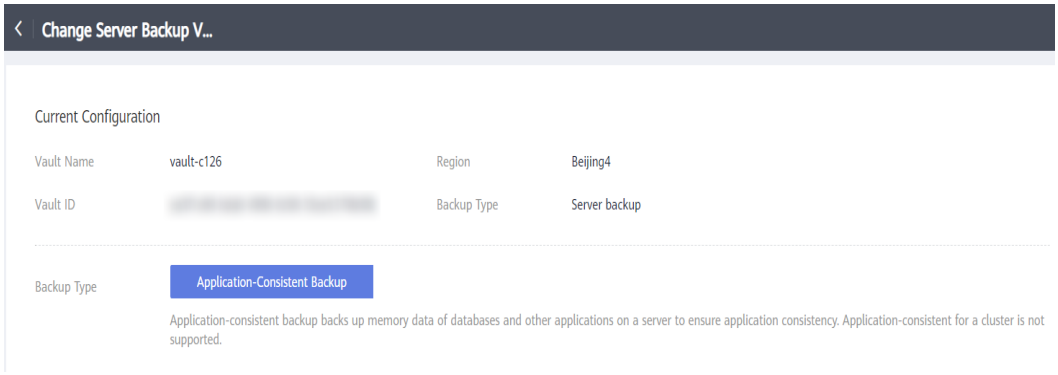
Procedimento

Passo 1 Faça logon no console de CBR.

1. **Efetue logon no console de gerenciamento**.
2. Clique em no canto superior esquerdo e selecione sua região e projeto.
3. Escolha **Storage** > **Cloud Backup and Recovery**. Selecione uma guia de backup no painel de navegação esquerdo.

Passo 2 Na página **Cloud Server Backups**, localize o cofre de destino. Escolha **More** > **Change Specifications** na coluna **Operation** do cofre. Veja **Figura 2-6**.

Figura 2-6 Alterar especificações



Passo 3 Defina **Backup Type** como **Application-Consistent Backup**. Clique em **Next**.

Passo 4 Clique em **Pay** e conclua o pagamento. O sistema altera automaticamente as especificações do cofre.

----Fim

2.9 Replicação de um cofre

O CBR permite replicar um cofre de backup do servidor, um cofre de backup em nuvem híbrida ou um cofre de backup do SFS Turbo inteiramente para um cofre de replicação em outra região. Réplicas de backups de servidor na região de destino podem ser usadas para criar imagens e provisionar servidores. Réplicas de backups do sistema de arquivos do SFS Turbo na região de destino podem ser usadas para criar sistemas de arquivos.

Dois modos de replicação estão disponíveis para replicar um cofre.

- Selecione um cofre de backup e replicá-lo manualmente.
- Configure uma política de replicação para replicar periodicamente backups que não foram replicados ou que não foram replicados para a região de destino

Restrições

- Os cofres de backup em disco não podem ser replicados para outras regiões.
- Esta característica está disponível somente nas regiões CN-Hong Kong, AP-Singapore e AP-Bangkok atualmente.
- A velocidade de replicação de um único backup é de cerca de 80 MB/s. Um máximo de oito backups podem ser replicados por vez.
- Os dados podem ser replicados para cofres em diferentes regiões de destino. A criação de uma réplica replicará todos os backups do cofre de fonte no cofre de destino.
- Um cofre de backup do servidor só pode ser replicado quando contiver pelo menos um backup que atenda a todas as seguintes condições:
  a. o backup é um backup do ECS.
  b. o backup contém dados do disco do sistema.
  c. o backup está no estado **Available**.
- Somente os cofres na região atual podem ser replicados. As réplicas não podem ser replicadas novamente, mas podem ser usadas para criar imagens ou sistemas de arquivos.
- Um cofre de backup pode ser replicado para diferentes regiões de destino. A regra de replicação varia com o método de replicação:
  – replicação manual: os backups podem ser replicados para a região de destino, desde que sua réplica seja excluída dessa região.
  – 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.

Procedimento

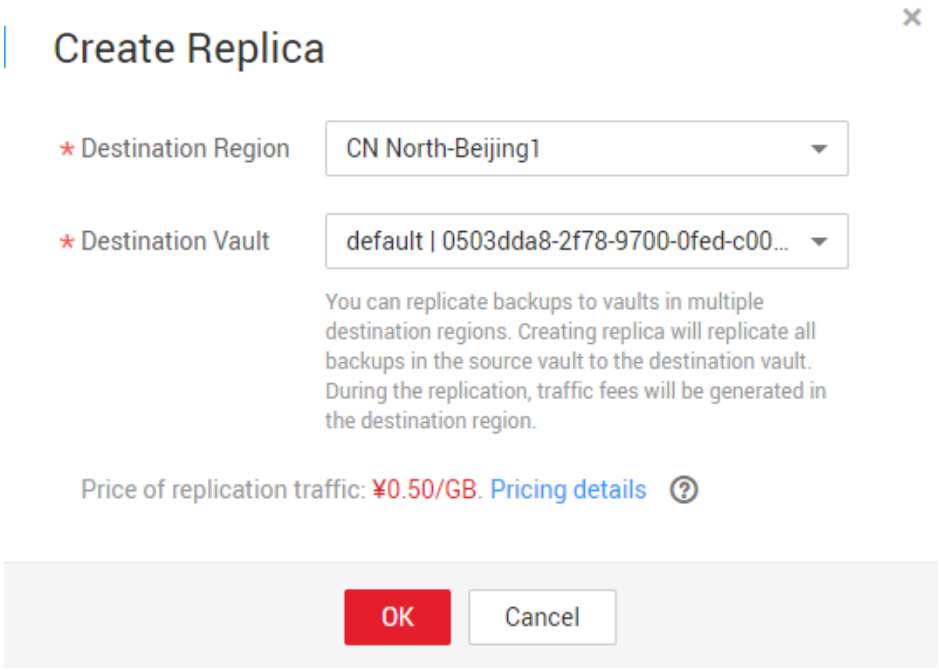
Passo 1 Faça logon no console de CBR.

1. **Efetue logon no console de gerenciamento**.
2. Clique em  no canto superior esquerdo e selecione sua região e projeto.
3. Escolha **Storage** > **Cloud Backup and Recovery**. Selecione uma guia de backup no painel de navegação esquerdo.

Passo 2 Clique na guia **Vaults** e localize o cofre de backup de destino.

Passo 3 Clique em **More** e escolha **Create Replica** na coluna **Operation** do cofre. Veja **Figura 2-7**.

Figura 2-7 Criar uma réplica



Passo 4 Na caixa de diálogo exibida, especifique os parâmetros descritos em **Tabela 2-3**.

Tabela 2-3 Descrição do parâmetro

Parâmetro	Descrição
Destination Region	Região para a qual o cofre é replicado Somente as regiões que oferecem suporte à replicação serão exibidas. ● Se a região selecionada contiver apenas um projeto, você poderá selecionar diretamente o nome da região. ● Se a região selecionada tiver vários projetos, o projeto principal da região será selecionado por padrão. Você pode selecionar outro projeto, se necessário.
Destination Vault	Um cofre de replicação na região de destino

Passo 5 Clique em **OK**.

Passo 6 Após a conclusão da replicação, você pode alternar para a região de destino para exibir réplicas geradas. Para mais detalhes, consulte **Consulta de um cofre**. Em seguida, você pode usar réplicas para criar imagens.

----Fim

2.10 Gerenciamento de tags do cofre

É possível adicionar identificadores a um cofre, bem como editar e excluir esses identificadores. Os identificadores do cofre são usados somente para filtrar e gerenciar os cofres.

Procedimento

Passo 1 Faça logon no console de CBR.

1. **Efetue logon no console de gerenciamento**.
2. Clique em  no canto superior esquerdo e selecione sua região e projeto.
3. Escolha **Storage** > **Cloud Backup and Recovery**. Selecione uma guia de backup no painel de navegação esquerdo.

Passo 2 Clique no nome de um cofre e selecione a guia **Tag** na página de informações do cofre exibida.

- Adicionar de uma tag
  a. Clique em **Add Tag** no canto superior esquerdo.
  b. Na caixa de diálogo exibida, defina a chave e o valor da nova tag.

  Uma tag é representada na forma de um par chave-valor. As tags são usadas para identificar, classificar e pesquisar recursos da nuvem. As tags do cofre são usados somente para filtrar e gerenciar os cofres. Um cofre pode ter no máximo 10 tags.

  Tabela 2-4 descreve os parâmetros de uma tag.

Tabela 2-4 Descrição do parâmetro de tag

Parâmetro	Descrição	Valor de exemplo
Chave	Chave da tag. Cada tag de um cofre tem uma chave única. Você pode personalizar a chave ou selecionar a chave de uma tag existente criada no TMS. Uma chave de marcação: ■ pode conter de 1 a 36 caracteres Unicode. ■ Pode conter apenas letras, dígitos, hífenes (-) e sublinhados (_).	Key_0001
Valor	Um valor de tag pode ser repetitivo ou deixado em branco. Um valor de tag: ■ pode conter de 0 a 43 caracteres Unicode. ■ Pode conter apenas letras, dígitos, hífenes (-) e sublinhados (_).	Value_0001

c. Clique em **OK**.

- Editar uma tag
  a. Na coluna **Operation** da tag que você deseja editar, clique em **Edit**.
  b. Na caixa de diálogo **Edit Tag** que é exibida, modifique o valor da tag. **Tabela 2-4** descreve os parâmetros.
  c. Clique em **OK**.
- Excluir uma tag
  a. Na coluna **Operation** da tag que você deseja exluir, clique em **Delete**.
  b. Na caixa de diálogo exibida, confirme as informações de exclusão.
  c. Clique em **OK**.

----Fim

2.11 Gerenciamento dos projetos empresariais de cofres

Se precisar modificar o projeto empresarial de um cofre, vá para a página **Enterprise Management** para mover o cofre do projeto empresarial original para um novo.

Procedimento

Passo 1 Clique em **Enterprise** no canto superior direito da página do console. Por default, a página **Overview** do Enterprise Management é exibida.

Passo 2 No painel de navegação da página **Enterprise Management**, escolha **Enterprise Project Management**.

Passo 3 Localize o projeto empresarial do qual o cofre será removido. Clique em **View Resources** na coluna **Operation**. A página de guia **Resources** é exibida. Você pode exibir recursos no projeto empresarial atual.

Passo 4 Selecione **Single Resource** para o modo de remoção

Passo 5 Selecione o projeto empresarial de destino ao qual o cofre deve ser adicionado e clique em **OK**.

Após o cofre ser removido do projeto empresarial, é possível visualizá-lo na lista de recursos do projeto empresarial de destino.

----Fim

3 Gerenciamento de backup

3.1 Visualização de um backup

Na lista de backup, você pode definir critérios de pesquisa para filtrar backups e visualizar detalhes de backup. Os resultados contêm tarefas de backup que estão em execução ou foram concluídas.

Pré-requisitos

Uma tarefa de backup foi criada.

Exibindo Detalhes do Backup

Passo 1 Faça logon no console de CBR.

1. **Efetue logon no console de gerenciamento**.
2. Clique em  no canto superior esquerdo e selecione sua região e projeto.
3. Escolha **Storage** > **Cloud Backup and Recovery**. Selecione uma guia de backup no painel de navegação esquerdo.

Passo 2 Em qualquer página de backup, clique na guia **Backups** e defina critérios de filtro para exibir os backups.

A última hora ativa exibida na lista de backup de arquivos mostra a última vez em que o Agente relatou seu status ao sistema.

- Você pode pesquisar backups selecionando um status na lista suspensa **All statuses** no canto superior direito da lista de backup. **Tabela 3-1** descreve os status de backup.

Tabela 3-1 Status de backup

Status	Atributo de status	Descrição
Todos os status	--	Todos os backups serão exibidos se esse valor for selecionado.

Status	Atributo de status	Descrição
Available	Um estado estável	Um estado estável de um backup após a criação do backup, indicando que o backup está disponível e não está sendo usado no momento. Este estado permite a maioria das operações.
Creating	Um estado intermediário	Um estado intermediário de um backup desde o início de um trabalho de backup até a conclusão deste trabalho. Na lista **Tasks**, uma barra de progresso é exibida para uma tarefa de backup nesse estado. Se a barra de progresso permanecer inalterada por um período prolongado, ocorreu uma exceção. Entre em contato com o atendimento ao cliente.
Restoring	Um estado intermediário	Um estado intermediário ao usar o backup para restaurar dados. Na lista **Tasks**, uma barra de progresso é exibida para uma tarefa de restauração nesse estado. Se a barra de progresso permanecer inalterada por um período prolongado, ocorreu uma exceção. Entre em contato com o atendimento ao cliente.
Deleting	Um estado intermediário	Um estado intermediário desde o início da exclusão do backup até a conclusão da exclusão do backup. Na lista **Tasks**, uma barra de progresso é exibida para uma tarefa de exclusão nesse estado. Se a barra de progresso permanecer inalterada por um período prolongado, ocorreu uma exceção. Entre em contato com atendimento ao cliente.
Erro	Um estado estável	Um backup entra no estado de **Error** quando ocorre uma exceção. Um backup nesse estado não pode ser usado para restauração e deve ser excluído manualmente. Se a exclusão manual falhar, entre em contato com atendimento ao cliente.

- Você pode procurar backups clicando em **Advanced Search** no canto superior direito da lista de backups.

  Você pode pesquisar especificando um status de backup, nome de backup, ID de backup, ID do cofre, nome do servidor, ID do servidor, tipo de servidor, se o backup é uma réplica, ou a data de criação.
- Você pode pesquisar backups selecionando um projeto na lista suspensa **All projects** no canto superior direito da lista de backup.

Passo 3 Clique no nome do backup para visualizar detalhes sobre o backup.

----Fim

3.2 Compartilhamento de um backup

Você pode compartilhar um servidor ou backup em disco com outras contas. Os backups compartilhados podem ser usados para criar servidores ou discos.

Contexto

Compartilhador

- Os backups só podem ser compartilhados entre contas na mesma região.
- Backups criptografados não podem ser compartilhados. Os backups não podem ser compartilhados entre regiões. A conta com a qual um backup é compartilhado deve estar na mesma região do backup.
- Os backups compartilhados aceitos serão excluídos assim que o compartilhamento excluir o backup original. Se um backup compartilhado tiver sido usado para criar novos discos ou servidores, os recursos criados não serão excluídos.

Destinatário

- Um destinatário deve ter pelo menos um cofre de backup para armazenar o backup compartilhado aceito, e o espaço restante do cofre deve ser maior que o tamanho do backup a ser aceito.
- Um destinatário pode escolher se deseja aceitar um backup. Depois de aceitar um backup, o destinatário pode usar o backup para criar novos servidores ou discos.
- Os backups compartilhados aceitos serão excluídos assim que o compartilhamento excluir o backup original. Se um backup compartilhado tiver sido usado para criar novos discos ou servidores, os recursos criados não serão excluídos.

Procedimento para o Compartilhador

Passo 1 Faça logon no console de CBR.

1. **Efetue logon no console de gerenciamento**.
2. Clique em  no canto superior esquerdo e selecione sua região e projeto.
3. Escolha **Storage** > **Cloud Backup and Recovery**. Selecione uma guia de backup no painel de navegação esquerdo.

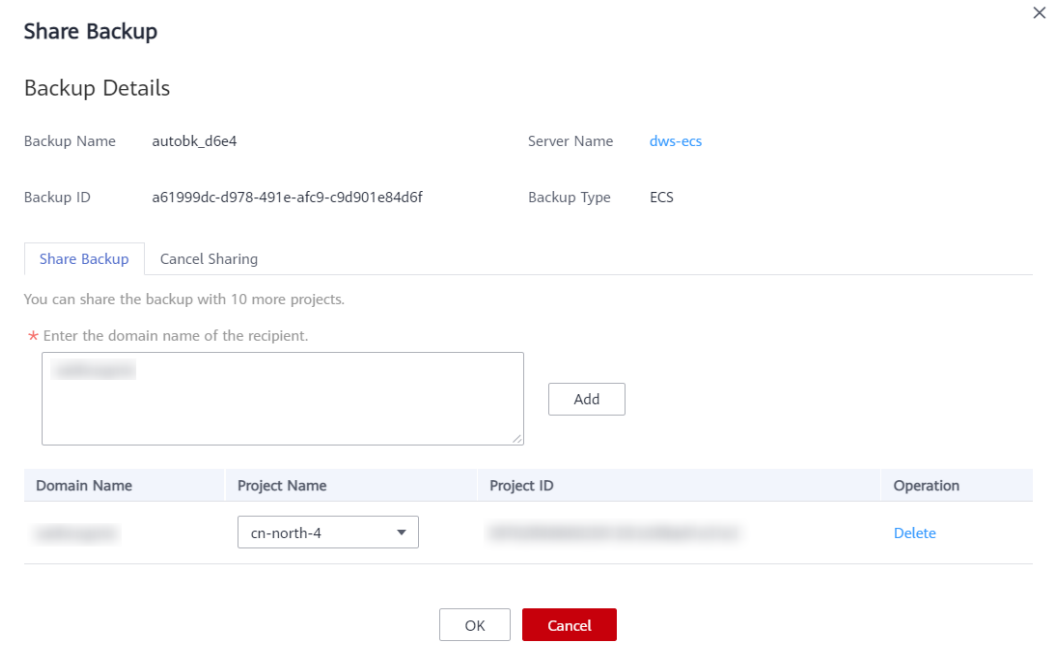
Passo 2 Na página de backup do servidor em nuvem ou do disco em nuvem, clique na guia **Backups** e defina os critérios de filtro para exibir os backups.

Passo 3 Localize o backup de destino e escolha **More** > **Share Backup** na coluna **Operation**.

O nome do backup, o nome do servidor, o ID do backup e o tipo de backup são exibidos.

- Compartilhar um backup

Figura 3-1 Compartilhar um backup

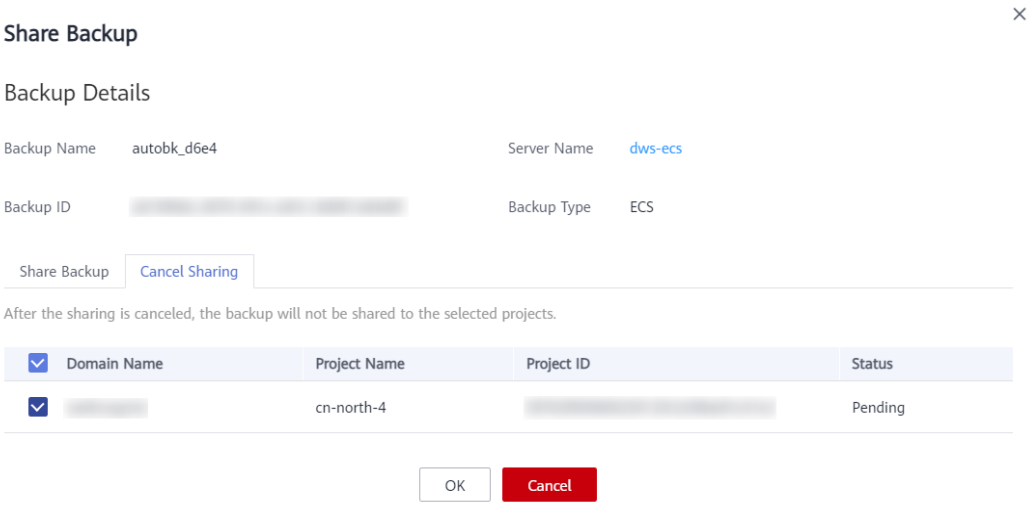


1. Clique na guia **Share Backup**.
2. Digite o nome da conta do locatário com quem o backup será compartilhado.
3. Clique em **Add**. O nome da conta e o projeto a ser adicionado são exibidos na lista. Você pode continuar a adicionar nomes de conta. Um backup pode ser compartilhado com no máximo dez projetos.
4. Clique em **OK**.

- Cancelar o compartilhamento

1. Localize o backup de destino e escolha **More** > **Share Backup** na coluna **Operation**.
2. Na página exibida, clique na guia **Cancel Sharing** e selecione o backup que não precisa mais de ser compartilhado. Em seguida, clique em **OK**. Veja **Figura 3-2**.

Figura 3-2 Cancelar o compartilhamento



----Fim

Procedimento para o Destinatário

Passo 1 Faça logon no console de CBR.

1. **Efetue logon no console de gerenciamento**.
2. Clique em no canto superior esquerdo e selecione sua região e projeto.
3. Escolha **Storage** > **Cloud Backup and Recovery**. Selecione uma guia de backup no painel de navegação esquerdo.

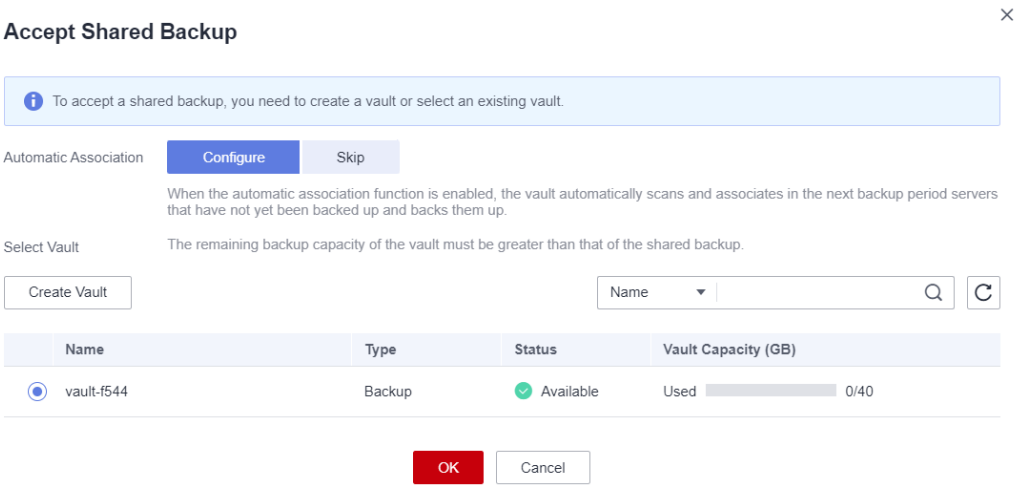
Passo 2 Na página do servidor em nuvem ou backup de disco em nuvem, clique na guia **Backups** e, em seguida, clique em **Backups Shared with Me**.

Passo 3 Certifique-se de que o destinatário tenha pelo menos um cofre de backup antes de aceitar o backup compartilhado. Para saber como comprar um cofre de backup, consulte **Compra de um cofre**.

Passo 4 Clique em **Accept**. Na página exibida, selecione o cofre usado para armazenar o backup compartilhado. Certifique-se de que a capacidade restante do cofre seja maior que o tamanho do backup. Veja **Figura 3-3**.

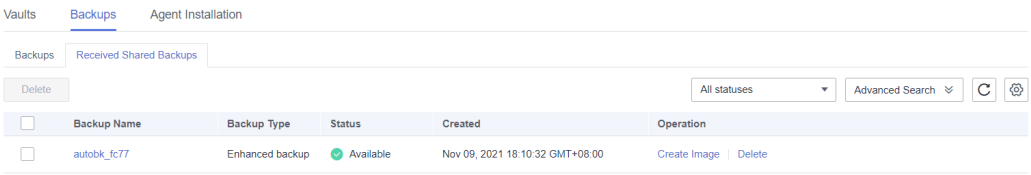
Associação automática: determine se deseja ativar a associação automática para o cofre. Se você seleciona **Configure**, o cofre verifica e associa automaticamente nos servidores do próximo período de backup que não foram copiados e executa o backup.

Figura 3-3 Aceitar um backup compartilhado



Passo 5 Depois que um backup compartilhado for aceito, ele será exibido na lista de backup. Veja **Figura 3-4**.

Figura 3-4 Backup compartilhado aceito



----Fim

3.3 Exclusão de um backup

Você pode excluir backups indesejados para reduzir o uso de espaço e os custos.

A exclusão de um backup de um cofre de backup na nuvem híbrida não afeta o backup correspondente no local e vice-versa.

Se um backup tiver sido usado para criar uma imagem, o backup não poderá ser excluído. Nesse caso, exclua a imagem primeiro com base nas instruções em **Exclusão de imagens**.

Contexto

O CBR suporta exclusão manual de backups e exclusão automática de backups expirados. Este último é implementado com base na regra de retenção de backup na política de backup. Para mais detalhes, consulte **Criação de uma política de backup**.

Pré-requisitos

- Existe pelo menos um backup.
- O backup a ser excluído está no estado **Available** ou **Error**.

Procedimento

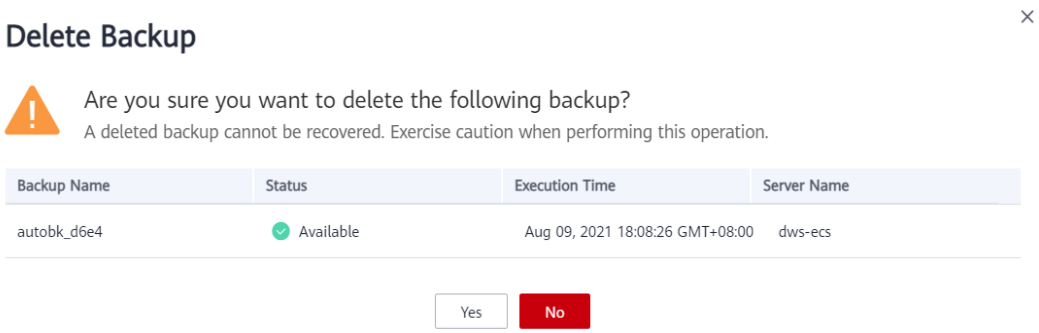
Passo 1 Faça logon no console de CBR.

1. **Efetue logon no console de gerenciamento**.
2. Clique em no canto superior esquerdo e selecione sua região e projeto.
3. Escolha **Storage** > **Cloud Backup and Recovery**. Selecione uma guia de backup no painel de navegação esquerdo.

Passo 2 Em qualquer página de backup, clique na guia **Backups** e localize o backup desejado. Para mais detalhes, consulte **Visualização de um backup**.

Passo 3 Na linha do backup, escolha **More** > **Delete**. Veja **Figura 3-5**. Como alternativa, selecione os backups que deseja excluir e clique em **Delete** no canto superior esquerdo para excluí-los em um lote.

Figura 3-5 Excluir um backup



Passo 4 Clique em **Yes**.

----Fim

Procedimento de acompanhamento

Quando você usa o CBR para fazer backup de um disco, todos os dados do disco, incluindo os dados invisíveis, serão copiados. Se as operações frequentes de adição, exclusão e modificação tiverem sido executadas no disco antes de cada tarefa de backup, uma grande quantidade de espaço do cofre ainda será ocupada mesmo depois que alguns backups forem excluídos. Para saber como reduzir o espaço ocupado do cofre, consulte **Como reduzir o espaço ocupado do cofre por backups?**

3.4 Criação de uma imagem usando um backup

O CBR 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.

Pré-requisitos

- Confirme se as seguintes operações foram executadas antes de usar um backup do ECS para criar uma imagem:
  - você otimizou o ECS do Linux (consultando **Optimização da imagem privada do Linux**) e instalou o Cloud-Init (consultando **Instalação do Cloud-Init**).
  - você otimizou o ECS do Windows (consultando **Optimização da imagem privada do Windows**) e instalou o Cloudbase-Init (consultando **Instalação e Configuração do Cloudbase-Init**).
- Um backup pode ser usado para criar uma imagem em um dos seguintes cenários: 1. O backup está no estado **Available**. 2. O backup está no estado **Creating** que é marcado com **Image can be created**.

  NOTA

  Depois que uma criação de backup é iniciada, o backup entra no estado **Creating**. Após um período de tempo, uma mensagem informando "Imagem pode ser criada" é exibida em **Creating**. Nesse caso, o backup pode ser usado para criar uma imagem, mesmo que ela ainda esteja sendo criada e não possa ser usada para restauração.
- O backup que você deseja usar para criar uma imagem contém os dados do disco do sistema.
- Somente os backups do ECS podem ser usados para criar imagens.

Descrição da função

- As imagens criadas usando um backup são as mesmas, portanto, o CBR permite que você use um backup para criar apenas uma imagem ECS completa que contenha todos os dados do disco do sistema e dos discos de dados de um ECS, a fim de salvar a cota de imagem. Depois que uma imagem é criada, você pode usá-la para provisionar vários ECSs em um lote.
- Um backup com uma imagem criada não pode ser excluído diretamente. Se você quiser excluir esse backup, exclua sua imagem primeiro. Se um backup for gerado automaticamente com base em uma política de backup e o backup tiver sido usado para criar uma imagem, o backup não será contado como um backup retido e não será excluído automaticamente.
- Um backup é compactado quando é usado para criar uma imagem. Portanto, o tamanho da imagem gerada é menor que o do backup.

Procedimento

Passo 1 Faça logon no console de CBR.

1. **Efetue logon no console de gerenciamento**.
2. Clique em no canto superior esquerdo e selecione sua região e projeto.
3. Escolha **Storage** > **Cloud Backup and Recovery**. Selecione uma guia de backup no painel de navegação esquerdo.

Passo 2 Clique na guia **Backups**. Localize o backup desejado. Para mais detalhes, consulte **Visualização de um backup**.

Passo 3 Na linha do backup, escolha **More** > **Create Image**.

Passo 4 Crie uma imagem consultando **Criação de uma imagem ECS completa a partir de um backup do CBR** no *Guia de usuário do Image Management Service*.

Passo 5 Se você quiser usar uma imagem para provisionar ECSs, consulte **Criação de um ECS a partir de uma imagem** no *Guia de usuário do Image Management Service*.

----Fim

3.5 Criação de um disco usando um backup

Você pode usar um backup em disco para criar um disco. Depois que o disco é criado, os dados no novo disco são os mesmos que no backup em disco.

Depois que um novo disco é criado usando os dados de backup de um disco do sistema, o novo disco só pode ser montado no servidor de nuvem como um disco de dados e não pode ser montado como um disco do sistema.

Os backups em disco só podem ser usados para criar discos do EVS, mas não servidores.

Procedimento

Passo 1 Faça logon no console de CBR.

1. **Efetue logon no console de gerenciamento**.
2. Clique em  no canto superior esquerdo e selecione sua região e projeto.
3. Escolha **Storage** > **Cloud Backup and Recovery**. Selecione uma guia de backup no painel de navegação esquerdo.

Passo 2 Clique na guia **Backups**. Localize o backup desejado. Para mais detalhes, consulte **Visualização de um backup**.

Passo 3 Se o status do backup de destino estiver **Available**, clique em **Create Disk** na coluna **Operation** do backup.

Passo 4 Defina os parâmetros do disco.

NOTA

Para obter detalhes sobre esses parâmetros, consulte a tabela de descrição de parâmetros na seção "Compra de um disco do EVS" na *Guia de usuário do Elastic Volume Service*.

Observe os seguintes itens ao definir os parâmetros do disco:

- você pode escolher a AZ à qual o disco de origem de backup pertence ou pode escolher uma AZ diferente.
- o novo disco deve ser pelo menos tão grande quanto o disco de origem do backup.

  Se a capacidade do novo disco for maior que a do disco de origem de backup, inicialize o disco seguindo as etapas fornecidas na seção "Extensão de partições de disco e sistemas de arquivos" do *Guia de usuário do Elastic Volume Service*.
- você pode criar um disco de qualquer tipo, independentemente do tipo de disco do backup.

Passo 5 Clique em **Next**.

NOTA

Você pode escolher **Pay-per-use** ou **Yearly/Monthly** como seu **Billing Mode**. As taxas que você paga dependem do modo de cobrança escolhido. As etapas a seguir usam o modo de cobrança **Yearly/Monthly** como exemplo.

Passo 6 Confirme as informações dos discos e clique em **Submit**.

Passo 7 Pague as taxas conforme solicitado e clique em **OK**.

Passo 8 Volte para a lista de discos. Verifique se o disco foi criado com êxito.

Você verá o status do disco mudar da seguinte forma: **Creating**, **Available**, **Restoring**, **Available**. Você pode não perceber o status **Restoring** porque o Instant Restore é suportado e a velocidade de restauração é muito rápida. Depois que o status do disco for alterado de **Creating** para **Available**, o disco será criado com êxito. Depois que o status for alterado de **Restoring** para **Available**, os dados de backup foram restaurados com êxito no disco criado.

----Fim

3.6 Criação de um sistema de arquivos usando um backup

No caso de um ataque de vírus, exclusão acidental ou falha de software ou hardware, 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.

Procedimento

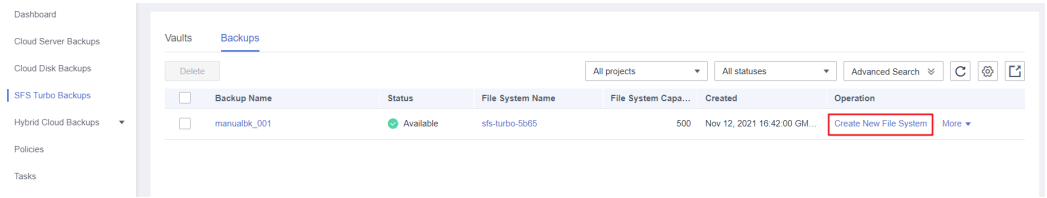
Passo 1 Faça logon no console de CBR.

1. **Efetue logon no console de gerenciamento**.
2. Clique em no canto superior esquerdo e selecione sua região e projeto.
3. Escolha **Storage** > **Cloud Backup and Recovery**. Selecione uma guia de backup no painel de navegação esquerdo.

Passo 2 Clique na guia **Backups**. Localize o backup desejado. Para mais detalhes, consulte **Visualização de um backup**.

Passo 3 Se o status do backup de destino estiver **Available**, clique em **Create File System** na coluna **Operation** do backup.

Figura 3-6 Visualizar um backup



NOTA

Para saber como criar backups, consulte **Compra de um cofre de backup do SFS Turbo** e **Criação de um backup do SFS**.

Passo 4 Defina os parâmetros do sistema de arquivos.

NOTA

- Para obter descrições detalhadas dos parâmetros, consulte a tabela "Descrição do parâmetro" em **Criação de um sistema de arquivos do SFS Turbo**.
- Você pode alterar a classe de armazenamento do sistema de arquivos dentro de um determinado intervalo. Por exemplo, você pode alterar um sistema de arquivos de Padrão para Desempenho, mas não pode de Padrão para Padrão - Aprimorado.
- O modo de cobrança do novo sistema de arquivos só pode ser pagamento por uso.

Passo 5 Clique em **Next**.

Passo 6 Confirme as informações do sistema de arquivos e clique em **Submit**.

Passo 7 Pague as taxas conforme solicitado e clique em **OK**.

Passo 8 Volte para a lista do sistema de arquivos e verifique se o sistema de arquivos foi criado com êxito.

Você verá o status do sistema de arquivos mudar da seguinte forma: **Creating**, **Available**, **Restoring**, **Available**. Você pode não perceber o status **Restoring** porque a Restauração instantânea é suportada e a velocidade de restauração é muito rápida. Depois que o status do sistema de arquivos for alterado de **Creating** para **Available**, o sistema de arquivos será criado com êxito. Depois que o status for alterado de **Restoring** para **Available**, os dados de backup foram restaurados no sistema de arquivos com êxito.

----Fim

3.7 Replicação de um backup (entre regiões)

O CBR permite replicar backups do servidor e backups do SFS Turbo de uma região para outra. Réplicas de backups de servidor na região de destino podem ser usadas para criar imagens e provisionar servidores. Réplicas de backups do sistema de arquivos do SFS Turbo na região de destino podem ser usadas para criar sistemas de arquivos. Com a replicação de backup, você pode implantar rapidamente serviços em uma região diferente. O estado do novo recurso na região de destino é o mesmo do recurso de origem no ponto de tempo de backup na região de origem.

O console do CBR fornece os seguintes métodos de replicação:

- selecione um backup na lista de backup e execute a replicação pontual manualmente.
- selecione um cofre de backup e replicá-lo manualmente. Em alternativa, pode configurar uma política de replicação para replicar periodicamente cópias de segurança que não tenham sido replicadas ou que não tenham sido replicadas para a região de destino.

Esta seção usa a primeira maneira de descrever como replicar um backup. Para obter detalhes sobre o segundo método, consulte **Replicação de um cofre**.

NOTA

As restrições a seguir se aplicam a ambos os métodos de replicação.

Restrições

- Os backups em disco em nuvem não podem ser replicados para outras regiões.
- Esta característica está disponível somente nas regiões CN-Hong Kong, AP-Singapore, e AP-Bangkok atualmente.

- um backup de servidor pode ser replicado somente quando atende a todas as seguintes condições:
  a. é um backup do ECS.
  b. contém dados do disco do sistema.
  c. está no estado **Available**.
- Somente backups e cofres na região atual podem ser replicados. As réplicas não podem ser replicadas novamente, mas podem ser usadas para criar imagens ou sistemas de arquivos.
- 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 tiver sido excluída na região de destino.
  – 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.

Procedimento

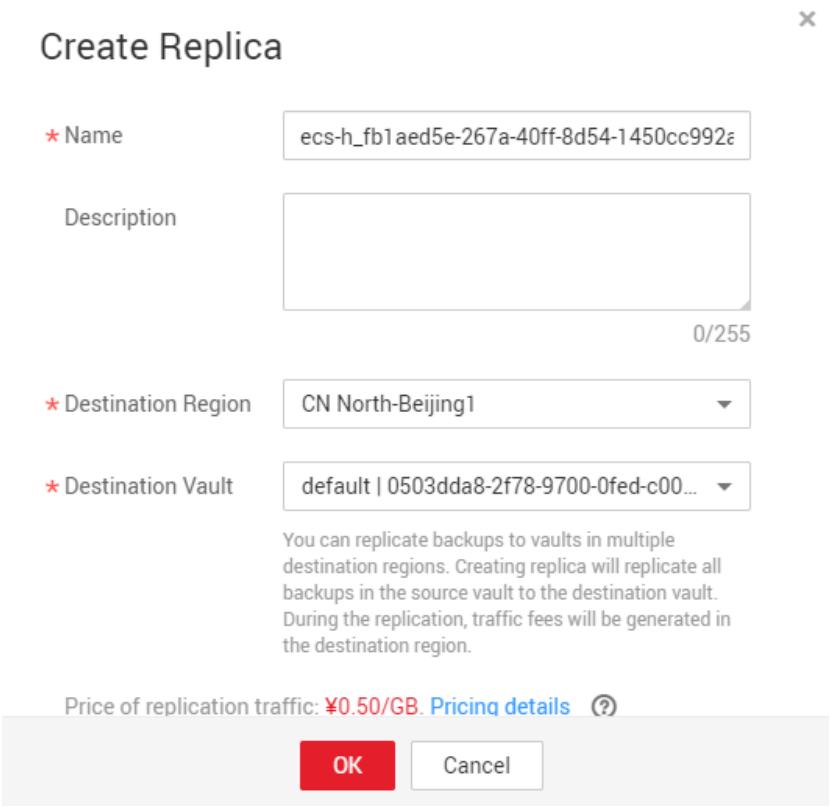
Passo 1 Faça logon no console de CBR.

1. **Efetue logon no console de gerenciamento**.
2. Clique em  no canto superior esquerdo e selecione sua região e projeto.
3. Escolha **Storage** > **Cloud Backup and Recovery**. Selecione uma guia de backup no painel de navegação esquerdo.

Passo 2 Clique na guia **Backups** e localize o backup desejado. Para mais detalhes, consulte **Visualização de um backup**.

Passo 3 Clique em **More** e escolha **Create Replica** na coluna **Operation** do backup. Veja **Figura 3-7**.

Figura 3-7 Criar uma réplica



Passo 4 Na caixa de diálogo exibida, especifique os parâmetros descritos em **Tabela 3-2**.

Tabela 3-2 Descrição do parâmetro

Parâmetro	Descrição
Name	Nome da réplica Um nome deve conter de 1 a 64 caracteres, incluindo dígitos, letras, sublinhados (_) ou hífenes (-).
Description	Descrição da réplica Não pode exceder 255 caracteres.
Destination Region	Região para a qual o cofre é replicado Somente as regiões que oferecem suporte à replicação serão exibidas. ● Se a região selecionada contiver apenas um projeto, você poderá selecionar diretamente o nome da região. ● Se a região selecionada tiver vários projetos, o projeto principal da região será selecionado por padrão. Você pode selecionar outro projeto, se necessário.

Parâmetro	Descrição
Destination Vault	Um cofre de replicação na região de destino Você pode replicar backups em cofres de diversas regiões de destino. A criação de uma réplica replicará todos os backups do cofre de fonte no cofre de destino.

NOTA

O tráfego para replicação entre regiões é o tamanho do backup replicado.

Passo 5 Clique em **OK**.

Passo 6 Após a conclusão da replicação, você pode alternar para a região de destino para exibir réplicas geradas. Para mais detalhes, consulte **Visualização de um backup**. Em seguida, você pode usar réplicas para criar imagens.

----Fim

4 Gerenciamento de políticas

4.1 Criação de uma política de backup

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.

Para implementar backup periódico, você precisa criar uma política de backup primeiro. O CBR executará backups periodicamente de acordo com o tempo de execução especificado na política de backup. Você pode optar por usar a política de backup padrão fornecida pelo CBR ou criar uma conforme necessário.

Você pode aplicar políticas de backup a cofres de backup do servidor, cofres de backup do SFS Turbo, e cofres de backup em disco.

Contexto

- Depois que uma política de backup é ativada, o CBR faz backup automaticamente dos recursos associados aos cofres que foram associados à política e exclui periodicamente os backups expirados.
- Cada conta pode criar um máximo de 32 políticas de backup.
- Ao configurar o tempo de backup e o tempo de replicação, certifique-se de que uma tarefa de replicação seja iniciada após a conclusão de uma tarefa de backup. Ou, a replicação pode falhar.
- Quando os backups expirados são apagados com base nas regras de retenção de uma política, apenas os backups automáticos são excluídos. O backup manual não será excluído.
- Somente servidores no estado **Running** ou **Stopped** podem ser copiados.
- Somente os discos no estado **Available** ou **In-use** podem ser copiados.

Procedimento

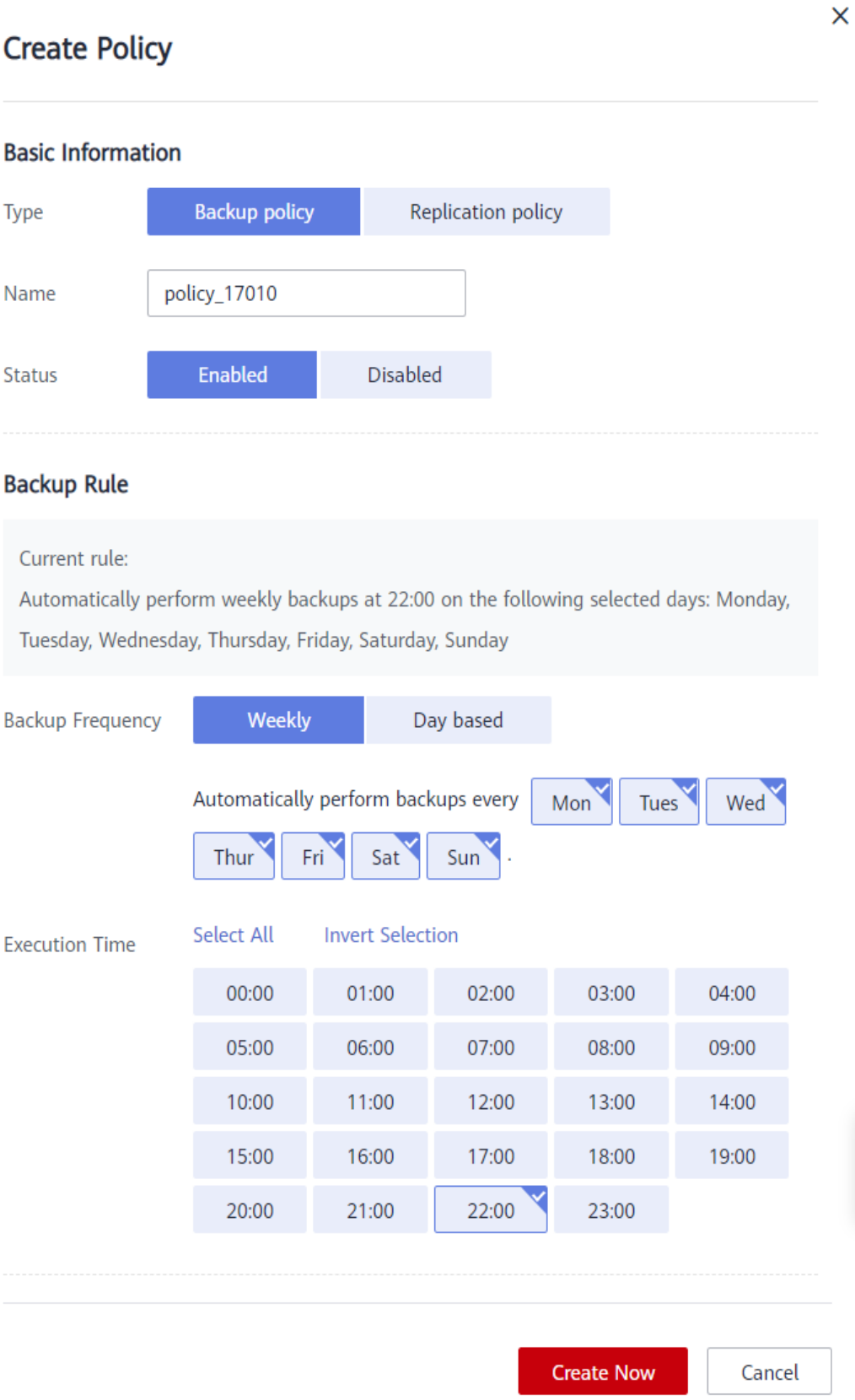
Passo 1 Faça logon no console de CBR.

1. **Efetue logon no console de gerenciamento**.

2. Clique em  no canto superior esquerdo e selecione sua região e projeto.
3. Escolha **Storage** > **Cloud Backup and Recovery**. Selecione uma guia de backup no painel de navegação esquerdo.

Passo 2 Escolha **Policies** e clique na guia **Backup Policies**. No canto superior direito, clique em **Create Policy**. Veja **Figura 4-1**.

Figura 4-1 Criar uma política de backup



Passo 3 Definir os parâmetros da política de backup. **Tabela 4-1** descreve os parâmetros.

Tabela 4-1 Descrição do parâmetro de política de backup

Parâmetro	Descrição	Valor de exemplo
Type	Selecione um tipo de política. Esta seção usa a criação de uma política de backup como um exemplo.	Política de backup
Name	Nome da política de backup Um nome deve conter de 1 a 64 caracteres, incluindo dígitos, letras, sublinhados (_) ou hífenes (-).	backup_policy
Status	Se deve ativar a política de backup.	Somente após a ativação de uma política de backup, o CBR fará backup automático de servidores e discos associados aos cofres aplicados à política e excluirá backups expirados.
Backup Frequency	Datas para realização de backups ● **Weekly** Especifica em quais dias de cada semana a tarefa de backup será executada. Você pode selecionar vários dias. ● **Day based** Especifica o intervalo (a cada 1 a 30 dias) para a execução da tarefa de backup.	Todos os dias Se você selecionar backup baseado em dia, o primeiro horário de backup deverá ser no dia em que a política de backup for criada. Se o tempo de criação da política de backup for posterior ao tempo de execução mais recente, o backup inicial será realizado no próximo ciclo de backup. Recomenda-se que os backups sejam realizados fora do horário de pico ou quando não houver serviços em execução.

Parâmetro	Descrição	Valor de exemplo
Execution Time	Tempo de execução Os backups podem ser agendados no início de cada hora. Várias seleções são suportadas. **AVISO** ● Pode haver uma diferença de tempo entre o tempo de backup agendado e o tempo de backup real. ● Para fazer backup de uma grande quantidade de dados, é aconselhável definir um cronograma de backup menos frequente. Se uma tarefa de backup demorar mais do que o intervalo de backup, o sistema ignorará o próximo tempo de execução de backup. Por exemplo, conforme programado em uma política de backup, um disco precisa ser copiado às 00:00, 01:00 e 02:00. Às 00:00, o disco começa a ser copiado. Como os dados incrementais de alto volume precisam ser copiados ou uma pilha de tarefas de backup são executadas ao mesmo tempo, essa tarefa de backup leva 90 minutos e é concluída às 01:30. Nesse caso, o sistema realiza o próximo backup às 02:00. Portanto, apenas dois backups serão gerados no total, um às 00:00 e outro às 02:00.	00:00, 02:00 Recomenda-se que os backups sejam realizados fora do horário de pico ou quando não houver serviços em execução.
Full Backup	Se realizar backups completos periódicos. ● Enable Ativar o backup completo melhora a confiabilidade dos dados, mas backups completos usarão mais espaço de armazenamento. Configurar uma frequência de backup completa. O valor varia de **0** a **100**. Valor **0** indica que um backup completo será realizado em todas as tarefas de backup. ● Do not enable O backup completo periódico não será realizado. Em vez disso, o sistema sempre executará backups incrementais após o backup inicial. **AVISO** Um backup completo geralmente leva um longo tempo. Se um backup completo de um recurso estiver sendo executado, outros backups desse recurso não serão gerados. Por exemplo, quaisquer backups orientados por políticas planejados para serem executados durante o backup completo serão ignorados. Você pode fazer backup de dados fora do horário de pico.	7

Parâmetro	Descrição	Valor de exemplo
Retention Rule	Regra que especifica como os backups serão mantidos ● **Time period** Você pode optar por manter backups por um mês, três meses, seis meses, um ano ou por qualquer número desejado (2 a 99999) de dias. ● **Backup quantity** Você pode definir o número máximo de backups do servidor em nuvem a serem mantidos para um servidor em nuvem. O valor varia de 2 a 99999. ● **Advanced Options** Você também pode definir regras de retenção de longo prazo com opções avançadas. As regras de retenção de longo prazo e as regras de retenção baseadas em quantidade não entram em conflito. Ambos serão aplicados. – **Day-based**: O valor varia de **0** a **100**. – **Weekly**: O valor varia de **0** a **100**. – **Monthly**: O valor varia de **0** a **100**. – **Yearly**: O valor varia de **0** a **100**. Por exemplo, a opção avançada baseada em dia retém o backup mais recente por dia. Se o backup de um disco for feito várias vezes em um dia, somente o backup mais recente daquele dia será mantido. Se você definir o valor como 5, o sistema manterá o backup mais recente de cada um dos últimos cinco dias que tiveram backups gerados. Se houver mais de cinco arquivos de backup, o sistema excluirá automaticamente os primeiros backups. Se as opções avançadas diárias, semanais, mensais e anuais estiverem todas configuradas, os backups de união serão selecionados para retenção. Por exemplo, se o número de backups diários retidos for definido como 5 e o número de backups semanais retidos for definido como 1, cinco backups serão retidos. A regra de retenção de longo prazo e a regra de retenção baseada em quantidade podem ser eficazes ao mesmo tempo. ● **Permanent**	6 meses

Parâmetro	Descrição	Valor de exemplo
	NOTA – Quando o número de backups retidos excede o valor predefinido, o sistema exclui automaticamente os backups mais antigos. Quando os períodos de retenção dos backups retidos excedem o valor predefinido, o sistema exclui automaticamente todos os backups expirados. Por padrão, o sistema apaga automaticamente os dados a cada dois dias. O backup excluído não afeta outros backups para restauração. – Os backups expirados não são excluídos logo após expirarem. Eles serão excluídos das 12:00 às 0:00 em lotes. – Esse parâmetro se aplica somente aos backups gerados com base em uma política de backup agendada. Os backups manuais não são afetados por este parâmetro e não serão excluídos automaticamente. Você pode excluí-los manualmente da lista de backup. – Depois que um backup é usado para criar uma imagem, o backup não será contado como um backup retido e não será excluído automaticamente. – Um máximo de 10 backups são mantidos para tarefas de backup periódicas com falha. Eles são mantidos por um mês e podem ser excluídos manualmente.	

NOTA

Intervalos de backup mais frequentes criam mais backups ou retêm backups por mais tempo, protegendo os dados em maior medida, mas ocupando mais espaço de armazenamento. Defina um ciclo de backup apropriado, conforme necessário.

Passo 4 Clique em **OK**.

Passo 5 Localize o Vault desejado e escolha **More** > **Apply Backup Policy** para aplicar a política criada ao cofre. É possível visualizar a política aplicada na página de detalhes do cofre.

Depois que a política for aplicada, os dados serão periodicamente copiados para o cofre com base na política.

----Fim

Exemplo

Um usuário tem um cofre associado a um disco. Às 10:00 da manhã. na segunda-feira, o usuário define uma política de backup para o cofre, ou seja, executa uma tarefa de backup às 02:00 da manhã. todos os dias e retendo no máximo três backups. Às 11:00 da manhã. no sábado, três backups são mantidos, que são gerados na quarta-feira, quinta-feira e sexta-feira. O backup gerado às 2:00 da manhã. na terça-feira foi automaticamente excluído.

4.2 Criação de uma política de replicação

Depois que uma política de replicação é configurada, o CBR replicará periodicamente backups que não foram replicados ou que não foram replicados para a região de destino.

Você pode aplicar políticas de replicação a cofres de backup do servidor, cofres de backup da nuvem híbrida, e cofres de backup do SFS Turbo.

Contexto

Ao configurar o tempo de backup e o tempo de replicação, certifique-se de que uma tarefa de replicação seja iniciada após a conclusão de uma tarefa de backup. Ou, a replicação pode falhar.

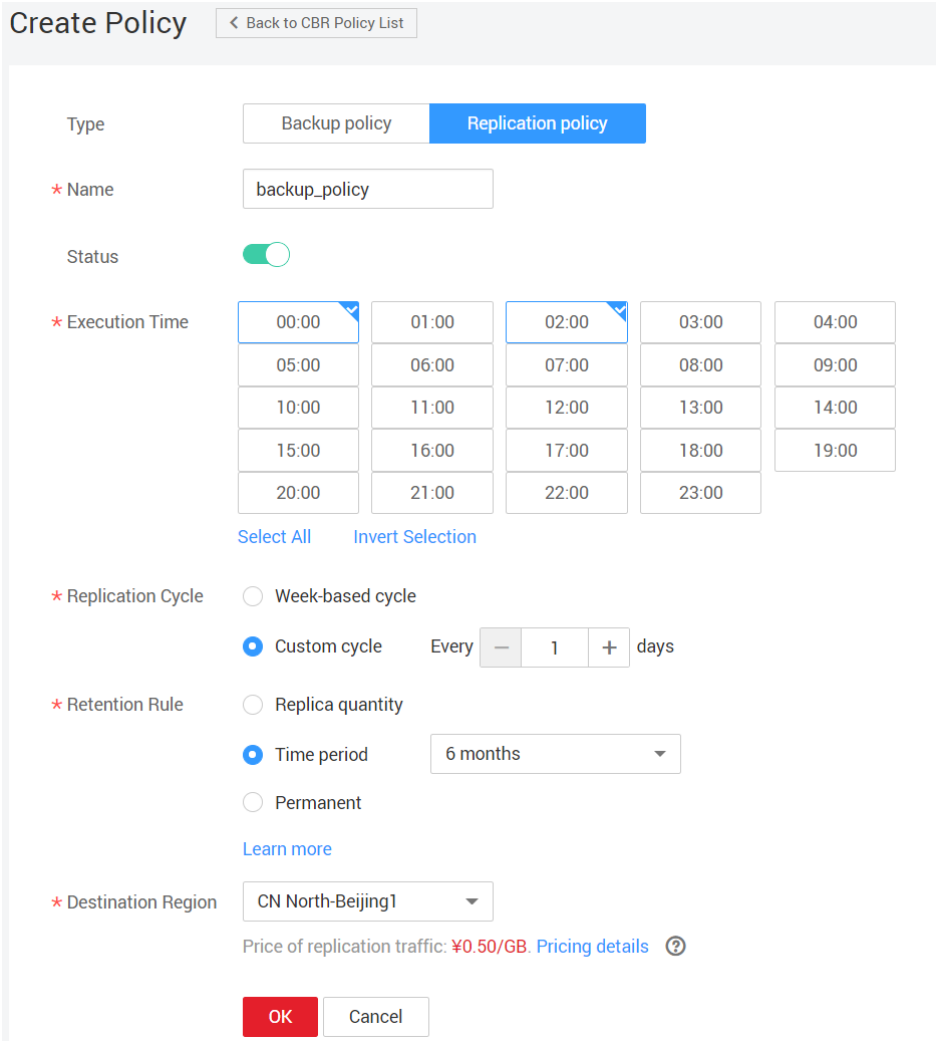
Procedimento

Passo 1 Faça logon no console de CBR.

1. **Efetue logon no console de gerenciamento**.
2. Clique em  no canto superior esquerdo e selecione sua região e projeto.
3. Escolha **Storage** > **Cloud Backup and Recovery**. Selecione uma guia de backup no painel de navegação esquerdo.

Passo 2 Clique na guia **Replication Policies**. No canto superior direito, clique em **Create Policy**. Veja **Figura 4-2**.

Figura 4-2 Criar de uma política de replicação



Passo 3 Definir os parâmetros da política de replicação. **Tabela 4-2** descreve os parâmetros.

Tabela 4-2 Descrição do parâmetro de política de replicação

Parâmetro	Descrição	Observações
Type	Selecione um tipo de política. Esta seção usa a criação de uma política de replicação como um exemplo.	Política de replicação
Name	Nome da política de replicação Um nome deve conter de 1 a 64 caracteres, incluindo dígitos, letras, sublinhados (_) ou hífenes (-).	replication_policy

Parâmetro	Descrição	Observações
Status	Se ativar a política de replicação	Somente depois que uma política de replicação for ativada, o CBR replicará automaticamente os backups nos cofres que foram associados à política e excluirá os backups expirados.
Execution Time	Tempos de execução da política de replicação em um dia As tarefas de replicação podem ser agendadas no início de cada hora. Várias seleções são suportadas.	00:00, 02:00 Recomenda-se que a replicação seja realizada fora do horário de pico ou quando não houver serviços em execução.
Replication Frequency	Datas de execução da tarefa de replicação ● **Weekly** Especifica em que dias de cada semana a tarefa de replicação será executada. Você pode selecionar vários dias. ● **Day based** Especifica o intervalo (a cada 1 a 30 dias) para execução da tarefa de replicação.	Todos os dias Se seleccionar replicação baseada em dia, a primeira hora de replicação deverá ser no dia em que a política de replicação é criada. Se o tempo de criação da política de replicação for posterior ao tempo de execução mais recente, a replicação inicial será executada no próximo ciclo de replicação.

Parâmetro	Descrição	Observações
Retention Rule	Regras de retenção de réplicas geradas na região de destino ● **Replica quantity** Especifica o número máximo de réplicas permitidas para um único servidor de nuvem. O valor varia de 2 a 99999. Você também pode definir regras de retenção de longo prazo com opções avançadas. As regras de retenção de longo prazo e as regras de retenção baseadas em quantidade não entram em conflito. Ambos serão aplicados. – **Day-based**: o valor varia de **0** a **100**. – **Weekly**: o valor varia de **0** a **100**. – **Monthly**: o valor varia de **0** a **100**. – **Yearly**: o valor varia de **0** a **100**. Por exemplo, a opção avançada diária mantém a réplica de backup mais recente por dia. Embora o backup seja replicado várias vezes em um dia, somente a última réplica do dia atual é mantida. Se você definir o valor como 5, o sistema manterá a réplica mais recente de cada um dos últimos cinco dias com réplicas de backup geradas. Se houver mais de cinco réplicas de backup, o sistema excluirá automaticamente as réplicas de backup mais antigas. Se as opções avançadas diárias, semanais, mensais e anuais estiverem configuradas, as réplicas de backup da união serão selecionadas para retenção. Por exemplo, se o número de réplicas de backup diárias retidas for definido como 5 e o número de réplicas de backup semanais retidas for definido como 1, cinco réplicas de backup serão retidas. A regra de retenção de longo prazo e a regra de retenção baseada em quantidade podem ser eficazes ao mesmo tempo. ● **Time period** Você pode optar por manter réplicas por um mês, três meses, seis meses, um ano ou por qualquer número desejado (2 a 99999) de dias. ● **Permanent**	6 meses

Parâmetro	Descrição	Observações
	NOTA – Quando o número de réplicas de backup retidas excede o valor predefinido, o sistema exclui automaticamente as réplicas mais antigas. Quando os períodos de retenção das réplicas retidas excedem o valor predefinido, o sistema exclui automaticamente todas as réplicas vencidas. Por padrão, o sistema apaga automaticamente os dados a cada dois dias. – Há um atraso na exclusão de réplicas de backup expiradas, mas normalmente esse atraso não será superior a 24 horas. – Este parâmetro aplica-se apenas a réplicas geradas com base numa política de replicação agendada. Essas réplicas criadas manualmente não são afetadas por esse parâmetro e não serão excluídas automaticamente. Você pode excluí-los manualmente da lista de backup. – Depois que uma réplica for usada para criar uma imagem ou um sistema de arquivos, ela não será contada como um backup retido e não será excluída automaticamente.	
região de destino	Região para a qual o backup é replicado Somente as regiões que oferecem suporte à replicação serão exibidas. ● Se a região selecionada contiver apenas um projeto, você poderá selecionar diretamente o nome da região. ● Se a região selecionada tiver vários projetos, o projeto principal da região será selecionado por padrão. Você pode selecionar outro projeto, se necessário.	AP-Bangkok
Ativar aceleração	Se acelera a replicação A função de aceleração é faturada pelo tráfego.	-

Passo 4 Clique em **Create Now**.

Passo 5 Localize o cofre desejado e escolha **More** > **Apply Replication Policy** para aplicar a política de replicação criada ao cofre. É possível visualizar a política de replicação aplicada na página de detalhes do cofre.

Depois que a configuração é bem-sucedida, os backups são replicados periodicamente para o cofre de destino com base na política de replicação.

----Fim

Exemplo

Um usuário aplica uma política de replicação a um cofre às 11:00 a.m. quinta-feira em uma determinada região. De acordo com a política, os backups serão replicados para a região de destino às 02:00 da manhã. todos os dias, e duas réplicas de backup serão mantidas. Esse cofre também tem uma política de backup aplicada, que cria automaticamente dois backups às 00:00 todos os dias. Às 12:00 p.m. no sábado, o cofre de replicação conterá duas réplicas de backup, que são replicadas no sábado. Réplicas de backup geradas às 02:00 a.m. na sexta-feira foram excluídos automaticamente de acordo com a política de replicação.

4.3 Modificação de uma política

Esta seção descreve como modificar uma política.

Pré-requisitos

Você criou pelo menos uma política.

Procedimento

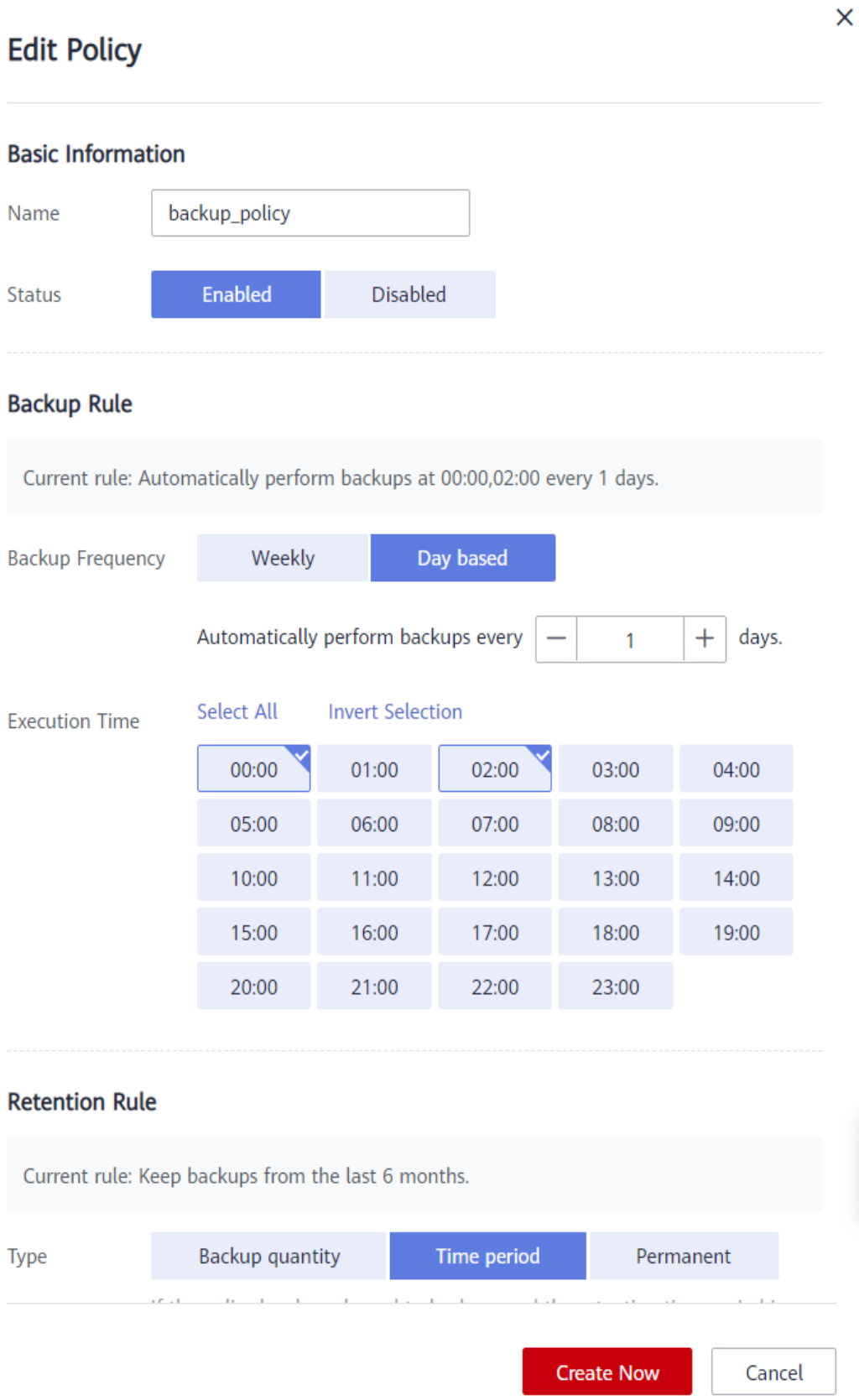
Passo 1 Faça logon no console de CBR.

1. **Efetue logon no console de gerenciamento**.
2. Clique em  no canto superior esquerdo e selecione sua região e projeto.
3. Escolha **Storage** > **Cloud Backup and Recovery**. Selecione uma guia de backup no painel de navegação esquerdo.

Passo 2 Em qualquer página de backup, localize o cofre de destino e clique no nome do cofre para visualizar os detalhes do cofre.

Passo 3 Na área **Policies**, clique em **Edit** para abrir a página de edição de política. Veja **Figura 4-3**.

Figura 4-3 Editar uma política de backup



Os parâmetros relacionados são descritos em **Tabela 4-1** e **Tabela 4-2**.

Passo 4 Clique em **OK**.

Se a regra de retenção de política for modificada, a nova regra entrará em vigor dependendo de como você a alterou. Para mais detalhes, consulte **Por que a regra de retenção não entra em vigor depois de ser modificada**

Passo 5 Como alternativa, você pode selecionar **Policies** na árvore de navegação à esquerda e editar a política desejada.

----Fim

4.4 Exclusão de uma política

Você pode excluir políticas de backup e replicação, se necessário.

Pré-requisitos

Você criou pelo menos uma política.

Procedimento

Passo 1 Faça logon no console de CBR.

1. **Efetue logon no console de gerenciamento**.
2. Clique em no canto superior esquerdo e selecione sua região e projeto.
3. Escolha **Storage** > **Cloud Backup and Recovery**. Selecione uma guia de backup no painel de navegação esquerdo.

Passo 2 Clique em **Backup Policies**, localize a linha que contém a política que pretende excluir e clique em **Delete**.

NOTA

A exclusão de uma política não excluirá os backups gerados com base na política. Você pode excluir manualmente backups indesejadas.

Passo 3 Confirme as informações e clique em **Yes**.

----Fim

4.5 Aplicação de uma política a um cofre

Uma política de backup ou replicação permite que um cofre execute automaticamente tarefas de backup ou replicação em horários ou intervalos especificados. Backups periódicos podem ser usados para restaurar dados rapidamente contra corrupção ou perda de dados.

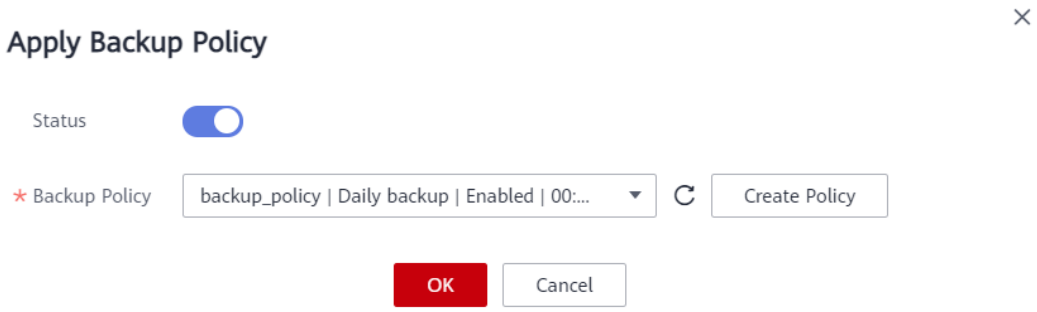
Procedimento

Passo 1 Faça logon no console de CBR.

1. **Efetue logon no console de gerenciamento**.
2. Clique em no canto superior esquerdo e selecione sua região e projeto.
3. Escolha **Storage** > **Cloud Backup and Recovery**. Selecione uma guia de backup no painel de navegação esquerdo.

Passo 2 Em qualquer página de backup, localize o cofre de destino e escolha **More** > **Apply Backup Policy** ou **More** > **Apply Replication Policy**. Veja **Figura 4-4**.

Figura 4-4 Definir uma política de backup



Passo 3 Você pode selecionar uma política de backup existente na lista suspensa ou criar uma nova. Para saber como criar uma política, veja **Criação de uma política de backup** e **Criação de uma política de replicação**.

Passo 4 Depois que a política é aplicada com êxito, você pode visualizar os detalhes na área **Policies** na página de detalhes do cofre.

----Fim

4.6 Removimento de uma política de um cofre

Se você não precisar mais de backup ou replicação automático para um cofre, remova a política do cofre.

Pré-requisitos

Uma política foi aplicada ao cofre.

Procedimento

Passo 1 Faça logon no console de CBR.

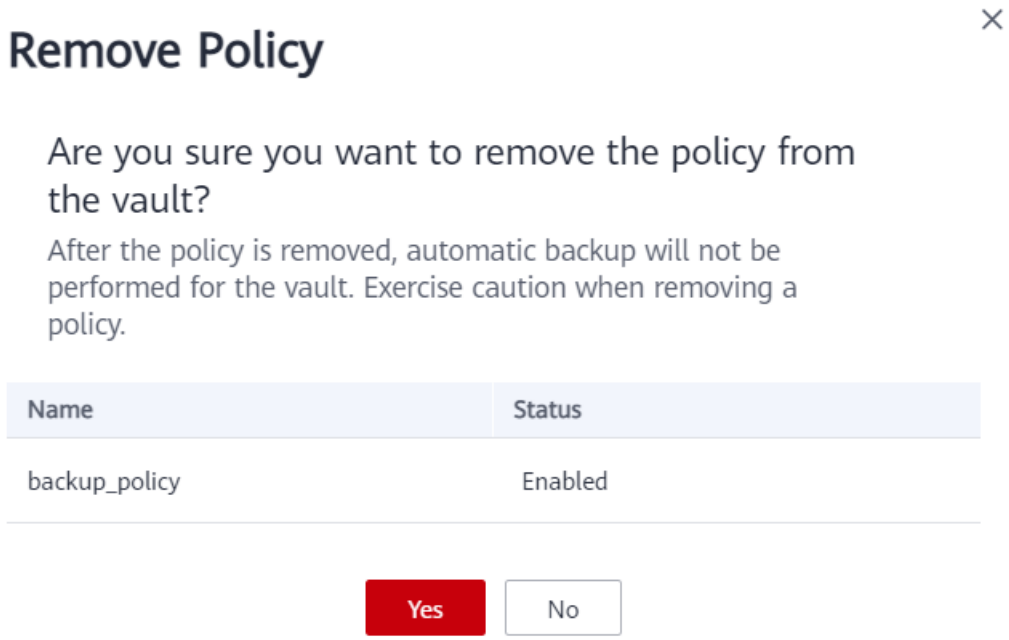
1. **Efetue logon no console de gerenciamento**.

2. Clique em no canto superior esquerdo e selecione sua região e projeto.
3. Escolha **Storage** > **Cloud Backup and Recovery**. Selecione uma guia de backup no painel de navegação esquerdo.

Passo 2 Em qualquer página de backup, localize o cofre de destino e clique no nome do cofre para visualizar os detalhes do cofre.

Passo 3 Na área **Policies**, clique em **Remove Policy**. Veja **Figura 4-5**.

Figura 4-5 Remover uma política



NOTA

- Se uma tarefa de backup estiver sendo executada para um recurso no cofre, a política poderá ser removida normalmente. No entanto, a tarefa de backup continuará e os backups serão gerados.
- Depois que uma política for removida, os backups retidos por tempo expirarão com base na regra de retenção, mas os backups retidos por quantidade não serão excluídos automaticamente. Você pode excluir manualmente backups indesejados.

Passo 4 Clique em **Yes**. O cofre não executará mais tarefas conforme especificado nesta política.

----Fim

5 Restauração de dados

5.1 Restauração de dados usando o Cloud Server Backup

Quando os discos de um servidor estão com defeito ou os dados do servidor são perdidos devido a operações incorretas, você pode usar um backup para restaurar o servidor.

Para restaurar dados em outro servidor, consulte **Como restaurar dados no servidor original para um novo servidor?**

Contexto

- Os dados em discos de dados não podem ser restaurados para discos do sistema.
- Os dados não podem ser restaurados para servidores no estado **Faulty**.
- A restauração simultânea de dados não é suportada.

Pré-requisitos

- Discos no servidor cujos dados precisam de ser restaurados estão funcionando corretamente.
- O servidor cujos dados precisam ser restaurados tem pelo menos um backup **Available**.

Procedimento

Passo 1 Faça logon no console de CBR.

1. **Efetue logon no console de gerenciamento**.
2. Clique em  no canto superior esquerdo e selecione sua região e projeto.
3. Escolha **Storage** > **Cloud Backup and Recovery**. Selecione uma guia de backup no painel de navegação esquerdo.

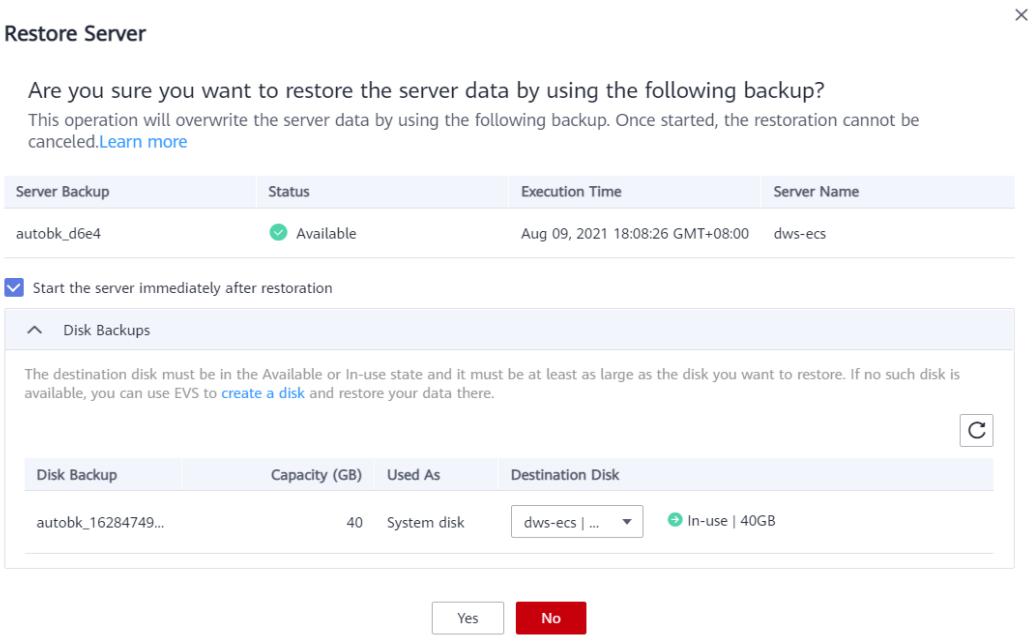
Passo 2 Clique na guia **Backups**. Localize o backup desejado. Para mais detalhes, consulte **Visualização de um backup**.

Passo 3 Na linha do backup, clique em **Restore Server**. Veja **Figura 5-1**.

AVISO

Os dados históricos no ponto de backup no tempo substituirão os dados atuais do servidor. A restauração não pode ser desfeita.

Figura 5-1 Restaurar um servidor



Passo 4 (Opcional) Desmarque **Start the server immediately after restoration**.

Se você desmarcar **Start the server immediately after restoration**, inicie manualmente o servidor após a conclusão da restauração.

AVISO

Os servidores são desligados durante a restauração. Portanto, é recomendável que você realize operações de restauração fora do horário de pico.

Passo 5 Na lista suspensa **Specified Disk**, selecione o disco de destino para o qual o backup será restaurado.

NOTA

- Se o servidor tiver apenas um disco, o backup será restaurado no disco por padrão.
- Se o servidor tiver vários discos, o backup será restaurado para os discos originais, respectivamente, por padrão. Você também pode restaurar o backup em outro disco no servidor de backup selecionando o disco na lista suspensa. No entanto, o disco de destino especificado deve ser pelo menos tão grande quanto o disco de origem de backup.
- Os dados de backup de discos de dados não podem ser restaurados em discos do sistema.

AVISO

Se o número de discos a serem restaurados for maior do que o número de discos que são armazenados em backup, a restauração pode causar inconsistência de dados.

Por exemplo, se os dados da Oracle estiverem espalhados por vários discos e apenas alguns deles forem restaurados, ocorrerá inconsistência de dados após a restauração e a aplicação poderá não conseguir iniciar.

Passo 6 Clique em **Yes** e confirme se a restauração foi bem-sucedida.

Na lista de backup, visualize o status de restauração. Quando o backup entra no estado **Available** e não existem novas tarefas de restauração com falha em **Tasks**, a restauração é bem-sucedida. O recurso é restaurado para o estado no momento em que você fez esse backup.

Para obter detalhes sobre como exibir tarefas de restauração com falha, consulte **Gerenciamento de tarefas**.

AVISO

Se um servidor Windows for restaurado, os discos de dados podem não ser exibidos devido a limitações do Windows.

Depois de usar um backup do servidor de nuvem para restaurar um grupo de volumes lógicos, o grupo de volumes lógicos precisa ser anexado novamente.

Você precisa on-line manualmente esses discos de dados. Para obter detalhes, consulte **Discos de dados não são exibidos depois que um Windows Server é restaurado**.

----Fim

5.2 Restauração de dados usando um backup de disco em nuvem

Você pode usar um backup em disco para restaurar um disco para o momento em que o backup foi criado.

Pré-requisitos

- O status do disco a ser restaurado deve estar **Available**.

- Antes de restaurar os dados do disco, interrompa o servidor ao qual o disco está conectado e desconecte o disco do servidor. Depois que os dados do disco forem restaurados, conecte o disco ao servidor e inicie o servidor.

Restrições

- Se o sistema operacional do servidor for alterado após o backup do disco do sistema, o backup do disco do sistema não poderá ser restaurado para o disco do sistema original devido a razões como a alteração do UUID do disco. Você pode usar o backup de disco do sistema para criar um novo disco e, em seguida, importar dados para o disco do sistema original.
- Os backups só podem ser restaurados em discos originais. Se você quiser restaurar um backup em um disco diferente do original, use diretamente o backup para criar um novo disco.
- Para restaurar o backup de um disco de dados para o disco do sistema, consulte **Como restaurar um backup de disco de dados para um disco do sistema?**
- A restauração simultânea de dados não é suportada.

Procedimento

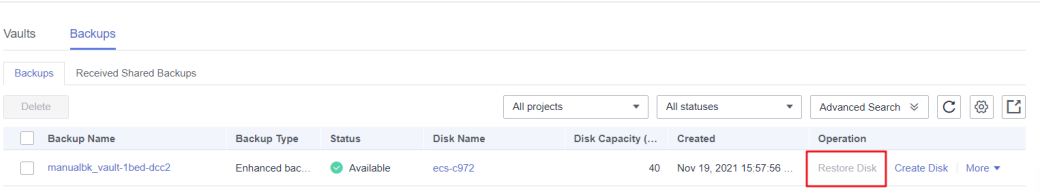
Passo 1 Faça logon no console de CBR.

1. **Efetue logon no console de gerenciamento**.
2. Clique em  no canto superior esquerdo e selecione sua região e projeto.
3. Escolha **Storage** > **Cloud Backup and Recovery**. Selecione uma guia de backup no painel de navegação esquerdo.

Passo 2 Clique na guia **Backups**. Localize o backup desejado. Para mais detalhes, consulte **Visualização de um backup**.

Passo 3 Na linha do backup, clique em **Restore Disk**. A página **Restore Disk** é exibida. Veja **Figura 5-3**.

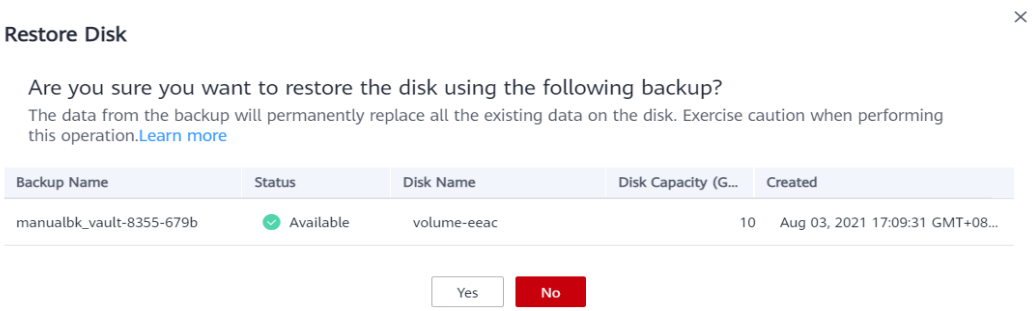
Figura 5-2 Localizar o backup de destino



AVISO

- Os dados de backup substituirão os dados atuais do disco e a restauração não poderá ser desfeita.
- Se o botão de restauração estiver acinzentado, pare o servidor, desconecte o disco a ser restaurado e, em seguida, restaure os dados. Depois que os dados do disco forem restaurados, conecte o disco ao servidor e inicie o servidor.

Figura 5-3 Discos restaurados



Passo 4 Clique em **Yes**. Você pode verificar se os dados foram restaurados com êxito na página da guia **Backups** de **Disk Backups** ou no console do EVS.

Quando o status do backup é alterado para **Available**, a restauração é bem-sucedida. O recurso é restaurado para o estado no momento em que você fez esse backup.

Passo 5 Após a conclusão da restauração, volte a anexar o disco ao servidor. Para obter detalhes, consulte **Anexação de um disco não compartilhado existente**

----Fim

5.3 Restauração de dados usando um backup em nuvem híbrida

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.

Restaurar dados usando um backup de VMware

Você pode sincronizar os backups de máquinas virtuais de VMware locais para a nuvem e restaurar para servidores em nuvem usando os backups. Configure grupos de segurança antes da restauração. Caso contrário, a restauração pode falhar. Para obter detalhes, consulte **Restauração para servidores em nuvem usando backups de VMware**.

5.4 Restauração de dados usando um backup de arquivo

Você pode usar um backup de arquivo para restaurar os dados de um cliente de backup para o estado em um determinado momento em que foi feito backup dos dados.

Restrições

- O status do Agente do cliente de backup deve ser **Normal**.
- É aconselhável não restaurar backups de arquivos para aplicativos em execução. Pare os aplicativos e, em seguida, restaurar os arquivos.

Método 1

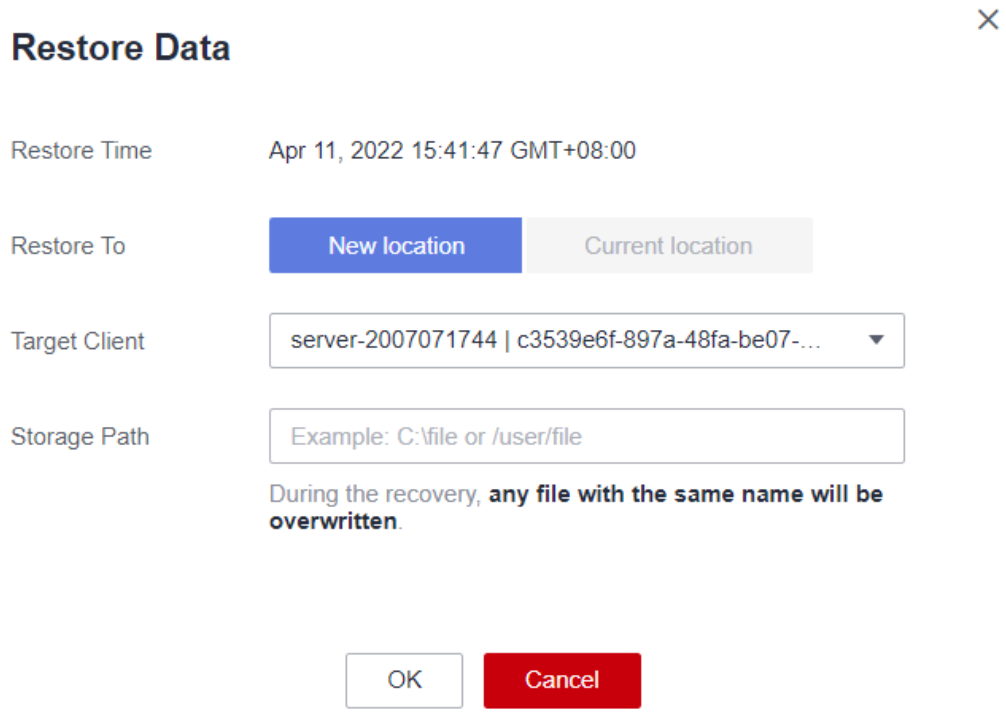
Passo 1 Faça logon no console do CBR.

1. Acesse o console de gerenciamento.
2. Clique em no canto superior esquerdo e selecione sua região e projeto.
3. Escolha **Storage** > **Cloud Backup and Recovery** > **File Backups**.

Passo 2 Na página de guia **File Backup**, clique no nome do cliente de backup de destino.

Passo 3 Encontre o backup desejado e clique em **Restore Data**.

Figura 5-4 Restaurar um arquivo



Passo 4 Selecione um local de restauração.

- **Current location**: os dados serão restaurados para o caminho do arquivo original no cliente de backup atual e qualquer arquivo com o mesmo nome será substituído. Essa opção está disponível apenas para clientes de backup de Linux.
- **New location**: os dados serão restaurados para um servidor diferente. Você pode selecionar um cliente de destino e especificar um caminho.

  Você só pode escolher entre os clientes de backup cujo status de agente é **Normal**. Se o servidor de destino não estiver na lista, vá para a lista de backup de arquivos e instale o Agente.

Passo 5 Clique em **OK**. Você pode verificar se os dados foram restaurados com êxito na área **Backup Details** da página de detalhes do cliente ou no host local.

Quando o status do backup é alterado para **Available**, a restauração é bem-sucedida.

----Fim

Método 2

Passo 1 Faça logon no console do CBR.

1. Acesse o console de gerenciamento.
2. Clique em no canto superior esquerdo e selecione sua região e projeto.
3. Escolha **Storage** > **Cloud Backup and Recovery** > **File Backups**.

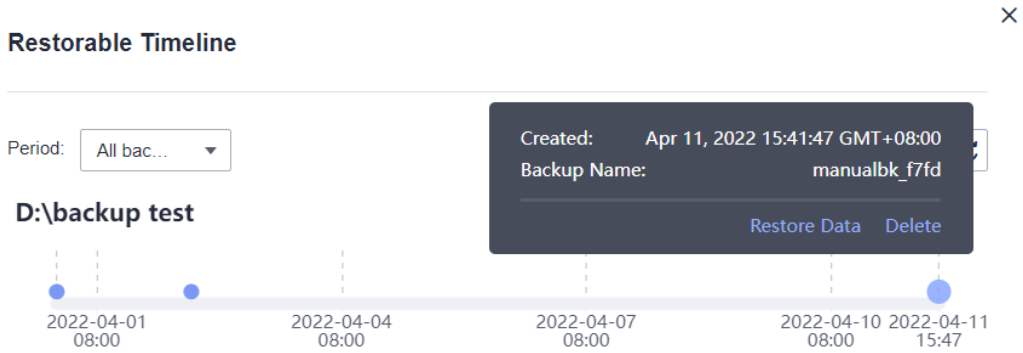
Passo 2 Na página de guia **File Backup**, clique no nome do cliente de backup de destino.

Passo 3 Clique em **Restorable Timeline** na coluna **Operation**.

Passo 4 Selecione um tempo de restauração e clique em **Restore Data**. Consulte **Figura 5-5**.

O sistema restaurará os dados para o estado no horário selecionado.

Figura 5-5 Linha do tempo restaurável



Passo 5 Selecione um local de restauração.

- **Current location**: os dados serão restaurados para o caminho do arquivo original no cliente de backup atual e qualquer arquivo com o mesmo nome será substituído.
- **New location**: os dados serão restaurados para um servidor diferente. Você pode selecionar um cliente de destino e especificar um caminho.

  Você só pode escolher entre os clientes de backup cujo status de agente é **Normal**. Se o servidor de destino não estiver na lista, vá para a lista de backup de arquivos e instale o Agente.

Passo 6 Clique em **OK**. Você pode verificar se os dados foram restaurados com êxito na área **Backup Details** da página de detalhes do cliente ou no host local.

Quando o status do backup é alterado para **Available**, a restauração é bem-sucedida.

----Fim

6 Backup consistente com a aplicação

6.1 O que é backup consistente com a aplicação?

Visão geral

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

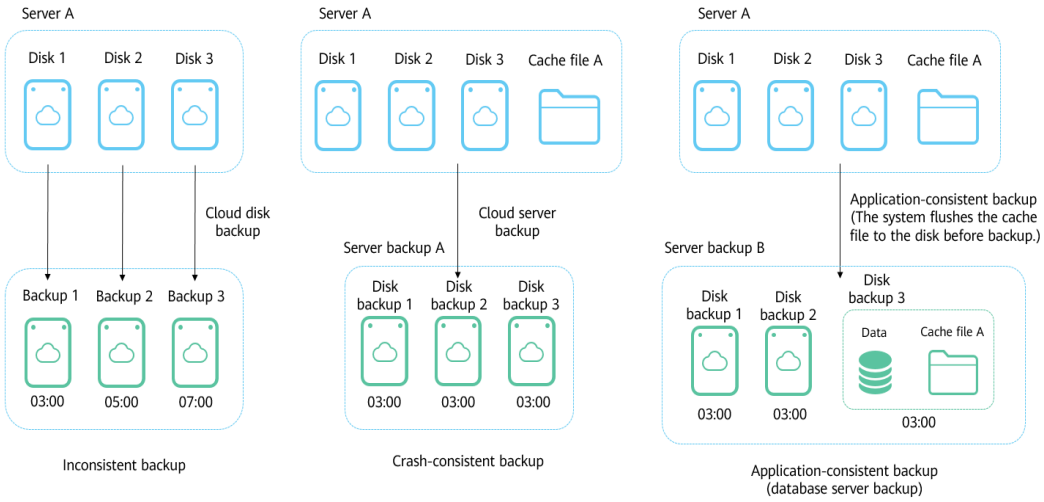
- Backup inconsistente: os arquivos em um backup inconsistente contêm dados obtidos de diferentes pontos no tempo. Isso geralmente ocorre se forem feitas alterações em seus arquivos ou nos dados em seus discos enquanto o backup está em execução. O backup do servidor em nuvem CBR usa a tecnologia de snapshot de consistência para discos para proteger dados de ECSs e BMSs. Se você fizer backup de vários discos do EVS separadamente, os pontos de tempo de backup dos discos do EVS serão diferentes. Como resultado, os dados de backup dos discos do EVS são inconsistentes.
- 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 aplicação. A consistência de backup dos sistemas de aplicação 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.

Figura 6-1 compara esses tipos de backup em detalhes.

O CBR suporta backup consistente com falhas e backup consistente com a aplicação (também chamado de backup do servidor de banco de dados).

Se um banco de dados MySQL ou SAP HANA for implantado em um servidor, você poderá usar o backup consistente com a aplicação CBR para fazer backup dos dados do servidor e do cache da aplicação. O backup consistente com falhas faz backup apenas de dados e alguns caches de aplicativos sem interromper os serviços. Se um sistema falhar ou ocorrer perda de dados, você pode usar um backup consistente com a aplicação para reiniciar rapidamente os serviços. Um backup consistente com falhas, no entanto, pode falhar ao restaurar algumas configurações de aplicativos.

Figura 6-1 Consistência de backup



Diferenças entre backup consistente com a aplicação backup de servidor em nuvem

Item	Backup consistente com a aplicação	Backup de servidor em nuvem
Objeto de backup e restauração	Servidores em nuvem com banco de dados MySQL ou SAP HANA implantados	Servidores em nuvem excluindo aplicativos de banco de dados
Unidade de backup	Servidor em nuvem	Servidor em nuvem
Tipo de cofre	Cofre de backup de servidor	Cofre de backup de servidor
Cenário recomendado	Os dados dos servidores em nuvem, bem como seus bancos de dados implantados, como o banco de dados MySQL ou SAP HANA, precisam ser copiados. Todos os dados e configurações de aplicativos precisam ser restaurados em caso de erro.	Apenas os dados dos servidores em nuvem precisam ser copiados. Todos os dados precisam ser restaurados em caso de erro. No caso de um backup de servidor em nuvem ser realizado para um servidor implantado com um banco de dados MySQL ou SAP HANA, se o backup for usado para restaurar dados, algumas configurações de banco de dados podem falhar ao serem restauradas e podem ocorrer problemas após o banco de dados ser reiniciado.

Escopo da aplicação

Tabela 6-1 lista os SOs que suportam a instalação do Agente.

Tabela 6-1 SOs que suportam a instalação do Agente

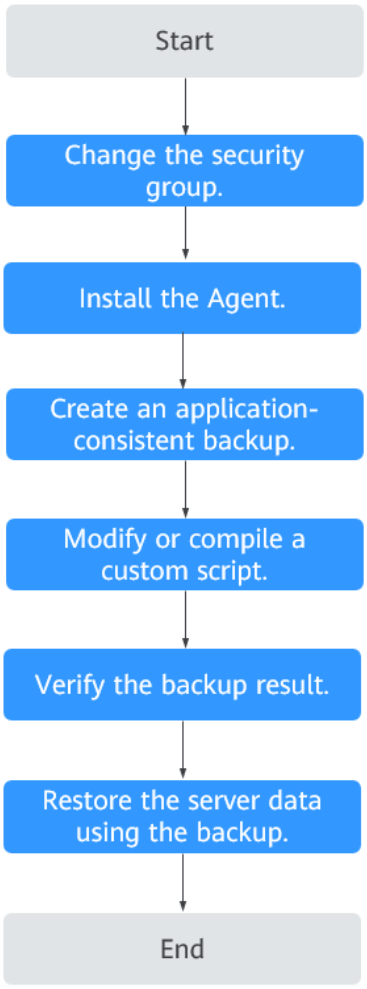
Banco de dados	SO	Versão
SQL Server 2008/2012	Windows	Windows Server 2008, 2008 R2, 2012, 2012 R2 for x86_64
SQL Server 2014/2016/EE	Windows	Windows Server 2014, 2014 R2, 2016 Datacenter for x86_64
MySQL 5.5/5.6/5.7	Red Hat	Red Hat Enterprise Linux 6, 7 for x86_64
	SUSE	SUSE Linux Enterprise Server 11,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

Para os bancos de dados não incluídos nesta lista, você pode personalizar um script para executar backup consistente com a aplicação consultando a seção "Implementação de backup consistente com a aplicação usando um script personalizado" nas *Práticas recomendadas de backup e recuperação em nuvem*.

Processo

Figura 6-2 mostra o processo de backup consistente com a aplicação.

Figura 6-2 Processo de backup consistente com a aplicação



Passo 1 Altere o grupo de segurança: antes de executar uma tarefa de backup consistente com a aplicação, altere o grupo de segurança do servidor que você deseja fazer backup. Para mais detalhes, consulte **Alteração de um grupo de segurança**.

Passo 2 Instale o Agente: altere o grupo de segurança e instale o agente em qualquer sequência. Certifique-se de que as duas operações sejam concluídas antes de fazer o backup do servidor desejado. Para mais detalhes, consulte **Instalação do Agente**.

Passo 3 Crie backups consistentes com a aplicação: depois de criar um cofre de backup do servidor para armazenar backups consistentes com a aplicação, associe-o ao servidor de banco de dados desejado e crie um backup consistente com a aplicação. Para mais detalhes, consulte **Criação de um backup consistente com a aplicação**.

Passo 4 Modifique ou compile um script personalizado: após fazer backup de um servidor de banco de dados no console do CBR, modifique ou compile um script personalizado no banco de dados do servidor. Para obter detalhes, consulte **UImplementação de um backup consistente com a aplicação usando um script personalizado**.

Passo 5 Verifique o resultado do backup: depois que o backup é executado, verifique se o backup é bem-sucedido. Para obter detalhes, consulte **Verificação de resultado do backup consistente com a aplicação**.

Passo 6 Use o backup para restaurar os dados do servidor: use o backup consistente com a aplicação para restaurar os dados do servidor. Os aplicativos e dados de banco de dados restaurados são os mesmos que no ponto de backup no tempo. Para mais detalhes, consulte **Restauração de dados usando o Cloud Server Backup**.

----Fim

6.2 Alteração de um grupo de segurança

Contexto

Um grupo de segurança é uma coleção de regras de controle de acesso para ECSs que têm os mesmos requisitos de proteção de segurança e são mutuamente confiáveis em uma VPC Depois da criação de um grupo de segurança, você pode criar diferentes regras de acesso para o grupo de segurança com o intuito de proteger os ECSs adicionados a esse grupo de segurança. A regra de grupo de segurança padrão permite todos os pacotes de dados de saída. Os ECSs em um grupo de segurança podem acessar uns aos outros sem a necessidade de adicionar regras. O sistema cria um grupo de segurança para cada conta de nuvem por padrão. Você também pode criar grupos de segurança personalizados por conta própria.

Ao criar um grupo de segurança, você deve adicionar as regras de acesso de entrada e saída e habilitar as portas necessárias para o backup consistente com aplicativo para evitar falhas de backup consistentes com aplicativo.

Instruções de operação

Antes de usar a função de backup consistente com o aplicativo, você precisa alterar o grupo de segurança. Para garantir a segurança da rede, o CBR não definiu a direção de entrada de um grupo de segurança, portanto, é necessário configurá-lo manualmente.

Na direção de saída do grupo de segurança, as portas 1 a 65535 no segmento de rede 100.125.0.0/16 devem ser configuradas. Na direção de entrada, as portas 59526 a 59528 no segmento de rede 100.125.0.0/16 devem ser configuradas. A regra de saída padrão é 0.0.0.0/0, ou seja, todos os pacotes de dados são permitidos. Se a regra padrão na direção de saída não for modificada, não será necessário configurar a direção de saída.

Procedimento

Passo 1 Efetue logon no console do ECS.

1. Acesse o console de gerenciamento.
2. Clique em  no canto superior esquerdo e selecione sua região e projeto.
3. Sob **Computing**, clique em **Elastic Cloud Server**.

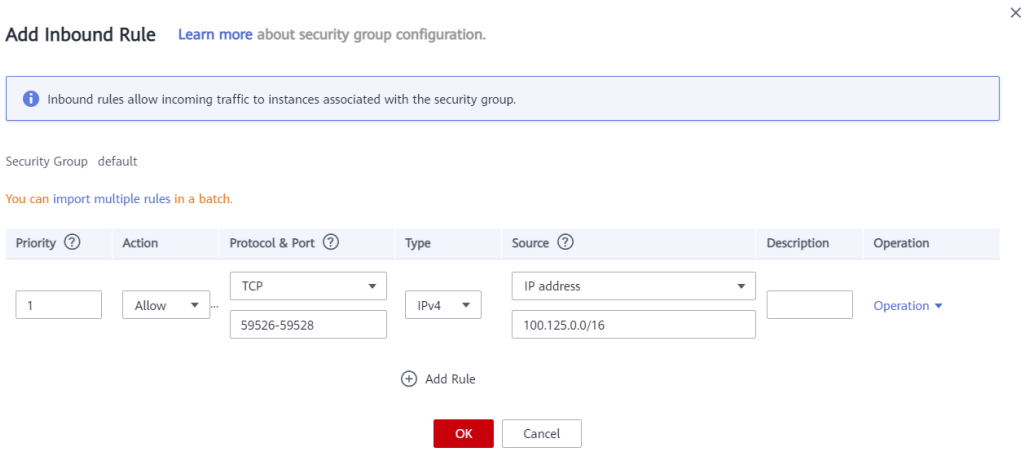
Passo 2 No painel de navegação à esquerda, escolha **Elastic Cloud Server** ou **Bare Metal Server**. Na página exibida, selecione o servidor de destino. Vá para a página de detalhes do servidor.

Passo 3 Clique na guia **Security Groups** e selecione o grupo de segurança de destino. À direita da página ECS, clique em **Modify Security Group Rule** para um ECS. Clinque em **Alterar grupo de segurança** para um BMS. Na caixa de diálogo exibida, clique em **Manage Security Group**.

Passo 4 Na página **Security Groups**, clique na guia **Inbound Rules** e, em seguida, clique em **Add Rule**. A caixa de diálogo **Add Inbound Rule** é exibida, conforme mostrado na **Figura 6-3**.

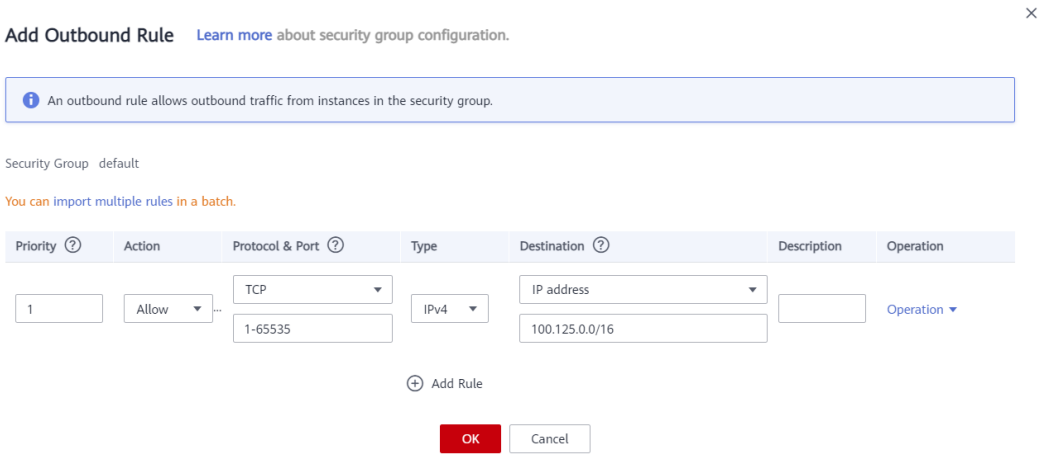
Selecione **TCP** para **Protocol/Application**, digite **59526-59528** em **Port & Source**, selecione **IP address** para **Source** e digite **100.125.0.0/16**. Depois de complementar a descrição, clique em **OK** para concluir a configuração da regra de entrada.

Figura 6-3 Adicionar uma regra de entrada



Passo 5 Clique na guia **Outbound Rules** e, em seguida, clique em **Add Rule**. A caixa de diálogo **Add Outbound Rule** é exibida, como mostrado na **Figura 6-4**. Selecione **TCP** para **Protocol/Application**, insira **1-65535** em **Port & Source**, selecione **IP address** para **Destination** e digite **100.125.0.0/16**. Depois de complementar a descrição, clique em **OK** para concluir a configuração da regra de saída.

Figura 6-4 Adicionar uma regra de saída



----Fim

6.3 Instalação do Agente

Antes de habilitar o backup consistente com a aplicação, altere o grupo de segurança e instale o Agente nos ECSs com êxito.

Se o backup consistente com a aplicação estiver ativado, mas o Agente não estiver instalado nos servidores, o backup consistente com a aplicação falhará e, em vez disso, será realizado

um backup comum do servidor. Para garantir que o backup consistente com a aplicação seja executado corretamente, baixe e instale o Agente primeiro.

Instruções de operação

- O backup consistente com a aplicação suporta apenas ECSs baseados em x86, não ECSs baseados em Kunpeng.
- Durante a instalação do Agente, o sistema requer as permissões do usuário **rdadmin** para executar o programa de instalação. Para melhorar a segurança de O&M, altere a senha do usuário **rdadmin** do SO do Agente regularmente e desative a permissão de logon remoto desse usuário. Para mais detalhes, consulte **Alteração da senha do usuário rdadmin**.
- **Tabela 6-2** lista SOs que suportam a instalação do Agente.

Tabela 6-2 SOs que suportam a instalação do Agente

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

AVISO

Para instalar o Agente, o sistema abrirá o firewall de uma porta de 59526 a 59528 do ECS. Quando a porta 59526 está ocupada, o firewall da porta 59527 está habilitado, e assim por diante.

Pré-requisitos

- Você obteve um nome de usuário e sua senha para fazer logon no console de gerenciamento.
- O grupo de segurança foi configurado.
- O **Agent Status** do ECS não está **Not installed**.
- Se você usar o Internet Explorer, precisará de adicionar os sites que usará a sites confiáveis.

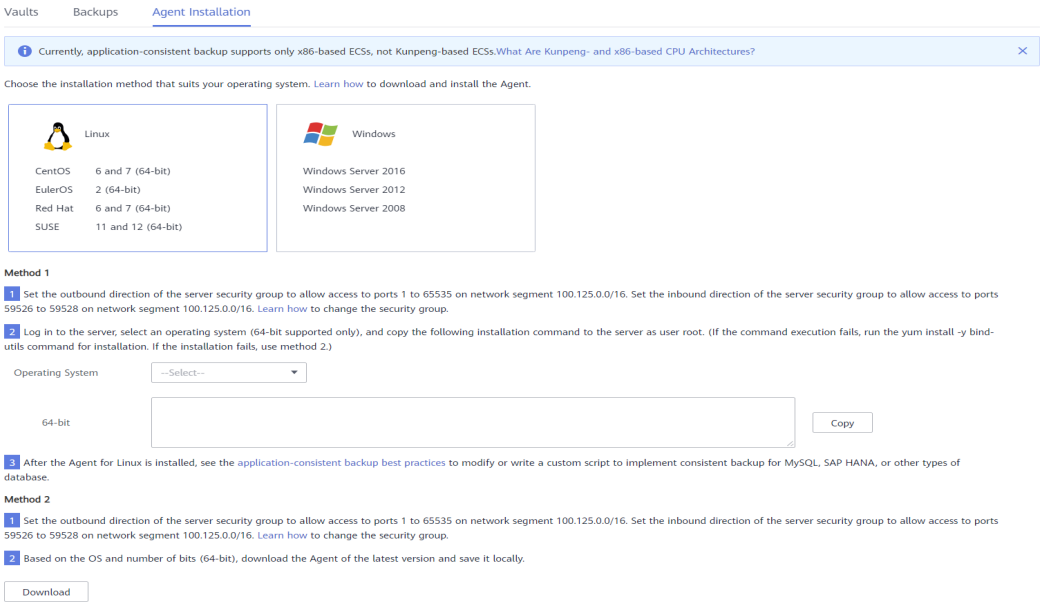
Instalar o Agente para um sistema operacional Linux (Método 1)

Passo 1 Faça logon no console de CBR.

1. **Efetue logon no console de gerenciamento**.
2. Clique em no canto superior esquerdo e selecione sua região e projeto.
3. Escolha **Storage** > **Cloud Backup and Recovery**. Selecione uma guia de backup no painel de navegação esquerdo.

Passo 2 Clique na guia **Agent Installation**.

Figura 6-5 Página de instalação para Linux



Passo 3 No método 1, selecione a versão do Agente correspondente conforme necessário e copie o comando de instalação na etapa 2.

Passo 4 Na página ECS, selecione o servidor de destino e clique em **Remote login** na coluna **Operation** para efetuar logon no ECS.

Passo 5 Cole o comando de instalação na etapa 2 no servidor e execute o comando como usuário **root**. Se a execução falhar, execute o comando **yum install -y bind-utils** para instalar o módulo dig. Se a instalação ainda falhar, use o método 2 para instalar o Agente para um sistema operacional Linux.

Passo 6 Após a conclusão da instalação, o Agente está sendo executado corretamente. Para implementar backup consistente com a aplicações para MySQL, SAP HANA ou outros tipos de bancos de dados, modifique ou compile um script personalizado consultando *Práticas recomendadas de backup e recuperação em nuvem*.

----Fim

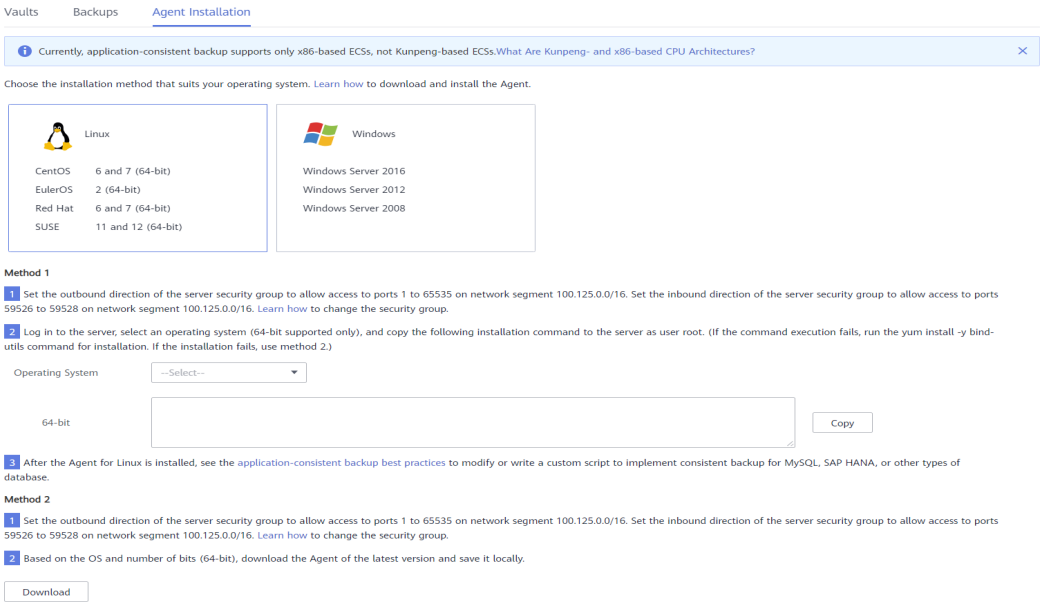
Instalar o Agente para um sistema operacional Linux (Método 2)

Passo 1 Faça logon no console de CBR.

1. **Efetue logon no console de gerenciamento**.
2. Clique em no canto superior esquerdo e selecione sua região e projeto.
3. Escolha **Storage** > **Cloud Backup and Recovery**. Selecione uma guia de backup no painel de navegação esquerdo.

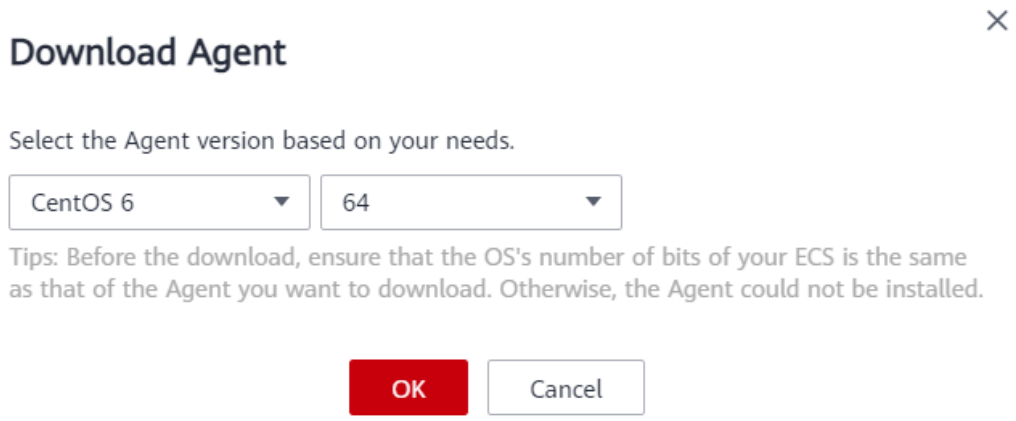
Passo 2 Clique na guia **Agent Installation**.

Figura 6-6 Página de instalação para Linux



Passo 3 No método 2, clique em **Download**. Na caixa de diálogo do cliente de download exibida, selecione a versão a ser baixada com base no tipo de sistema operacional do ECS de destino e clique em **OK**. Veja **Figura 6-7**.

Figura 6-7 Baixar o Agente



Passo 4 Após fazer o download do Agente, use uma ferramenta de transferência de arquivos, como Xftp, SecureFX ou WinSCP, para fazer upload do pacote de instalação do Agente para o ECS.

Passo 5 Após o upload, acesse a página ECS. Selecione o servidor de destino e clique em **Remote login** na coluna **Operation** para efetuar logon no ECS.

Passo 6 Execute o comando **tar -zxvf** para descompactar o pacote de instalação do Agente em qualquer diretório e execute o seguinte comando para ir para o diretório **bin**:

cd bin

Passo 7 Execute o seguinte comando para executar o script de instalação:

sh agent_install_ebk.sh

Passo 8 O sistema exibe uma mensagem indicando que o cliente foi instalado com êxito. Veja **Figura 6-8**.

Figura 6-8 Instalação bem-sucedida do cliente para Linux

Passo 9 Se o banco de dados MySQL ou SAP HANA tiver sido instalado no ECS, execute o seguinte comando para criptografar a senha para efetuar logon no banco de dados MySQL ou SAP HANA:

/home/rdadmin/Agent/bin/agentcli encpwd

Passo 10 Use a senha criptografada em **previous step** para substituir a senha de logon do banco de dados no script em **/home/rdadmin/Agent/bin/thirdparty/ebk_user/**.

Passo 11 Após a conclusão da instalação, o Agente está sendo executado corretamente. Para implementar backup consistente com a aplicações para MySQL, SAP HANA ou outros tipos de bancos de dados, modifique ou compile um script personalizado consultando *Práticas recomendadas de backup e recuperação em nuvem*.

----Fim

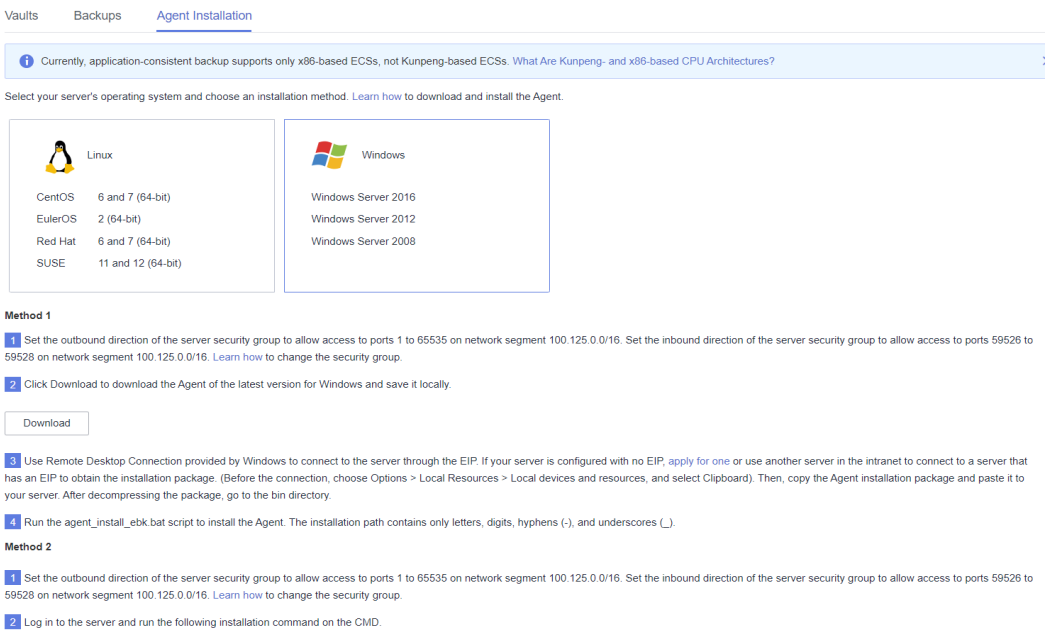
Instalar o Agente para um sistema operacional Windows (Método 1)

Passo 1 Faça logon no console de CBR.

1. **Efetue logon no console de gerenciamento**.
2. Clique em no canto superior esquerdo e selecione sua região e projeto.
3. Escolha **Storage** > **Cloud Backup and Recovery**. Selecione uma guia de backup no painel de navegação esquerdo.

Passo 2 Clique na guia **Agent Installation**.

Figura 6-9 Página de instalação para Windows



Passo 3 No método 1, clique em **Download**. Salve o pacote de instalação baixado em um diretório local.

Passo 4 Após fazer o download do Agente, use uma ferramenta de transferência de arquivos, como Xftp, SecureFX ou WinSCP, para fazer upload do pacote de instalação do Agente para o ECS.

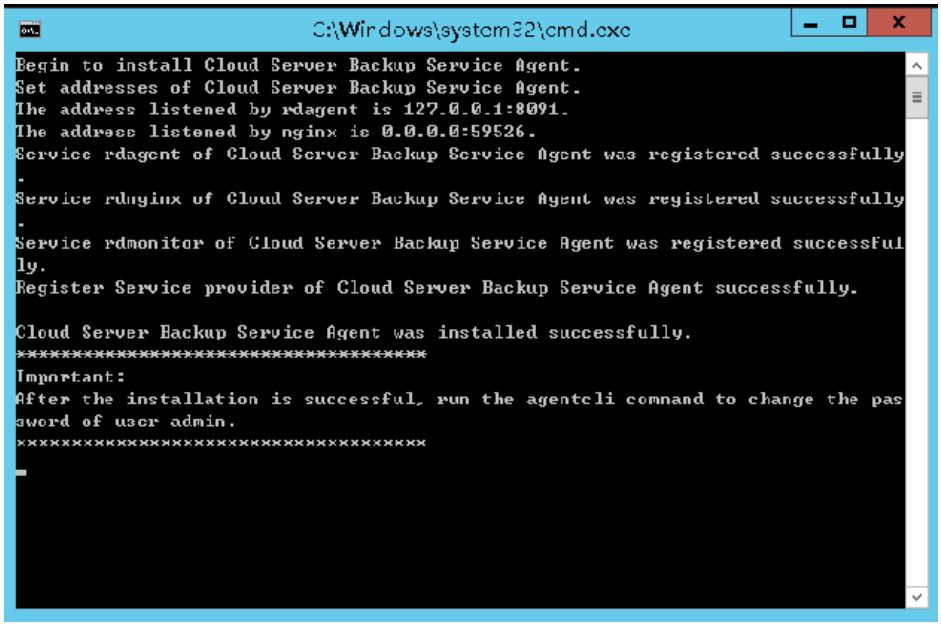
Passo 5 Faça logon no console e, em seguida, faça logon no ECS como administrador.

Passo 6 Descompacte o pacote de instalação em qualquer diretório e vá para o diretório *Installation path***bin**.

Passo 7 Clique duas vezes no script **agent_install_ebk.bat** para iniciar a instalação.

Passo 8 O sistema exibe uma mensagem indicando que o cliente foi instalado com êxito. Consulte **Figura 6-10**.

Figura 6-10 Instalação bem-sucedida do cliente para Windows



----Fim

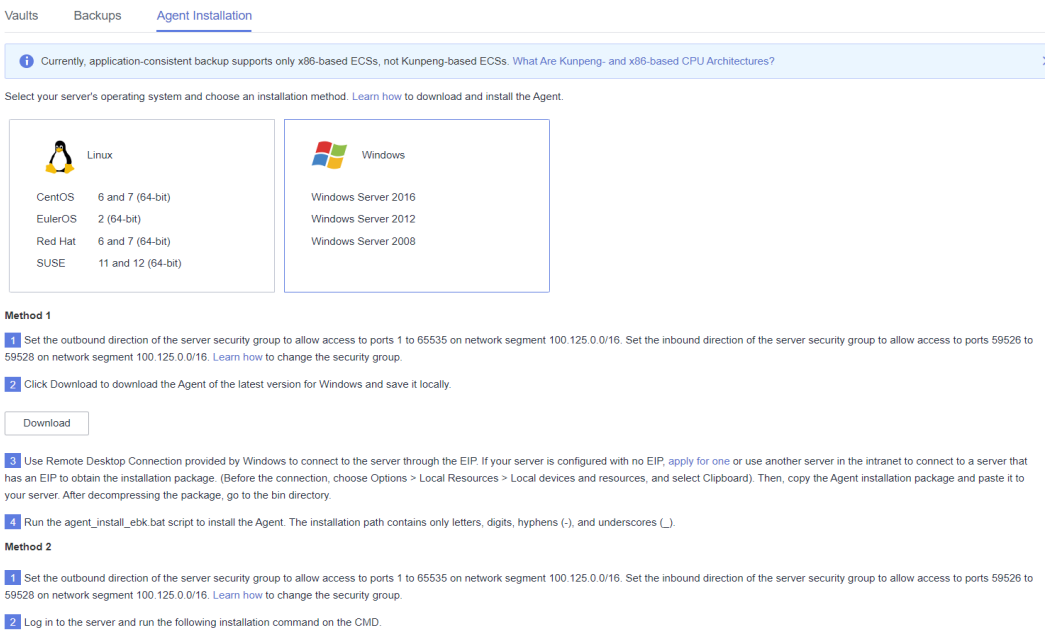
Instalar o Agente para um sistema operacional Windows (Método 2)

Passo 1 Faça logon no console de CBR.

1. **Efetue logon no console de gerenciamento**.
2. Clique em no canto superior esquerdo e selecione sua região e projeto.
3. Escolha **Storage** > **Cloud Backup and Recovery**. Selecione uma guia de backup no painel de navegação esquerdo.

Passo 2 Clique na guia **Agent Installation**.

Figura 6-11 Página de instalação para Windows



Passo 3 Na página ECS, selecione o servidor de destino e clique em **Remote login** na coluna **Operation** para efetuar logon no ECS como administrador.

Passo 4 Copie os comandos de instalação na etapa 2 do método 2 para o servidor e execute o comando no prompt de comando.

Passo 5 Copie qualquer endereço IP no nome da resposta, cole-o na caixa de endereço do navegador e substitua **0.0.0.0** no seguinte endereço pelo endereço. Substitua ***ap-southeast-1*** pela região real. O comando a seguir usa ***ap-southeast-1*** como exemplo. Em seguida, pressione **Enter** no navegador para baixar o pacote de instalação.

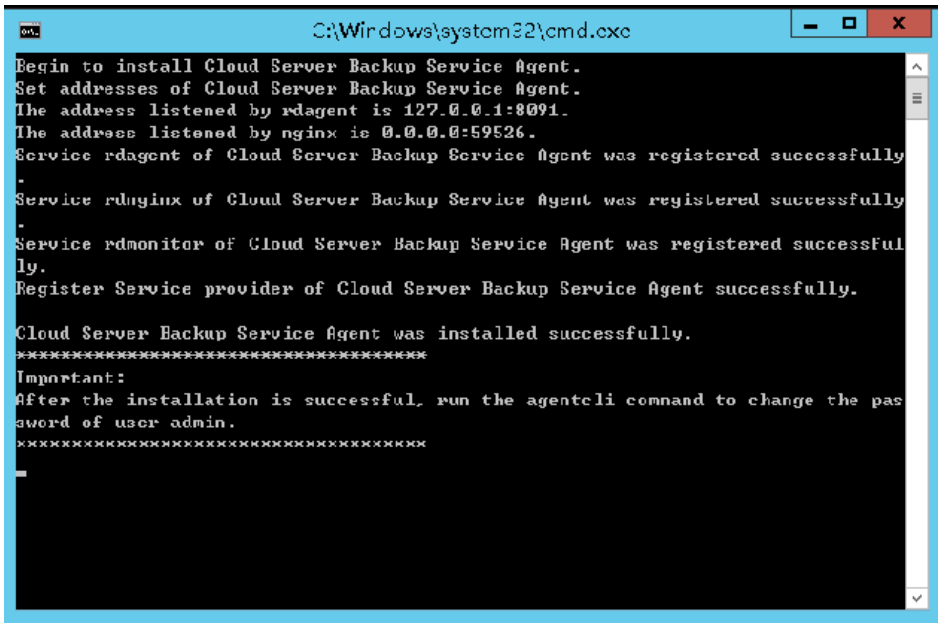
http://*0.0.0.0*/csbs-agent-*ap-southeast-1*/Cloud Server Backup Agent-WIN64.zip

Passo 6 Descompacte o arquivo para obter o arquivo de instalação. Descompacte o pacote de instalação em qualquer diretório e vá para o diretório *Installation path***bin**.

Passo 7 Clique duas vezes no script **agent_install_ebk.bat** para iniciar a instalação.

Passo 8 O sistema exibe uma mensagem indicando que o cliente foi instalado com êxito. Consulte **Figura 6-12**.

Figura 6-12 Instalação bem-sucedida do cliente para Windows



----Fim

6.4 Criação de um backup consistente com a aplicação

O CBR suporta backup consistente com a aplicação, além de backup consistente com falhas. O backup consistente com a aplicação garante a consistência dos dados da aplicação 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.

Restrições

- No momento, o backup consistente com a aplicação não é suportado para aplicações de cluster, como o MySQL Cluster. Ele é suportado apenas para aplicações em servidores autônomos.
- Você é aconselhado a executar backup consistente com a aplicação em horários fora de pico.

Procedimento

Passo 1 Faça logon no console de CBR.

1. **Efetue logon no console de gerenciamento**.
2. Clique em no canto superior esquerdo e selecione sua região e projeto.
3. Escolha **Storage** > **Cloud Backup and Recovery**. Selecione uma guia de backup no painel de navegação esquerdo.

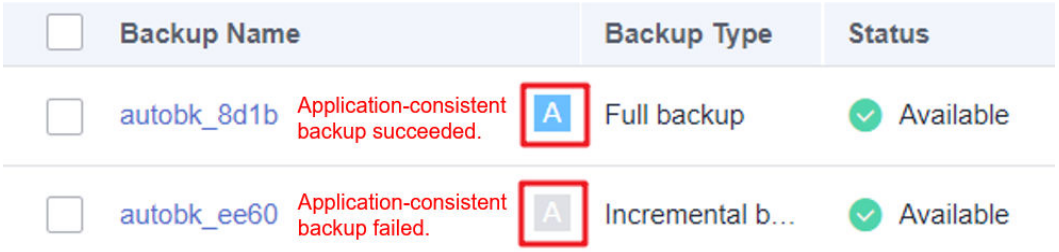
Passo 2 Crie um cofre para backups consistentes com a aplicação, consulte **Compra de um cofre de backup de servidor**. Selecione **Enable** para **Application-Consistent Backup**.

Passo 3 Associe os servidores de nuvem ao cofre criado. Verifique se o Agente foi instalado nos servidores.

Passo 4 Crie um backup do servidor em nuvem **Criação do Cloud Server Backup**.

- Se um backup consistente com a aplicação for criado com êxito, uma letra azul "A" será exibida ao lado do nome do backup na lista de backup.
- Se um backup consistente com a aplicação falhar ao ser criado, o sistema criará automaticamente um backup do servidor em nuvem e armazenará o backup no cofre, e uma letra cinza "A" será exibida ao lado do nome do backup na lista de backup. Você pode visualizar a causa da falha na área **Management Information** na página de detalhes do backup. Veja **Figura 6-13**.

Figura 6-13 Status do backup consistente com a aplicação



Passo 5 Volte para a página de backup do servidor de nuvem conforme solicitado. Se a execução do backup falhar, corrija a falha com base nos detalhes da falha mostrados na página.

----Fim

Procedimento de acompanhamento

Se os dados forem perdidos devido a ataques de vírus ou falhas de banco de dados, você poderá restaurar os dados seguindo as instruções em **Restauração de dados usando o Cloud Server Backup** e **Criação de uma imagem usando um backup**.

6.5 Desinstalação do Agente

Cenários

Esta seção descreve como desinstalar o Agente quando o backup consistente com o aplicativo não é mais necessário.

Pré-requisitos

O nome de usuário e a senha para efetuar logon em um ECS foram obtidos.

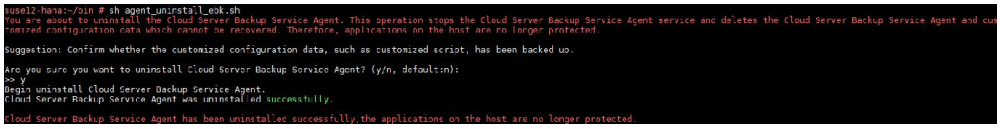
Desinstalar o agente para Linux

Passo 1 Faça logon no ECS e execute o comando **su -root** para alternar para o usuário **root**.

Passo 2 No diretório **home/rdadmin/Agent/bin**, execute o seguinte comando para desinstalar o Agente. **Figura 6-14** exibe um exemplo. Se a palavra **successfully** em verde for exibida, o Agente será desinstalado com êxito.

sh agent_uninstall_ebk.sh

Figura 6-14 Agente desinstalado com sucesso do Linux



----Fim

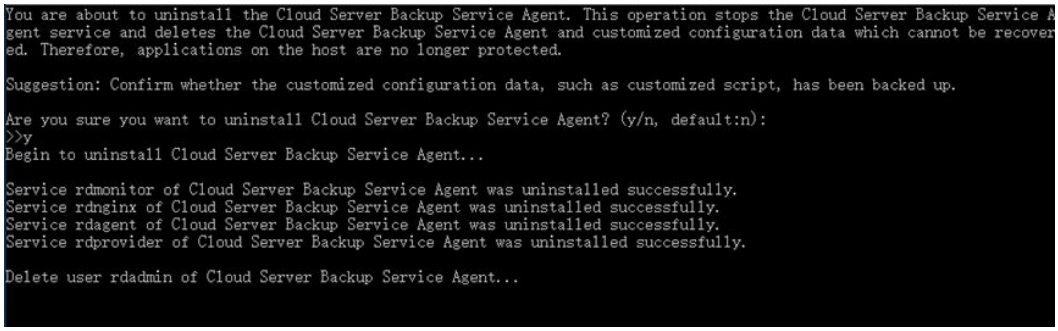
Desinstalar o Agente para Windows

Passo 1 Efetue logon no ECS.

Passo 2 No diretório *Installation path*/**bin**, clique duas vezes em **agent_uninstall_ebk.bat**. A janela para desinstalar o Agente é exibida.

Depois que a desinstalação for concluída e bem-sucedida, a janela será fechada automaticamente. Consulte **Figura 6-15**.

Figura 6-15 Agente desinstalado com sucesso do Windows



----Fim

7 Backup de arquivos

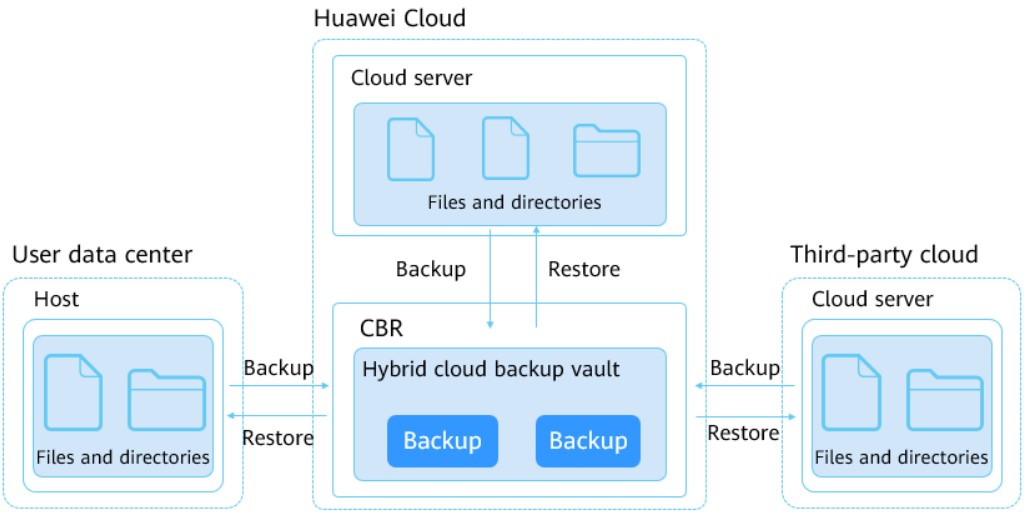
7.1 O que é backup de arquivos?

Visão geral do backup de arquivos

O CBR fornece backup de arquivos que permite fazer backup de arquivos e diretórios em seus servidores em nuvem e hosts locais, para que você não precise fazer backup de seus servidores ou discos inteiros. Os servidores em nuvem podem ser servidores da Huawei Cloud ou seus homólogos de uma nuvem de terceiros. Se ocorrer uma exclusão acidental ou uma falha de software/hardware em seus arquivos, você poderá restaurar os dados a qualquer momento no passado, quando um backup foi gerado.

Figura 7-1 mostra a arquitetura de backup do arquivo.

Figura 7-1 Arquitetura de backup de arquivos



Escopo de backup de arquivos

Tabela 7-1 lista os sistemas operativos suportados para os hosts no local.

Tabela 7-1 Sistemas operacionais que suportam backup de arquivos

Sistema operacional	Versão suportada
Servidor Windows	Windows Server 2019 for x86_64 Windows Server 2016 for x86_64 Windows Server 2012 for x86_64
Windows	Windows 10 Windows 7
CentOS	CentOS 7
EulerOS	Euler OS 2.5

NOTA

Se você estiver executando o Windows Server 2019, Windows Server 2012 ou Windows 7, uma mensagem indicando que MSVCR100.dll está ausente será retornada durante a instalação do Agente. Nesse caso, corrija o problema consultando **Atualização de segurança do MFC** e reinstale o Agente.

Diferenças entre o backup do SFS Turbo e o backup de arquivos

Item	Backup do SFS Turbo	Backup de arquivos
Objeto de backup e restauração	Sistema de arquivos do SFS Turbo	Um único ou vários arquivos de servidores em nuvem e hosts locais
Unidade de backup	Sistema de arquivos do SFS Turbo	Arquivo
Tipo de cofre	Cofres de backup do SFS Turbo	Cofre de backup em nuvem híbrida
Cenário recomendado	Os dados nos sistemas de arquivos do SFS Turbo precisam de ser protegidos. Os dados de backup não são armazenados no sistema de arquivos e podem ser usados para criar novos sistemas de arquivos quando necessário.	Os dados em um único ou vários arquivos em servidores em nuvem e hosts locais precisam ser protegidos, e os dados podem ser rapidamente armazenados em backup e restaurados na nuvem.

Restrições de backup de arquivos

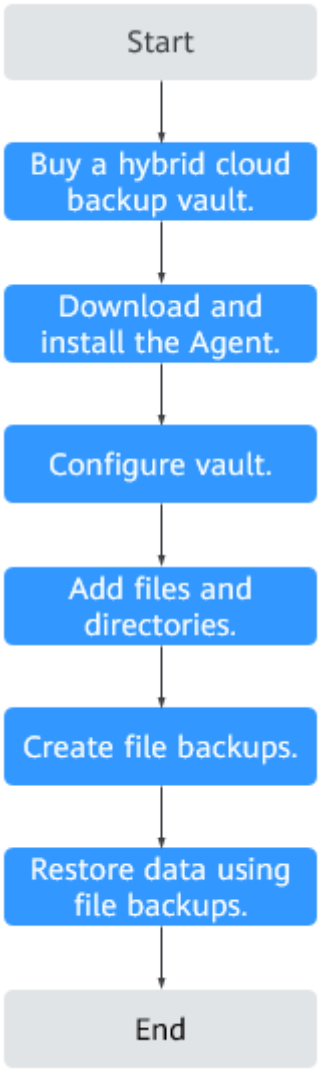
- Durante o backup de arquivos, se um arquivo estiver sendo alterado por uma aplicação e o cliente de backup tiver a permissão de leitura desse arquivo, os dados do backup ficarão incompletos. É aconselhável primeiro parar a aplicação e, em seguida, executar backup para garantir a integridade dos dados.
- 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 aplicações em execução. Pare as aplicações 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 arquivos 500.000.
- Um caminho pode conter no máximo 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.

7.2 Processo de backup de arquivos

Figura 7-2 mostra o processo de backup do arquivo.

Figura 7-2 Processo de backup de arquivos



1. Criar um cofre de backup em nuvem híbrida

   Antes de instalar o Agente de backup do arquivo, crie um cofre consultando **Criação de um cofre de backup em nuvem híbrida**. O cofre criado será usado para armazenar backups de arquivos gerados.

2. Baixar e instalar o Agente

   Instalar o Agente nos servidores de destino consultando **Download e instalação do Agente**. Depois que o Agente é instalado com êxito, os servidores aparecem automaticamente como clientes de backup na lista de backup de arquivos.

3. Configurar o cofre

   Configurar o cofre para os clientes de backup consultando **Configuração de cofre**. Os backups de arquivos gerados serão armazenados no cofre configurado.

4. Adicionar arquivos e diretórios.

   Adicionar os arquivos e diretórios que você deseja fazer backup consultando **Adição de diretórios**.

5. Criar backups de arquivos.

   Executar backups manualmente consultando **Criação de backups de arquivos** ou faça com que o sistema crie backups automaticamente. Os backups gerados serão armazenados no cofre.

6. Restaurar dados usando backups de arquivos.

   Restaurar dados consultando **Restauração de dados usando um backup de arquivo**. Você pode restaurar dados para servidores de origem ou servidores diferentes.

7.3 Criação de um cofre de backup em nuvem híbrida

Esta seção descreve como comprar um cofre de backup em nuvem híbrida para armazenar backups de arquivos.

Procedimento

Passo 1 Faça logon no console do CBR.

1. Acesse o console de gerenciamento.
2. Clique em no canto superior esquerdo e selecione sua região e projeto.
3. Escolha **Storage** > **Cloud Backup and Recovery** > **File Backups**.

Passo 2 No canto superior direito da página, clique em **Buy Hybrid Cloud Backup Vault**.

Passo 3 Selecione um 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 pagamento por uso é modo de cobrança 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.

Passo 4 Especifique a capacidade do cofre, que varia de 1 a 10240 TB.

É necessário planejar corretamente a capacidade do cofre, que deve ser pelo menos igual ao tamanho dos arquivos que deseja fazer backup. Verifique o tamanho do arquivo em seus hosts locais. À medida que o espaço usado do cofre cresce, é possível expandir a capacidade do cofre se ele se tornar insuficiente.

Passo 5 Determine se deve configurar o backup automático.

- Se você selecionar **Configure**, deverá selecionar uma política de backup existente ou criar uma nova política. Depois que o cofre for criado, o sistema aplicará a política a este cofre e todos os arquivos associados a este cofre serão automaticamente copiados com base nesta política.
- Se você selecionar **Skip**, os arquivos associados a este cofre não serão automaticamente copiados até que você aplique uma política de backup a ele.

Passo 6 (Opcional) Adicione tags ao cofre.

Uma tag é representada na forma de um par chave-valor. As tags são usadas para identificar, classificar e pesquisar por cofres. Os identificadores do cofre são utilizados somente para filtrar e gerenciar cofres. Um cofre pode ter no máximo 10 tags.

Tabela 7-2 descreve os parâmetros de uma tag.

Tabela 7-2 Descrição do parâmetro de tag

Parâmetro	Descrição	Valor de exemplo
Chave	Cada tag tem uma chave única. Você pode personalizar a chave ou selecionar a chave de uma tag existente criada no TMS. Uma chave de marcação: ● Pode conter de 1 a 36 caracteres Unicode. ● Pode conter apenas letras, dígitos, hífenes (-) e sublinhados (_).	Key_0001
Valor	Um valor de tag pode ser repetitivo ou deixado em branco. Um valor de tag: ● Pode conter de 0 a 43 caracteres Unicode. ● Pode conter apenas letras, dígitos, hífenes (-) e sublinhados (_).	Value_0001

Passo 7 Especifique um nome para o cofre.

Um nome deve conter de 1 a 64 caracteres, incluindo dígitos, letras, sublinhado (_) ou hífenes (-), por exemplo, **vault-f61e**.

NOTA

Você pode usar o nome padrão, que está no formato de **vault**_*xxxx*.

Passo 8 Especifique a duração necessária se você selecionar cobrança anual/mensal. O prazo de validade varia de 1 mês a 5 anos.

Determine se a renovação automática deve ser ativada. Se você selecionar **Auto Renewal**:

- sua assinatura será renovada a cada mês para cobrança mensal.
- sua assinatura será renovada a cada ano para cobrança anual.

Passo 9 Pague pelo pedido como solicitado.

Passo 10 Volte para a página **File Backups** e visualize o cofre criado na lista do cofre.

----Fim

7.4 Download e instalação do Agente

Cenários

Antes de fazer backup dos arquivos, você precisa alterar o grupo de segurança dos servidores ou das máquinas virtuais de destino e instalar o Agente neles. Esta seção descreve como fazer download e instalar o Agente.

Atualmente, apenas os hosts que executam sistemas operacionais de 64 bits são suportados.

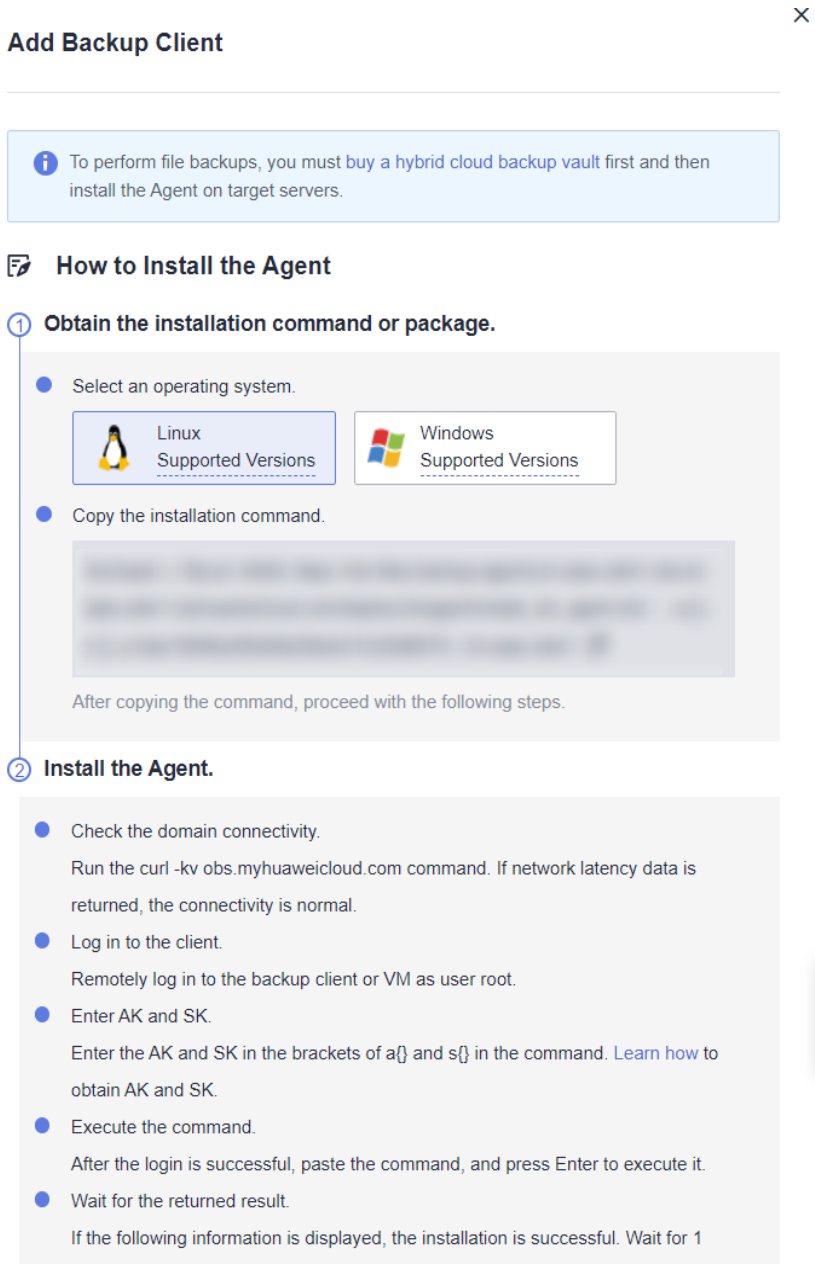
Instalar o Agente em um servidor de Linux

Passo 1 Faça logon no console do CBR.

1. Acesse o console de gerenciamento.
2. Clique em no canto superior esquerdo e selecione sua região e projeto.
3. Escolha **Storage** > **Cloud Backup and Recovery** > **File Backups**.

Passo 2 Clique em **Add Backup Client**. Na página exibida, selecione o sistema operacional Linux.

Figura 7-3 Linux



Passo 3 Efetue logon no host de destino como usuário **root**.

Passo 4 No host, execute o comando **curl -kv obs.myhuaweicloud.com**. Se os dados de latência da rede forem retornados, a conectividade é normal.

Passo 5 Conclua o comando de instalação fornecido no console do CBR inserindo AK e SK entre colchetes de **a {}** e **s {}** no comando. **Como obter uma AK/SK?**

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

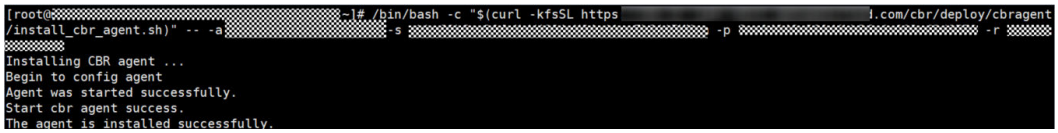
NOTA

Exclua os colchetes depois de inserir a AK e a SK.

Passo 6 Execute o comando obtido no host para instalar o Agente.

Passo 7 Se forem exibidas informações semelhantes às seguintes, o Agente foi instalado com êxito.

Figura 7-4 Executando o comando de instalação



Passo 8 Aguarde cerca de 1 minuto e visualize o cliente de backup na lista de backup de arquivos. Se o status do Agente for **Normal**, o sistema detecta com êxito o cliente e o Agente está sendo executado corretamente.

----Fim

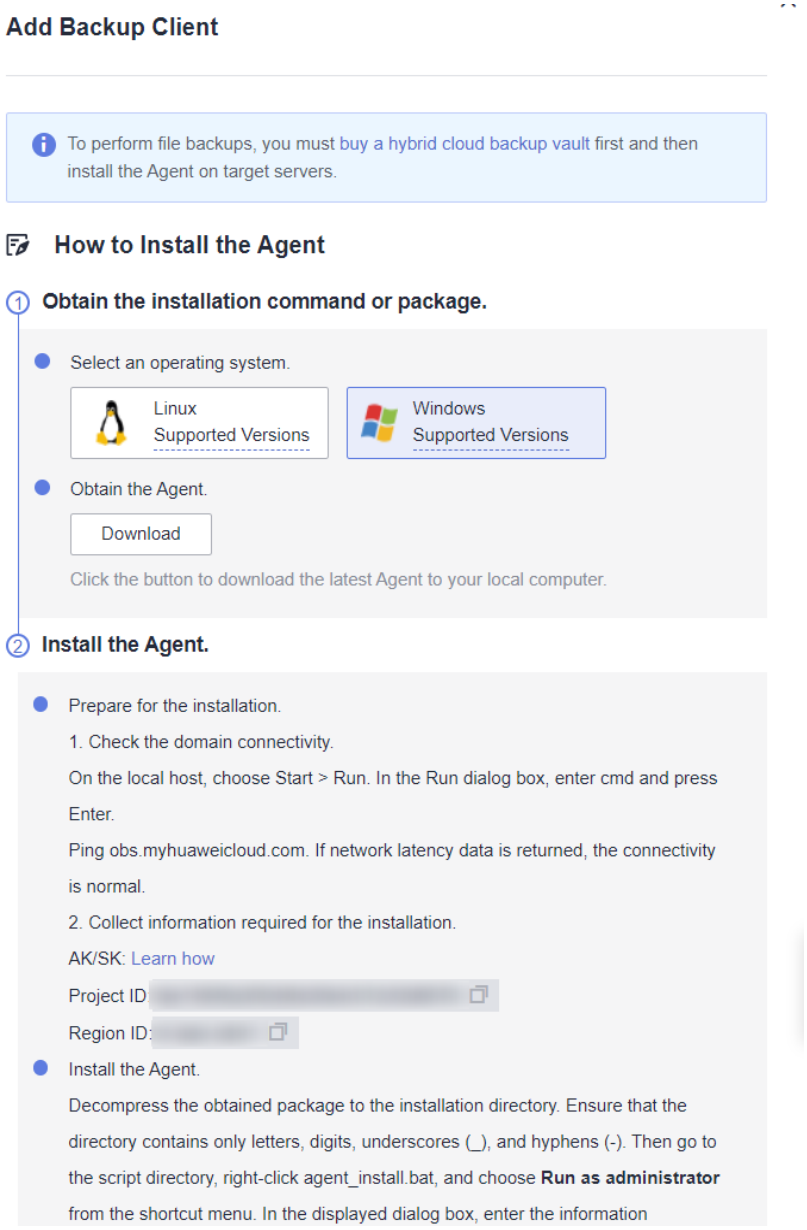
Instalar o Agente em um servidor de Windows

Passo 1 Faça logon no console do CBR.

1. Acesse o console de gerenciamento.
2. Clique em no canto superior esquerdo e selecione sua região e projeto.
3. Escolha **Storage** > **Cloud Backup and Recovery** > **File Backups**.

Passo 2 Clique em **Add Backup Client**. Na página exibida, selecione o sistema operacional Windows.

Figura 7-5 Windows



Passo 3 Clique em **Download** para baixar o pacote de instalação mais recente do Agente para o computador local.

Passo 4 No host local, escolha **Start** > **Run**. Na caixa de diálogo **Run**, insira **cmd** e pressione **Enter**.

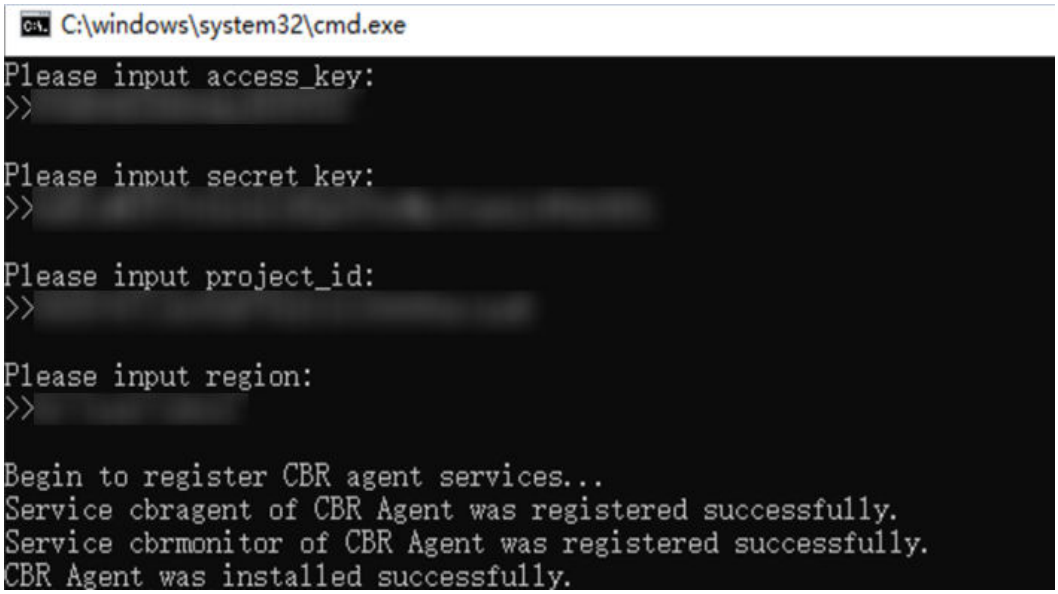
Execute o comando **ping obs.myhuaweicloud.com**. Se os dados de latência da rede forem retornados, a conectividade é normal.

Passo 5 Descompacte o pacote obtido no diretório de instalação. Certifique-se de que o diretório contém apenas letras, dígitos, sublinhados (_) e hífenes (-). Em seguida, vá para o diretório **script**, clique com o botão direito do mouse em **agent_install.bat** e escolha **Run as administrator** no menu de atalho. Na caixa de diálogo exibida, insira as informações necessárias.

Passo 6 Certifique-se de que o caminho de instalação contém apenas letras, dígitos, sublinhados (_) ou hífenes (-). Consulte **Figura 7-6**.

- **access_key**: insira a sua AK. **Como obter uma AK/SK?**
- **secret_key**: digite seu SK. **Como obter uma AK/SK?**
- **project_id**: copie o ID do projeto da página de instalação.
- **region**: copie o ID da região da página de instalação.

Figura 7-6 Executando o comando de instalação



NOTA

Se você estiver executando o Windows Server 2019, Windows Server 2012 ou Windows 7, uma mensagem indicando que MSVCR100.dll está ausente será retornada durante a instalação do Agente. Nesse caso, corrija o problema consultando **atualização de segurança do MFC** e reinstale o Agente.

Passo 7 Depois que "O Agente do CBR foi instalado com êxito" for retornado, aguarde cerca de 1 minuto, volte para a lista de backup de arquivos e encontre o cliente de backup. Se o status de Agente for **Normal**, o Agente foi instalado com êxito.

----Fim

Remover um cliente

Se um cliente de backup não for mais necessário, você poderá removê-lo.

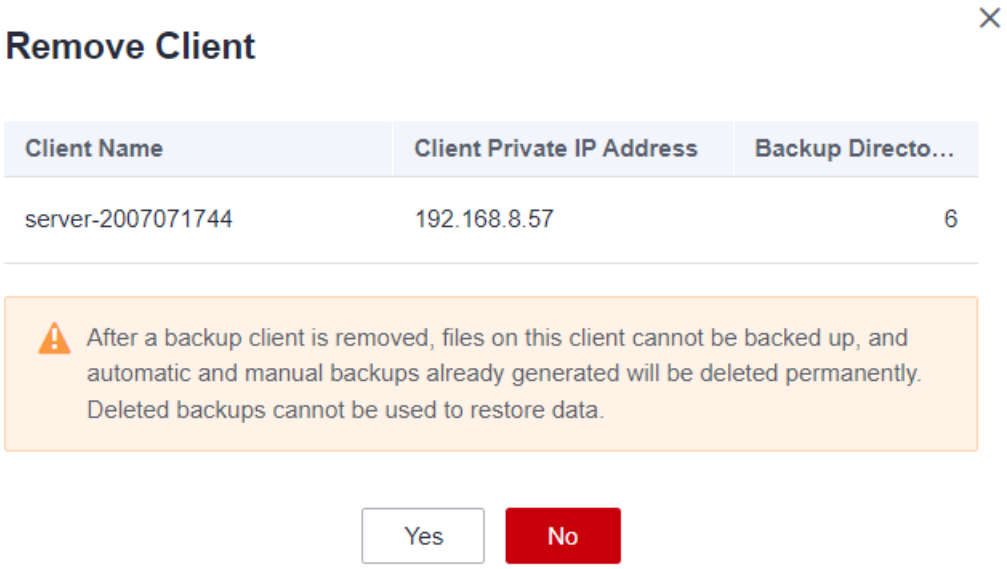
Passo 1 Faça logon no console do CBR.

1. Acesse o console de gerenciamento.
2. Clique em no canto superior esquerdo e selecione sua região e projeto.
3. Escolha **Storage** > **Cloud Backup and Recovery** > **File Backups**.

Passo 2 Localize a linha que contém o cliente de backup de destino, clique em **More** na coluna **Operation** e escolha **Remove Client**. Consulte **Figura 7-7**.

Depois que um cliente de backup for removido, não será possível fazer backup dos arquivos desse cliente, e os backups automáticos e manuais já gerados serão excluídos permanentemente. Os backups excluídos não podem ser usados para restaurar dados.

Figura 7-7 Remover cliente



Passo 3 Clique em **Yes**.

----Fim

7.5 Configuração de cofre

Cenários

Depois que o sistema detectar clientes de backup, configure um cofre para cada cliente para que os backups gerados sejam armazenados automaticamente no cofre.

Procedimento

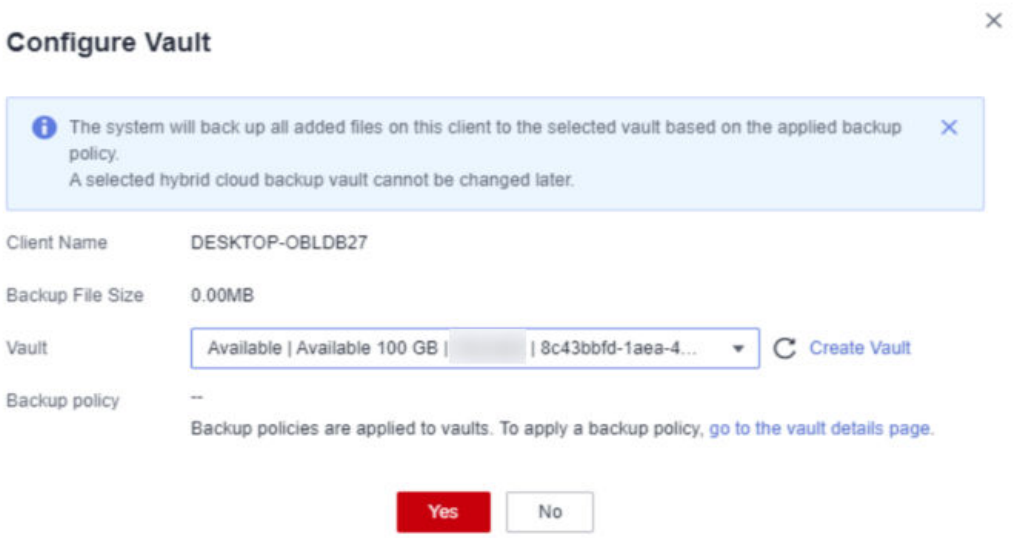
Passo 1 Faça logon no console do CBR.

1. Acesse o console de gerenciamento.
2. Clique em no canto superior esquerdo e selecione sua região e projeto.
3. Escolha **Storage** > **Cloud Backup and Recovery** > **File Backups**.

Passo 2 Clique na guia **File Backup** e localize o cliente de backup de destino. Em seguida, clique em **Configure Vault** na coluna **Backup Configuration**.

Passo 3 Na página exibida, selecione um cofre. Consulte **Figura 7-8**.

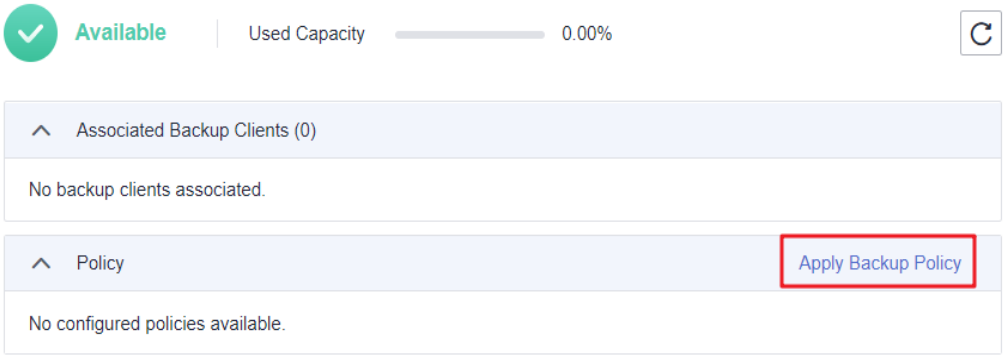
Figura 7-8 Configurar o cofre



Passo 4 Clique em **OK**. Exiba o vault configurado na coluna **Backup Configuration** da lista de backup de arquivos.

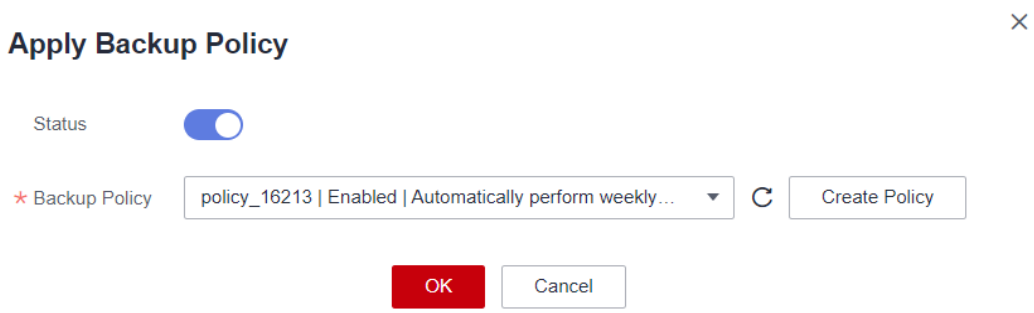
Passo 5 (Opcional) Se uma política de backup não for aplicada ao criar o cofre de backup na nuvem híbrida e agora você quiser configurar o backup automático para os clientes de backup, clique no nome do cofre na coluna **Backup Configuration** e aplique uma política de backup ao cofre. Consulte **Figura 7-9**.

Figura 7-9 Aplicar política



Passo 6 (Opcional) Clique em **Apply Backup Policy**. Selecione uma política de backup existente ou crie uma nova. Consulte **Figura 7-10**.

Figura 7-10 Aplicar política



Passo 7 (Opcional) Clique em **OK**. A política é aplicada com êxito ao cofre de backup em nuvem híbrida.

----Fim

7.6 Adição de diretórios

Cenários

Depois que o agente for instalado nos servidores de destino, o CBR os detectará e mostrará automaticamente como clientes de backup na lista de **Cloud Backup and Recovery** > **File Backups** > **File backup** Você precisa de adicionar os caminhos dos arquivos e diretórios que deseja fazer backup.

Restrições

- Um cliente de backup pode ter um máximo de 8 diretórios adicionados.
- Um diretório suporta até 100.000 arquivos.
- O tamanho de um diretório não pode exceder 500 GB.
- Um caminho deve ser um caminho absoluto, por exemplo, um caminho começando com /, C:\ ou D:\.

Adicionar diretórios

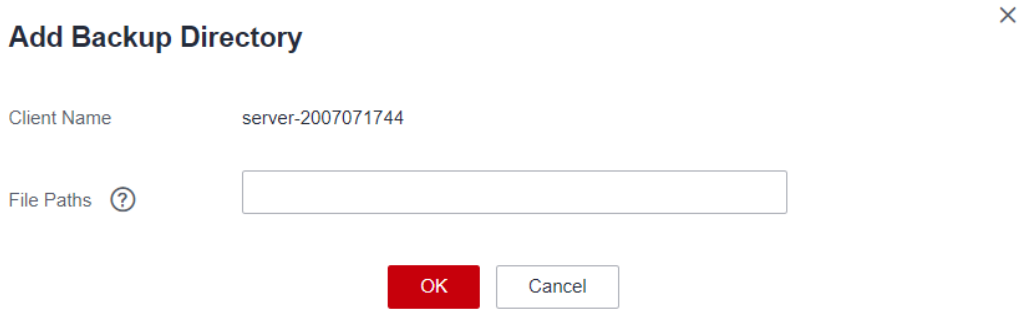
Passo 1 Faça logon no console do CBR.

1. Acesse o console de gerenciamento.
2. Clique em no canto superior esquerdo e selecione sua região e projeto.
3. Escolha **Storage** > **Cloud Backup and Recovery** > **File Backups**.

Passo 2 Localize o cliente de backup de destino e clique em seu nome para ir para a página de detalhes.

Passo 3 Clique em **Add Backup Directory**. Consulte **Figura 7-11**.

Figura 7-11 Adicionar diretório de backup



Passo 4 Cole os caminhos na caixa de texto e clique em **OK**.

Passo 5 Os caminhos dos arquivos serão exibidos na parte inferior da página.

----Fim

Remover diretórios

Se o backup não for mais necessário para um diretório ou se o número máximo de diretórios permitidos tiver sido atingido, você poderá remover diretórios.

Passo 1 Efetue logon no console do ECS.

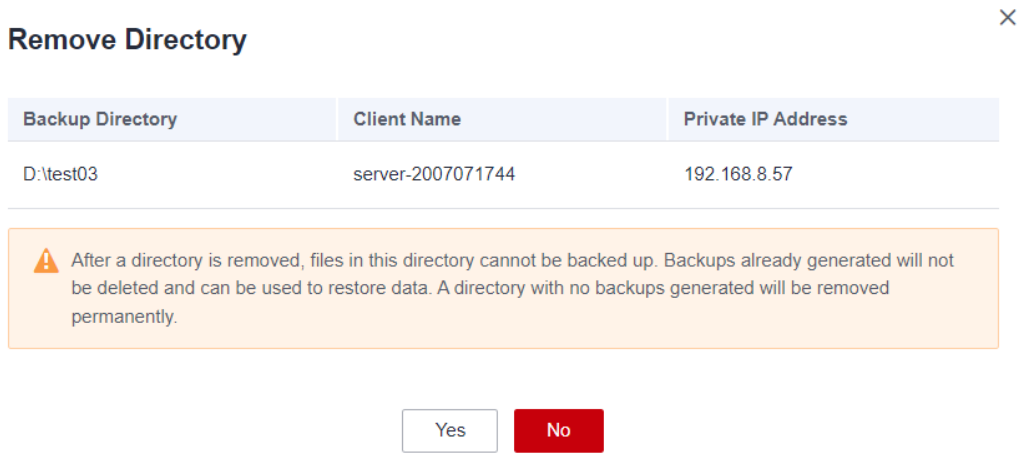
1. Acesse o console de gerenciamento.
2. Clique em no canto superior esquerdo e selecione sua região e projeto.
3. Escolha **Storage** > **Cloud Backup and Recovery** > **File Backups**.

Passo 2 Localize o cliente de backup de destino e clique em seu nome para ir para a página de detalhes.

Passo 3 Localize o diretório de destino e clique em **Remove Directory**. Consulte **Figura 7-12**.

Depois que um diretório é removido, os arquivos neste diretório não podem ser copiados. Os backups já gerados não serão excluídos e podem ser usados para restaurar dados. Um diretório sem backups gerados será removido permanentemente.

Figura 7-12 Remover diretório



Passo 4 Clique em **Yes**.

----Fim

7.7 Criação de backups de arquivos

Cenários

Esta seção descreve como criar manualmente backups de arquivos.

Para implementar o backup automático, crie uma política e aplique-a a um cofre consultando **Criação de uma política de backup**. Em seguida, o sistema executará backups automaticamente nos pontos de tempo especificados na política.

Restrições

- Somente os clientes de backup cujo status do Agente é **Normal**podem ser copiados.

Procedimento

Passo 1 Faça logon no console do CBR.

1. Acesse o console de gerenciamento.
2. Clique em  no canto superior esquerdo e selecione sua região e projeto.
3. Escolha **Storage** > **Cloud Backup and Recovery** > **File Backups**.

Passo 2 Clique na guia **File Backup** e localize o cliente de backup de destino.

Passo 3 Clique em **Perform Backup** na coluna **Operation**. O sistema cria automaticamente um backup para os arquivos.

Passo 4 Na página de guia **File Backup**, clique no nome do cliente de backup de destino. Na área **Backup Details** da página exibida, se os status de todos os backups gerados estiverem **Available**, a tarefa de backup será bem-sucedida.

NOTA

Se você fizer alterações em um arquivo durante o backup, o backup desse arquivo pode falhar. Para garantir a integridade dos dados, é aconselhável esperar até que a tarefa de backup seja concluída e, em seguida, alterar o arquivo e realizar um backup novamente.

Após a conclusão da tarefa de backup, você pode restaurar os dados do arquivo consultando **Restauração de dados usando um backup de arquivo** como necessário.

----Fim

7.8 Restauração de dados usando um backup de arquivo

Você pode usar um backup de arquivo para restaurar os dados de um cliente de backup para o estado em um determinado momento em que foi feito backup dos dados.

Restrições

- O status do Agente do cliente de backup deve ser **Normal**.
- É aconselhável não restaurar backups de arquivos para aplicativos em execução. Pare os aplicativos e, em seguida, restaurar os arquivos.

Método 1

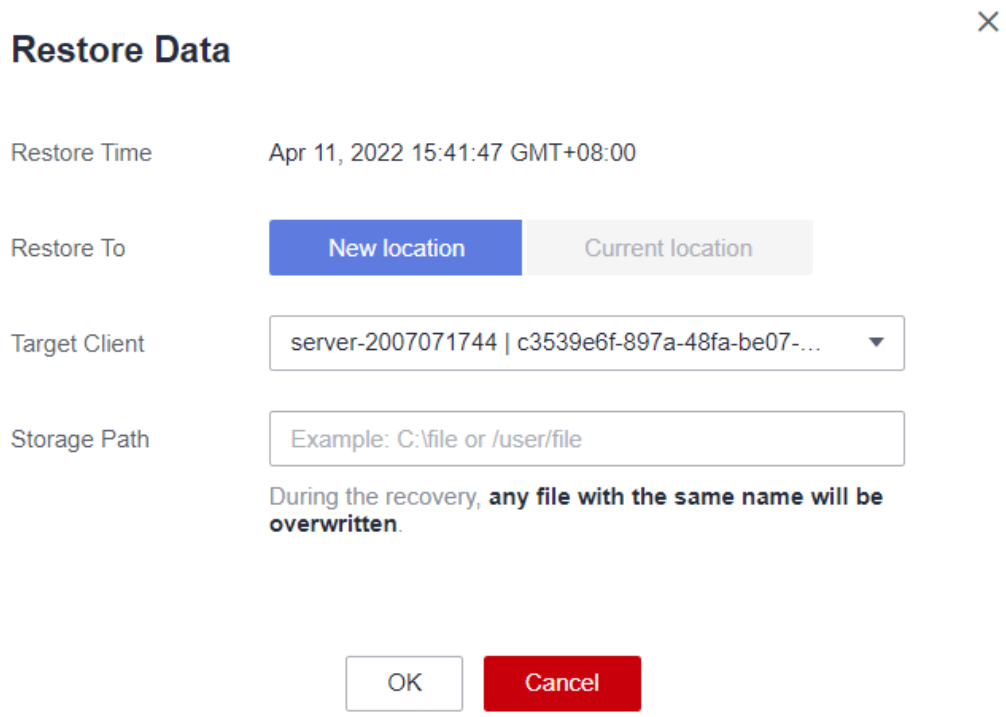
Passo 1 Faça logon no console do CBR.

1. Acesse o console de gerenciamento.
2. Clique em no canto superior esquerdo e selecione sua região e projeto.
3. Escolha **Storage** > **Cloud Backup and Recovery** > **File Backups**.

Passo 2 Na página de guia **File Backup**, clique no nome do cliente de backup de destino.

Passo 3 Encontre o backup desejado e clique em **Restore Data**.

Figura 7-13 Restaurar um arquivo



Passo 4 Selecione um local de restauração.

- **Current location**: os dados serão restaurados para o caminho do arquivo original no cliente de backup atual e qualquer arquivo com o mesmo nome será substituído. Essa opção está disponível apenas para clientes de backup de Linux.
- **New location**: os dados serão restaurados para um servidor diferente. Você pode selecionar um cliente de destino e especificar um caminho.

  Você só pode escolher entre os clientes de backup cujo status de agente é **Normal**. Se o servidor de destino não estiver na lista, vá para a lista de backup de arquivos e instale o Agente.

Passo 5 Clique em **OK**. Você pode verificar se os dados foram restaurados com êxito na área **Backup Details** da página de detalhes do cliente ou no host local.

Quando o status do backup é alterado para **Available**, a restauração é bem-sucedida.

----Fim

Método 2

Passo 1 Faça logon no console do CBR.

1. Acesse o console de gerenciamento.
2. Clique em no canto superior esquerdo e selecione sua região e projeto.
3. Escolha **Storage** > **Cloud Backup and Recovery** > **File Backups**.

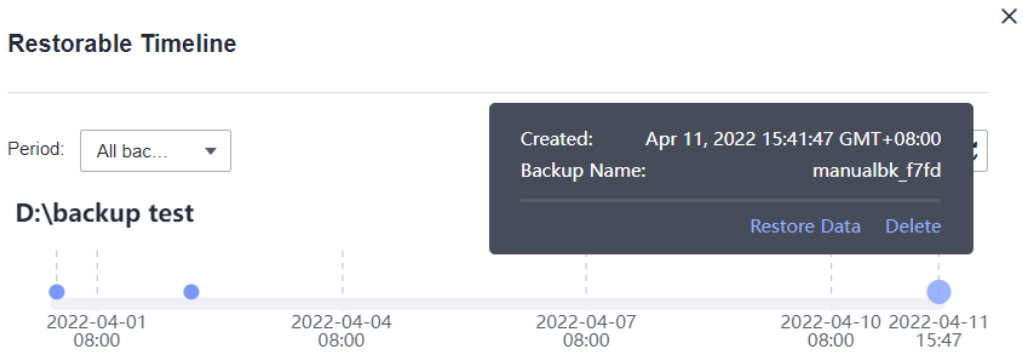
Passo 2 Na página de guia **File Backup**, clique no nome do cliente de backup de destino.

Passo 3 Clique em **Restorable Timeline** na coluna **Operation**.

Passo 4 Selecione um tempo de restauração e clique em **Restore Data**. Consulte **Figura 7-14**.

O sistema restaurará os dados para o estado no horário selecionado.

Figura 7-14 Linha do tempo restaurável



Passo 5 Selecione um local de restauração.

- **Current location**: os dados serão restaurados para o caminho do arquivo original no cliente de backup atual e qualquer arquivo com o mesmo nome será substituído.
- **New location**: os dados serão restaurados para um servidor diferente. Você pode selecionar um cliente de destino e especificar um caminho.

  Você só pode escolher entre os clientes de backup cujo status de agente é **Normal**. Se o servidor de destino não estiver na lista, vá para a lista de backup de arquivos e instale o Agente.

Passo 6 Clique em **OK**. Você pode verificar se os dados foram restaurados com êxito na área **Backup Details** da página de detalhes do cliente ou no host local.

Quando o status do backup é alterado para **Available**, a restauração é bem-sucedida.

----Fim

7.9 Desinstalação do Agente

Cenários

Desinstale o Agente de um cliente de backup se o backup do arquivo não for mais necessário.

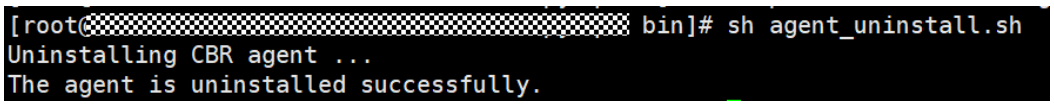
Desinstalando o Agente do Linux

Passo 1 Efetue logon no host do cliente e execute **su - root** para alternar para o usuário **root**.

Passo 2 No diretório **/opt/huaweicloud/cbragent/bin**, execute o seguinte comando para desinstalar o Agente. Se informação semelhante a **Figura 7-15** forem exibidas, o Agente foi desinstalado.

```
sh agent_uninstall.sh
```

Figura 7-15 Agente desinstalado do Linux



----Fim

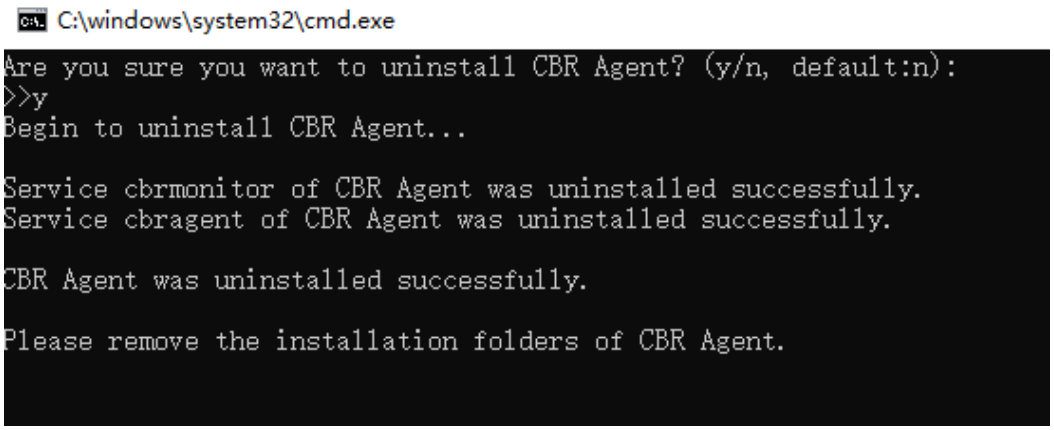
Desinstalando o Agente do Windows

Passo 1 Efetue logon no host do cliente.

Passo 2 Vá para o diretório **bin** no caminho de instalação e clique duas vezes em **agent_uninstall.bat**. Digite **y** para desinstalar o Agente.

Se informação semelhante a **Figura 7-16** forem exibidas, o Agente foi desinstalado.

Figura 7-16 Agente desinstalado do Windows



----Fim

7.10 Casos de resolução de problemas

Contexto

Quando você instala o Agente para adicionar clientes de backup, a instalação do Agente pode falhar ou pode ocorrer um erro após a instalação do Agente. Esta seção descreve alguns sintomas comuns, possíveis causas e soluções para ajudá-lo a localizar rapidamente o problema.

Status anormal do Agente

Sintoma:

depois que o Agente foi instalado, o status do Agente foi exibido como Anormal na lista de clientes.

Possível causa:

o status do Agente é anormal.

Solução:

1. verifique se o processo do Agente está sendo executado corretamente. Se o processo tiver terminado, inicie-o novamente.

   No Windows, clique duas vezes no arquivo **agent_start.bat**. No Linux, execute o comando **service cbragent start**.
2. Reinstale o Agente.
3. Verifique o fuso horário e a data no cliente de backup. Se a diferença de tempo entre o cliente e o servidor for superior a 15 minutos, ajuste a hora local com base na hora UTC. Se o status do Agente permanecer anormal depois que o horário do cliente for ajustado, aguarde cerca de meia hora até que o sistema atualize o status mais recente do Agente.

Falha na instalação do Agente com a mensagem "BackupService.7403, Invalid Agent" retornada

Sintoma:

a instalação do Agente falhou e a mensagem "BackupService.7403, Invalid Client" foi retornada.

Possível causa:

nenhum cofre de backup em nuvem híbrida está disponível antes da instalação do Agente.

Solução:

1. compre um cofre de backup em nuvem híbrida no console do CBR.
2. Reinstale o Agente.

Falha na instalação do Agente com a mensagem "Could not resolve host" retornada

Sintoma:

a instalação do Agente falhou e a mensagem "Could not resolve host" foi retornada.

Figura 7-17 Mensagem "Could not resolve host"

Possível causa:

o servidor DNS local não pode resolver o nome de domínio público da Huawei Cloud.

Solução:

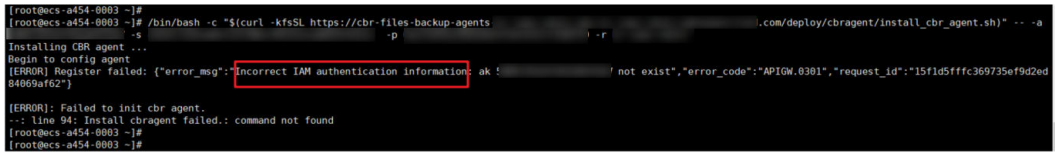
1. edite o arquivo **resolv.conf** no host local e verifique se o servidor DNS está configurado. Se você acessar a Huawei Cloud a partir da Internet, defina o servidor DNS como **8.8.8.8**.
2. Reinstale o Agente.

Falha na instalação do Agente com a mensagem "Incorrect IAM authentication information" retornada

Sintoma:

Falha na instalação do Agente com a mensagem "Incorrect IAM authentication information" retornada.

Figura 7-18 Mensagem "Incorrect IAM authentication information"



Possível causa:

a AK e a SK inseridos durante a instalação estão incorretos.

Solução:

1. obtenha a AK e a SK corretos e insira-os novamente.
2. Reinstale o Agente.

A instalação do Agente no Windows falhou com "OpenSCManager failed falhou" gravado no log

Sintoma:

falha na instalação do Agente no Windows com "OpenSCManager falhou" registrado no log.

Possível causa:

O script de instalação não é executado como administrador.

Solução:

execute o script de instalação como administrador para reinstalar o Agente.

O backup falhou depois que o Agente de um cliente Windows foi reinstalado e o status do Agente foi exibido como anormal no console

Sintoma:

depois que o Agente de um cliente de backup do Windows foi desinstalado e, em seguida, reinstalado, os backups falharam e o status do Agente foi exibido como Anormal no console.

Possível causa:

- o Agente falha ao enviar mensagens de pulsação ou o nome de domínio está incorreto.
- As gravações no arquivo de configuração do Agente falham ou encontram um erro.

Solução:

desinstale o Agente e reinstale-o.

O cliente Windows estava offline e não foi reiniciado

Sintoma:

falha na instalação do Agente no Windows com "OpenSCManager failed" registrado no log.

Possível causa:

há um grande número de arquivos .tmp (gerados devido a exceções de compactação de log) no diretório de log.

Solução:

1. Exclua todos os arquivos de log no diretório de log e desinstale o Agente.
2. Reinstale o Agente.

8 (Opcional) Migração de recursos do CSBS/VBS

Contexto

Huawei Cloud lançou o serviço de backup de última geração, o CBR. Se você tiver recursos de backup no CSBS ou no VBS, mas quiser alternar para o CBR para o gerenciamento desses recursos de backup histórico, poderá migrá-los para o CBR com apenas alguns cliques.

Se você nunca usou CSBS ou VBS, ou não precisa mais dos backups históricos, ignore esta seção.

Regras de migração

Durante a migração, o sistema criará cofres automaticamente com base em seus recursos históricos.

1. Se os servidores ou discos tiverem sido associados a uma política de backup e tiverem sido copiados, durante a migração, o sistema criará um cofre com o mesmo nome (até 64 caracteres) que o nome da política, independentemente de a política estar ativada. Após a criação do cofre, a política será aplicada ao cofre.
2. Se os servidores ou discos tiverem sido associados a uma política de backup, mas nenhum backup tiver sido gerado, durante a migração, o sistema criará um cofre somente quando a política estiver ativada. Após a criação do cofre, a política será aplicada ao cofre. A regra para nomear o cofre é a mesma da regra anterior.
3. Se os servidores ou discos tiverem sido aplicados com uma política de backup ou replicação, mas nenhum backup ou réplica tiver sido gerado e a política não estiver ativada, somente a política será migrada.
4. O sistema migrará políticas de backup e replicação, independentemente de estarem associadas a servidores ou discos.
5. Se o backup consistente com a aplicação estiver habilitado em uma política de backup, o sistema criará um cofre para armazenar backups consistentes com a aplicação gerados e o nome do cofre será o mesmo que o nome da política.
6. As réplicas de backup geradas serão armazenadas em um cofre de replicação chamado **default**.
7. Outros backups, como backups manuais, serão armazenados em um cofre de backup do servidor chamado **default**. Cofres diferentes serão criados automaticamente com base

em diferentes tipos de recursos. Por exemplo, o sistema criará um cofre de backup de disco durante a migração de backups em disco.

8. Depois que os recursos forem migrados, os backups criados usando o CBR também serão exibidos no console do VBS, mas você será cobrado apenas uma vez.

   NOTA

   Para excluir backups do console do VBS, localize esses backups no CBR e exclua-os. Em seguida, os backups também serão excluídos automaticamente do console do VBS.

9. Se uma imagem tiver sido criada usando um backup antes da migração e uma tag tiver sido adicionada à imagem, a migração de backup poderá falhar. Nesse caso, vá para o console do IMS, exclua a tag da imagem e, em seguida, execute a migração novamente. Após a conclusão da migração, adicione novamente a tag, se necessário.
10. Se os backups forem migrados de qualquer uma das seguintes regiões, todos os backups nessas regiões serão migrados: CN East-Shanghai1, CN North-Beijing4, CN South-Guangzhou, CN-Hong Kong, AP-Singapore, e AP-Bangkok. Para migrar backups em outras regiões, vá para a região correspondente e prossiga com a migração separadamente.

Com base nas regras anteriores, a capacidade de cada cofre criado pelo sistema é predefinida como 1,2 vezes do tamanho total do backup.

Por exemplo, um usuário tem um ECS de 100 GB e um ECS de 50 GB. A capacidade de armazenamento usada dos dois ECSs é de 20 GB e 10 GB, respectivamente. O usuário fez backup manualmente dos dois ECSs inteiros usando o backup do servidor em nuvem. Durante a migração, a capacidade do cofre criado automaticamente será de 1,2 vezes o tamanho total do backup. Neste exemplo, o tamanho total do backup multiplicado por 1,2 é 36 GB. Assim, o sistema criará automaticamente um cofre de 36 GB.

Restrições

- Por padrão, um cofre criado pelo sistema é cobrado na base de pagamento por uso. Se você desejar alterar o modo de cobrança para anual/mensal, consulte as instruções em **Alteração do modo de cobrança de pagamento por uso para anual/mensal**.
- Após a migração dos recursos, o VBS e o CSBS ficarão indisponíveis. O CBR utiliza novos padrões de cobrança. Para obter mais informações, consulte **Detalhes de preços do CBR**.
- Os cofres que você comprou não podem ser utilizados para migração. O sistema migrará automaticamente os recursos para os cofres criados pelo sistema.
- Os recursos de backup de uma conta precisam ser migrados apenas uma vez.
- Depois que os recursos forem migrados, os backups em disco e os backups do servidor serão armazenados automaticamente nos cofres do CBR. Não são necessárias mais operações.

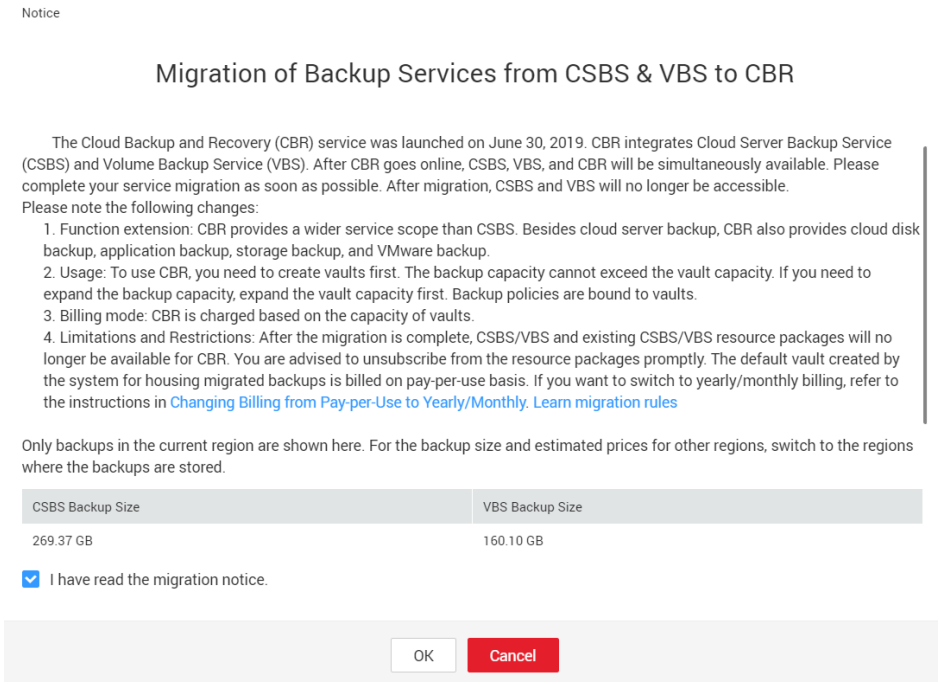
Procedimento

Passo 1 Faça logon no console de CBR.

1. **Efetue logon no console de gerenciamento**.
2. Clique em  no canto superior esquerdo e selecione sua região e projeto.
3. Escolha **Storage** > **Cloud Backup and Recovery**. Selecione uma guia de backup no painel de navegação esquerdo.

Passo 2 Clique em **Migrate to CBR** no canto superior direito. Leia o conteúdo na caixa de diálogo exibida e clique em **OK**. See **Figura 8-1**.

Figura 8-1 Migrar recursos para o CBR



Passo 3 O sistema migrará recursos automaticamente. Após a migração, um cofre chamado **default** será criado e uma mensagem será exibida na parte superior da página indicando que a migração foi bem-sucedida.

----Fim

FAQ

1. Por que os backups do CBR são exibidos no console do VBS?

   Se você migrou dados do CSBS e do VBS para o CBR e criou um backup no Console do CBR, o mesmo registro de backup será gerado no Console do VBS. Isto é devido a um mecanismo subjacente. O console do VBS exibe todos os backups gerados pelo CBR, CSBS e VBS. Esses backups não serão cobrados repetidamente.

2. Como fazer para excluir backups do console do VBS?

   Depois de migrar os dados do CSBS e do VBS para o CBR, os backups exibidos no console do VBS não podem ser excluídos sozinhos. Encontre esses backups no CBR e exclua-os. Em seguida, os backups também serão excluídos do console do VBS.

3. Quais são as diferenças entre CBR, CSBS e VBS?

   O CBR integra o CSBS e o VBS. Além disso, o CBR suporta backup do SFS Turbo e backup em nuvem híbrida. O uso e faturamento do CBR também são diferentes do CSBS e do VBS.

4. O que posso fazer se uma mensagem é exibida indicando que um recurso foi vinculado com CSBS ou VBS?

Escolha **Cloud Server Backup Service** ou **Volume Backup Service** na lista de serviços. No console de serviço correspondente, verifique se há recursos vinculados a políticas na guia **Policies**. Em caso afirmativo, desvincule os recursos da política e vá para o console do CBR para associar os recursos a um cofre.

9 Gerenciamento de tarefas

Esta seção descreve como visualizar falhas. A lista de tarefas mostra as tarefas de backup orientadas por políticas que foram executadas nos últimos 30 dias.

Pré-requisitos

Existe pelo menos uma tarefa com falha.

Procedimento

Passo 1 Faça logon no console de CBR.

1. Acesse o console de gerenciamento.
2. Clique em no canto superior esquerdo e selecione sua região e projeto.
3. Escolha **Storage** > **Cloud Backup and Recovery** > **Tasks**.

Passo 2 Você pode filtrar tarefas por projeto empresarial, tipo de tarefa, status da tarefa, ID da tarefa, ID do recurso, nome do recurso, ID do cofre, nome do cofre e hora.

Passo 3 Clique em na frente da tarefa para exibir os detalhes da tarefa.

Se uma tarefa falhar, você poderá visualizar a causa da falha nos detalhes da tarefa.

----Fim

10 Monitoramento

10.1 Métricas do CBR

Cenários

Esta seção descreve as métricas relatadas pelo CBR, bem como seus namespaces e dimensões. Você pode usar o console ou as **APIs** fornecidas pelo Cloud Eye para consultar as métricas geradas para o CBR.

Namespace

SYS.CBR

Métricas

Tabela 10-1 Métricas do CBR

ID da métrica	Nome da métrica	Descrição	Intervalo de valores	Objeto monitorado	Período de monitoramento (dados brutos)
used_vault_size	Tamanho do cofre usado	Capacidade usada do cofre Unidade: GB	≥ 0	cofre	15 min
vault_util	Utilização do cofre	Uso da capacidade do cofre	0~100%	cofre	15 min

Dimensões

Key	Value
instance_id	Nome/ID do cofre

Visualizar estatísticas de monitoramento

Passo 1 Acesse o console de gerenciamento.

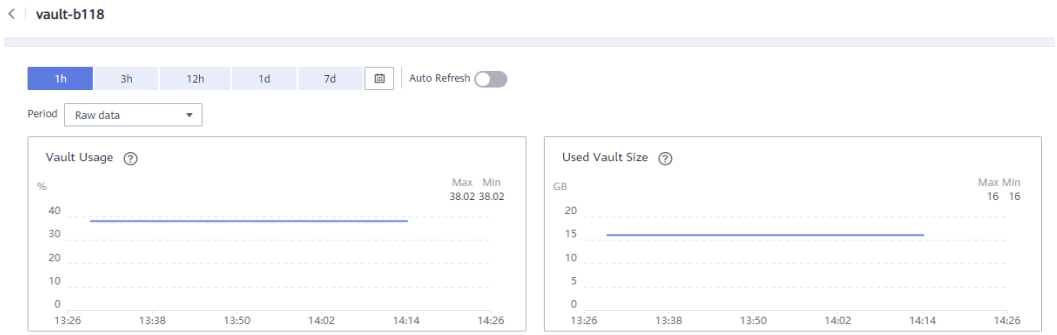
Passo 2 Visualize os gráficos de monitoramento usando um dos seguintes métodos.

- Método 1: escolha **Storage** > **Cloud Backup and Recovery**. Na lista do cofre, localize o cofre cujos dados de monitoramento deseja visualizar e escolha **More** > **View Monitoring Data** na coluna **Operation**.
- Método 2: escolha **Management & Governance** > **Cloud Eye** > **Cloud Service Monitoring** > **Cloud Backup and Recovery**. Na lista do cofre, clique em **View Metric** na coluna **Operation** do cofre cujos dados de monitoramento você deseja visualizar

Passo 3 Você pode visualizar os dados de monitoramento do cofre por métrica ou duração monitorada.

Figura 10-1 mostra os gráficos de monitoramento.Para obter mais informações, consulte o *Guia de usuário do Cloud Eye*.

Figura 10-1 Gráficos de monitoramento do cofre



----Fim

10.2 Criação de uma regra de alarme

Esta seção descreve como criar uma regra de alarme para o CBR.

O backup em nuvem híbrida permite o monitoramento apenas na capacidade do cofre. Operações e eventos locais não podem ser monitorados.

Procedimento

1. Acesse o console de gerenciamento.
2. Em **Management & Governance**, selecione **Cloud Eye**. No painel de navegação à esquerda, escolha **Alarm Management** > **Alarm Rules**.
3. Na página exibida, clique em **Create Alarm Rule** no canto superior direito.

4. Na caixa de diálogo **Create Alarm Rule**, defina os parâmetros.
   a. Defina **Name** e **Description**.

Tabela 10-2 Parâmetros para configurar o nome e a descrição da regra

Parâmetro	Descrição	Valor de exemplo
Name	Nome da regra de alarme. O sistema gera um nome aleatório, que você pode modificar.	alarme-cgnw
Description	Descrição da regra de alarme. Este parâmetro é opcional.	-

   b. Defina os parâmetros de conteúdo do alarme.
   c. Configure a notificação de alarme.

Tabela 10-3 Parâmetros para configurar a notificação de alarme

Parâmetro	Descrição	Valor de exemplo
Notificação de alarme	Especifica se os usuários devem ser notificados quando os alarmes forem disparados. As notificações podem ser enviadas por e-mail ou mensagem de texto, ou através de solicitações HTTP/HTTPS para servidores. Você pode ativar (recomendado) ou desativar **Alarm Notification**.	-
Período de validade	O Cloud Eye envia notificações somente dentro do período de validade especificado na regra de alarme. Por exemplo, se **Validity Period** estiver definido como **00:00-8:00**, o Cloud Eye enviará notificações apenas entre 00:00-8:00.	-
Objeto de notificação	Especifica o nome do tópico para o qual a notificação de alarme será enviada. Se você ativar a notificação de alarme, precisará selecionar um tópico. Se não houver tópicos desejáveis disponíveis, você precisa criar um primeiro, após o que o serviço SMN é invocado. Para obter detalhes sobre como criar um tópico, consulte o *Guia de usuário do Simple Message Notification*.	-
Condição de gatilho	Especifica a condição para disparar a notificação de alarme. Você pode selecionar **Generated alarm**, **Cleared alarm**, ou ambos.	-

d. Clique em **Create**.

Depois que a regra de alarme é criada, se os dados de métrica atingirem o limite especificado ou um evento do CBR acontecer, o Cloud Eye informará imediatamente que uma exceção ocorreu. Para obter detalhes, consulte o *Guia de usuário do Cloud Eye*.

11 Auditoria

Você pode usar o Cloud Trace Service (CTS) para rastrear operações no CBR.

Pré-requisitos

O CTS foi habilitado.

Principais operações gravadas pelo CTS

Tabela 11-1 Operações de CBR que podem ser gravadas pelo CTS

Operação	Tipo de recurso	Nome do rastreamento
Criar uma política	policy	criarPolítica
Atualizar uma política	policy	updatePolicy
Excluir uma política	policy	deletePolicy
Definir uma política de cofre	vault	associatePolicy
Remover uma política de um cofre	cofre	dissociatePolicy
Criar um cofre	cofre	createVault
Modificar um cofre	vault	updateVault
Excluir de um cofre	vault	deleteVault
Remover recursos	vault	removeResources
Adicionar recursos	vault	addResources
Executar uma replicação	vault	replicateVaultBackup
Realizar um backup	vault	createVaultBackup
Criar um backup	backup	createBackup
Excluir um backup	backup	deleteBackup

Operação	Tipo de recurso	Nome do rastreamento
Sincronizar um backup	backup	syncBackup
Restaurar um backup	backup	restoreBackup
Replicar um backup	backup	replicateBackup

Exibir registros de auditoria

Para saber como exibir logs de auditoria, consulte a seção "Consulta de rastreamentos em tempo real" no no *Guia de usuário do Cloud Trace Service*.

Desativar ou ativar um rastreador

O procedimento a seguir ilustra como desabilitar um rastreador existente no console CTS. Depois que um rastreador for desativado, o sistema interromperá as operações de gravação, mas você ainda pode visualizar registros históricos.

Passo 1 Acesse o console de gerenciamento.

Passo 2 No canto superior esquerdo da página, clique em e selecione a região e o projeto desejados.

Passo 3 Clique em **Service List** e escolha **Management & Governance** > **Cloud Trace Service**.

Passo 4 Clique em **Trackers** no painel de navegação esquerdo.

Passo 5 Na lista de rastreadores, clique em **Disable** na coluna **Operation**.

Passo 6 Clique em **Yes**.

Passo 7 Depois que o rastreador é desativado, a operação disponível muda de **Disable** para **Enable**. Para ativar o rastreador novamente, clique em **Enable** e, em seguida, clique em **Yes**. O sistema iniciará novamente as operações de gravação.

----Fim

12 Cotas

O que é cota?

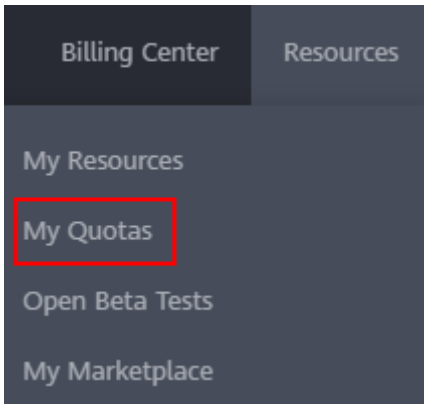
As cotas podem limitar o número ou a quantidade de recursos disponíveis para os usuários, como o número máximo dos ECSs ou discos EVS que podem ser criados.

Se a cota de recursos existente não puder atender aos seus requisitos de serviço, você poderá solicitar uma cota mais alta.

Como fazer para ver minhas cotas?

1. Acesse o console de gerenciamento.
2. Clique em no canto superior esquerdo e selecione a região e o projeto desejados.
3. No canto superior direito da página, escolha **Resources** > **My Quotas**.
   A página **Service Quota** é exibida.

   Figura 12-1 Minhas cotas

4. Visualize a cota usada e total de cada tipo de recursos na página exibida.
   Se uma cota não puder atender aos requisitos de serviço, solicite uma cota mais alta.

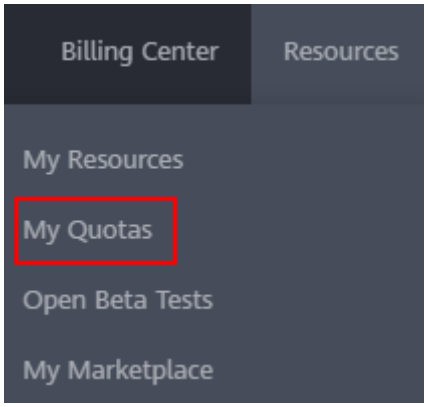
Como fazer para solicitar uma cota mais alta?

1. Acesse o console de gerenciamento.

2. No canto superior direito da página, escolha **Resources** > **My Quotas**.

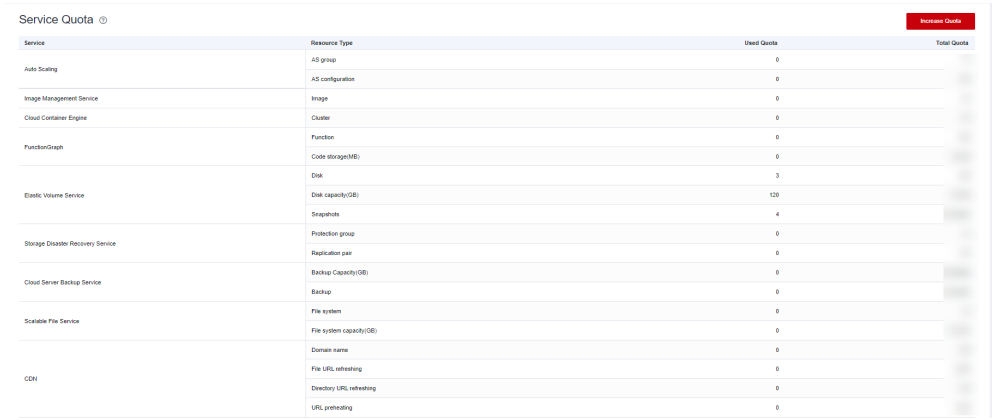
   A página **Service Quota** é exibida.

   Figura 12-2 Minhas cotas



3. Clique em **Increase Quota**.

   Figura 12-3 Increasing quota



4. Na página **Create Service Ticket**, configure os parâmetros conforme necessário.

   Na área **Problem Description**, preencha o conteúdo e o motivo do ajuste.

5. Depois que todos os parâmetros necessários estiverem configurados, selecione **I have read and agree to the Tenant Authorization Letter and Privacy Statement** e clique em **Submit**.

A Apêndice

A.1 Manutenção de segurança do Agente

A.1.1 Alteração da senha do usuário rdadmin

Cenários

- Para fins de segurança do O&M, é recomendável alterar regularmente a senha do usuário **rdadmin** do Agente do OS e desative a permissão de logon remoto desse usuário.
- No Linux, o usuário **rdadmin** não tem senha.
- Esta seção descreve como alterar a senha do usuário **rdadmin** no Windows 2012. Para outras versões, altere a senha de acordo com a situação real.

Pré-requisitos

- Você obteve um nome de usuário e sua senha para fazer logon no console de gerenciamento.
- O nome de usuário e a senha para fazer logon em um ECS do Windows foram obtidos.

Procedimento

Passo 1 Vá para o console do ECS e faça logon no ECS do Windows.

Passo 2 Escolha **Start** > **Control Panel**. Na janela **Control Panel**, clique em **User Accounts**.

Passo 3 Clique em **User Accounts**. A caixa de diálogo **User Account Control** é exibida. Selecione **rdadmin** e clique em **Reset Password**.

Passo 4 Digite a nova senha e clique em **OK**.

Passo 5 No **Task Manager**, clique na guia Serviços e, em seguida, clique em Abrir Serviço.

Passo 6 Selecione RdMonitor e RdNginx, respectivamente. Na caixa de diálogo exibida, selecione **Login**, altere a senha para a inserida na **Step 4**, e clique em **OK**.

----Fim

A.1.2 Alteração da senha da conta para relatórios de alarmes (SNMP v3)

Para melhorar a segurança de O&M do sistema, é aconselhável alterar a senha da conta para relatar alarmes.

Pré-requisitos

- Você obteve um nome de usuário e sua senha para fazer login no console de gerenciamento.
- O nome de usuário e a senha para fazer login em um servidor foram obtidos.

Contexto

Esta seção apresenta os procedimentos no Windows e no Linux.

AVISO

Se a senha de autenticação e a senha de criptografia de dados para SNMP v3 do Agente forem as mesmas, existem riscos de segurança. Para garantir a segurança do sistema, é aconselhável definir senhas diferentes para autenticação e criptografia de dados.

Obtenha a senha de autenticação inicial do suporte técnico.

NOTA

A senha deve atender aos seguintes requisitos de complexidade:

- contém 8 a 16 caracteres.
- contém pelo menos um dos seguintes caracteres especiais: `~!@#$%^&*()-_=+\|[{}];:",<.>/?
- contém pelo menos dois dos seguintes tipos de caracteres:
  - letras maiúsculas
  - letras minúsculas
  - caracteres numéricos
- não pode ser o mesmo que o nome de usuário ou o nome de usuário escrito na ordem inversa.
- não pode ser igual a senha anterior.
- não pode conter espaços.

Procedimento (Windows)

Passo 1 Efetue login no servidor em que o Agente está instalado.

Passo 2 Abra o CLI e vá ao diretório *installation path***bin**

Passo 3 Execute o comando **agentcli.exe chgsnmp**. Digite a senha de login do Agente e pressione **Enter**.

```
Please choose operation:
1: Change authentication password
2: Change private password
3: Change authentication protocol
4: Change private protocol
5: Change security name
6: Change security Level
```



```
7: Change security model
8: Change context engine ID
9: Change context name
Other: Quit
Please choose:
```

NOTA

admin é o nome de usuário configurado durante a instalação do Agente.

Passo 4 Selecione o SN da senha de autorização ou da senha de criptografia de dados que você deseja alterar e pressione **Enter**.

Passo 5 Digite a senha antiga e pressione **Enter**.

Passo 6 Digite a senha antiga e pressione **Enter**.

Passo 7 Digite a nova senha novamente e pressione **Enter**. A senha é alterada.

----Fim

Procedimento (Linux)

Passo 1 Efetue login no servidor Linux usando a senha do servidor.

Passo 2 Execute o comando **TMOUT=0** para evitar que o PuTTY saia devido ao tempo limite da sessão.

NOTA

Depois que o comando anterior é executado, o sistema permanece em execução mesmo quando nenhuma operação é executada, o que resulta em riscos de segurança. Para fins de segurança, execute o comando **exit** para sair do sistema após terminar de executar as operações.

Passo 3 Execute o comando **su - rdadmin** para alternar para o usuário **rdadmin**.

Passo 4 Execute o comando **/home/rdadmin/Agent/bin/agentcli chgsnmp** Digite a senha de login do Agente e pressione **Enter**.

NOTA

O caminho de instalação do Agente é **/home/rdadmin/Agent**.

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

Passo 5 Selecione o SN da senha de autorização ou da senha de criptografia de dados que você deseja alterar e pressione **Enter**.

Passo 6 Digite a senha antiga e pressione **Enter**.

Passo 7 Digite a senha antiga e pressione **Enter**.

Passo 8 Digite a nova senha novamente e pressione **Enter**. A senha é alterada.

----Fim

A.1.3 Substituição de certificado do servidor

Para fins de segurança, convém usar um certificado Secure Socket Layer (SSL) emitido por uma autoridade de certificação de terceiros. O Agente permite que você substitua certificados de autenticação e arquivos de chave privada, desde que você forneça os certificados de autenticação e os pares de chave privada-pública. A atualização do certificado pode ter efeito somente depois que o agente é reiniciado, portanto, é aconselhável atualizar o certificado durante o horário fora de pico.

Pré-requisitos

- Você obteve um nome de usuário e sua senha para fazer logon no console de gerenciamento.
- O nome de usuário e a senha para fazer logon em um servidor foram obtidos.
- Novos certificados no formato X.509v3 foram obtidos.

Contexto

- O Agente é pré-implantado com o certificado do Agent de CA **bcmagentca**, o arquivo de chave privada do certificado de CA **server.key** (), e o certificado de autenticação **server.crt**. Todos esses arquivos são salvos em **/home/rdadmin/Agent/bin/nginx/conf** (se você usa Linux) ou **\bin\nginx\conf** (se você usa Windows).
- Você precisa de reiniciar o Agente após substituir um certificado para torná-lo efetivo.

Procedimento (Linux)

Passo 1 Efetue logon no servidor Linux com o Agente instalado.

Passo 2 Execute o comando **TMOUT=0** para evitar que o PuTTY saia devido ao tempo limite da sessão.

NOTA

Depois que o comando anterior é executado, o sistema permanece em execução mesmo quando nenhuma operação é executada, o que resulta em riscos de segurança. Para fins de segurança, execute o comando **exit** para sair do sistema após terminar de executar as operações.

Passo 3 Execute o comando **su - rdadmin** para alternar para o usuário **rdadmin**.

Passo 4 Execute o comando **cd /home/rdadmin/Agent/bin** para ir para o caminho do script.

NOTA

O caminho de instalação do Agente é **/home/rdadmin/Agent**.

Passo 5 Execute o comando **sh agent_stop.sh** para parar a execução do Agente.

Passo 6 Coloque os novos certificados e arquivos de chave privada no diretório especificado.

NOTA

Coloque os novos certificados no diretório **/home/rdadmin/Agent/bin/nginx/conf**

Passo 7 Execute o comando **/home/rdadmin/Agent/bin/agentcli chgkey**.

As seguintes informações são exibidas:

```
Enter password of admin:
```

NOTA

admin é o nome de usuário configurado durante a instalação do Agente.

Passo 8 Digite a senha de logon do Agente e pressione **Enter**.

As seguintes informações são exibidas:

```
Change certificate file name:
```

Passo 9 Digite um nome para o novo certificado e pressione **Enter**.

NOTA

Se a chave privada e o certificado forem o mesmo arquivo, os nomes da chave privada e do certificado serão idênticos.

As seguintes informações são exibidas:

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

Passo 10 Digite um nome para o novo arquivo de chave privada e pressione **Enter**.

As seguintes informações são exibidas:

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

Passo 11 Digite a senha de proteção do arquivo de chave privada duas vezes. O certificado é então substituído com sucesso.

Passo 12 Execute o comando **sh agent_start.sh** para iniciar o Agente.

----Fim

Procedimento (Windows)

Passo 1 Efetue logon no servidor Windows com o agente instalado.

Passo 2 Abra o CLI e vá ao diretório *installation path***bin**

Passo 3 Execute o comando **sh agent_stop.sh** para parar a execução do Agente.

Passo 4 Coloque os novos certificados e arquivos de chave privada no diretório especificado.

NOTA

Coloque os novos certificados no diretório *installation path***bin\nginx\conf**.

Passo 5 Execute o comando **agentcli.exe chgkey**.

As seguintes informações são exibidas:

```
Enter password of admin:
```

NOTA

admin é o nome de usuário configurado durante a instalação do Agente.

Passo 6 Digite um nome para o novo certificado e pressione **Enter**.

NOTA

Se a chave privada e o certificado forem o mesmo arquivo, os nomes da chave privada e do certificado serão idênticos.

As seguintes informações são exibidas:

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

Passo 7 Digite um nome para o novo arquivo de chave privada e pressione **Enter**.

As seguintes informações são exibidas:

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

Passo 8 Digite a senha de proteção do arquivo de chave privada duas vezes. O certificado é então substituído com sucesso.

Passo 9 Execute o comando **agent_start.bat** para iniciar o Agente.

----Fim

A.1.4 Substituição de certificados de CA

Cenários

Um certificado de CA é um arquivo digital assinado e emitido por uma autoridade de autenticação. Ele contém a chave pública, informações sobre o proprietário da chave pública, informações sobre o emissor, período de validade e certas informações de extensão. Ele é usado para configurar um canal seguro de transferência de informações entre o agente e o servidor.

Se o certificado de CA não estiver em conformidade com os requisitos de segurança ou tiver expirado, substitua-o para fins de segurança.

Pré-requisitos

- O nome de usuário e a senha para efetuar logon em um ECS foram obtidos.
- Um novo certificado de CA está pronto.

Procedimento (Linux)

Passo 1 Efetue logon no servidor Linux com o Agente instalado.

Passo 2 Execute o seguinte comando para impedir o logout devido ao tempo limite do sistema:

TMOUT=0

Passo 3 Execute o seguinte comando para alternar para o usuário **rdadmin**:

su - rdadmin

Passo 4 Execute o seguinte comando para ir para o caminho para o script de início/parada do Agente:

cd /home/rdadmin/Agent/bin

Passo 5 Execute o seguinte comando para parar a execução do Agente:

sh agent_stop.sh

Passo 6 Execute o seguinte comando para ir para o caminho para o certificado de CA:

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

Passo 7 Execute o seguinte comando para excluir o certificado de CA existente:

rm bcmagentca.crt

Passo 8 Copie o novo arquivo de certificado de CA no diretório **/home/rdadmin/Agent/bin/nginx/conf** directory and rename the file **bcmagentca.crt**.

Passo 9 Execute o seguinte comando para alterar o proprietário do certificado de CA:

chown rdadmin:rdadmin bcmagentca.crt

Passo 10 Execute o seguinte comando para modificar as permissões no certificado de CA:

chmod 400 bcmagentca.crt

Passo 11 Execute o seguinte comando para ir para o caminho para o script de início/parada do Agente:

cd /home/rdadmin/Agent/bin

Passo 12 Execute o seguinte comando para iniciar o Agente:

sh agent_start.sh

----Fim

Procedimento (Windows)

Passo 1 Efetue logon no ECS com o Agente instalado.

Passo 2 Vá para o diretório *Installation path***bin**.

Passo 3 Execute o script **agent_stop.bat** para interromper o Agente.

Passo 4 Vá para o diretório *Installation path***nginx****conf**.

Passo 5 Exclua o arquivo de certificado **bcmagentca.crt**.

Passo 6 Copie o novo arquivo de certificado de CA no diretório *Installation path***nginx****conf** e renomeie o arquivo **bcmagentca.crt**.

Passo 7 Vá para o diretório *Installation path***bin**

Passo 8 Execute o script **agent_start.bat** para iniciar o Agente.

----Fim

A.2 História de mudanças

Lançado em	Descrição
21/11/2022	Esta edição é a sétima versão oficial, que incorpora a seguinte alteração: adição de uma restrição no backup de arquivos.

Lançado em	Descrição
20/07/2022	Esta edição é o sexto lançamento oficial, que incorpora a seguinte alteração: adição do conteúdo de backup do arquivo.
27/10/2021	Esta edição é o quinto lançamento oficial, que incorpora a seguinte alteração: adição do conteúdo de gerenciamento de permissões.
08/04/2020	Esta edição é a quarta versão oficial, que incorpora a seguinte alteração: adição do conteúdo de backup do sistema de arquivos.
25/02/2020	Esta edição é a terceira versão oficial, que incorpora a seguinte alteração: mudança da seção "Backup em nuvem híbrida" para uma nova documentação intitulada *Guia de recursos de backup em nuvem híbrida*.
27/08/2019	Esta edição é a segunda versão oficial, que incorpora a seguinte alteração: ● Exclusão da descrição sobre replicação entre regiões e backup do BMS.
31/07/2019	Esta edição é o primeiro lançamento oficial.

