

# Cloud Backup and Recovery

## User Guide

**Issue** 01  
**Date** 2025-01-16



**Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2025. All rights reserved.**

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Cloud Computing Technologies Co., Ltd.

## **Trademarks and Permissions**



HUAWEI and other Huawei trademarks are the property of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

## **Notice**

The purchased products, services and features are stipulated by the contract made between Huawei Cloud and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

---

# Contents

---

<b>1 Management permissions.....</b>	<b>1</b>
1.1 Creating a User and Granting CBR Permissions.....	1
1.2 Creating a Custom Policy.....	2
1.3 Configuring Forcible Backup Policies.....	4
<b>2 Vault Management.....</b>	<b>6</b>
2.1 Overview.....	6
2.2 Viewing a Vault.....	8
2.3 Deleting a Vault.....	11
2.4 Associating Resources to a Vault.....	13
2.5 Dissociating Resources from a Vault.....	17
2.6 Migrating Resources from a Vault.....	18
2.7 Expanding Vault Capacity.....	19
2.8 Reducing Vault Capacity.....	21
2.9 Changing from Pay-per-Use to Yearly/Monthly.....	22
2.10 Changing Vault Specifications.....	22
2.11 Replicating a Vault Across Regions.....	23
2.12 Managing Vault Tags.....	27
2.13 Managing the Enterprise Projects of Vaults.....	28
2.14 Enabling Backup Locking.....	29
<b>3 Backup Management.....</b>	<b>31</b>
3.1 Overview.....	31
3.2 Viewing a Backup.....	34
3.3 Changing a Backup Name.....	36
3.4 Sharing a Backup.....	37
3.5 Deleting a Backup.....	41
3.6 Replicating a Backup Across Regions.....	43
<b>4 Policy Management.....</b>	<b>46</b>
4.1 Overview.....	46
4.2 Viewing the Policy of a Vault.....	47
4.3 Creating a Backup Policy.....	48
4.4 Creating a Replication Policy.....	56
4.5 Modifying a Policy.....	61

4.6 Deleting a Policy.....	63
4.7 Applying a Policy to a Vault.....	63
4.8 Removing a Policy from a Vault.....	64
<b>5 Organizational Policy Management.....</b>	<b>66</b>
5.1 Overview.....	66
5.2 Creating an Organizational Backup Policy.....	66
5.3 Creating an Organizational Replication Policy.....	73
<b>6 Application-Consistent Backup.....</b>	<b>79</b>
6.1 Application-Consistent Backup.....	79
6.2 Changing a Security Group.....	83
6.3 Installing the Agent.....	84
6.4 Creating an Application-Consistent Backup.....	93
6.5 Uninstalling the Agent.....	94
<b>7 File Backup (Supported Conditionally).....</b>	<b>96</b>
7.1 File Backup.....	96
7.2 File Backup Process.....	98
7.3 Creating a Hybrid Cloud Backup Vault.....	100
7.4 Downloading and Installing the Agent.....	101
7.5 Configuring a File Backup Vault.....	107
7.6 Adding Directories.....	109
7.7 Creating File Backups.....	111
7.8 Restoring from a File Backup.....	111
7.9 Uninstalling the Agent.....	114
7.10 Troubleshooting Cases.....	115
<b>8 Restoring Data.....</b>	<b>118</b>
8.1 Restoring from a Cloud Server Backup.....	118
8.2 Creating an Image from a Cloud Server Backup.....	120
8.3 Restoring from a Cloud Disk Backup.....	122
8.4 Creating a Disk from a Cloud Disk Backup.....	123
8.5 Creating a File System from an SFS Turbo Backup.....	124
8.6 Restoring from a Desktop Backup.....	126
8.7 Restoring from a File Backup.....	127
8.8 Restoring from a Hybrid Cloud Backup.....	129
<b>9 (Optional) Migrating Resources from CSBS/VBS.....</b>	<b>131</b>
<b>10 Managing Tasks.....</b>	<b>135</b>
<b>11 Cloud Eye Monitoring.....</b>	<b>136</b>
11.1 Viewing Basic CBR Monitoring Data.....	136
11.2 Creating an Alarm Rule.....	138
<b>12 Recording CBR Operations Using CTS.....</b>	<b>142</b>

---

<b>13 Quotas.....</b>	<b>144</b>
<b>A Appendix.....</b>	<b>146</b>
A.1 Agent Security Maintenance.....	146
A.1.1 Changing the Password of User rdadmin.....	146
A.1.2 Changing the Password of the Account for Reporting Alarms (SNMP v3).....	147
A.1.3 Replacing the Server Certificate.....	149
A.1.4 Replacing CA Certificates.....	151

# 1 Management permissions

---

## 1.1 Creating a User and Granting CBR Permissions

This section describes how to use IAM to implement fine-grained permissions control for your CBR resources. With IAM, you can:

- Create IAM users for personnel based on your enterprise's organizational structure. Each IAM user has their own identity credentials for accessing CBR resources.
- Grant users only the permissions required to perform a given task based on their job responsibilities.
- Entrust a Huawei Cloud account or cloud service to perform efficient O&M on your CBR resources.

If your Huawei Cloud account does not require individual IAM users, skip this section.

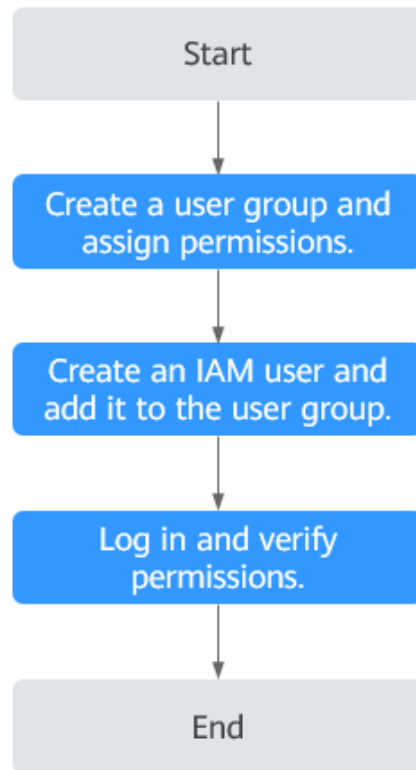
Figure [Figure 1-1](#) illustrates the procedure for granting permissions.

### Prerequisites

Learn about the permissions (see [CBR Permissions](#)) supported by CBR and choose policies or roles according to your requirements. For the system policies of other services, see [System Permissions](#).

## Process Flow

Figure 1-1 Process for granting CBR permissions



1. **Create a user group and assign permissions.**  
Create a user group on the IAM console, and assign the **CBR ReadOnlyAccess** policy to the group.
2. **Create an IAM user and add it to the user group.**  
Create a user on the IAM console and add the user to the group created in 1.
3. **Log in** and verify permissions.  
Log in to the CBR console as the created user and verify that the user has read-only permissions for CBR.
  - Choose **Service List > Cloud Backup and Recovery**. Then click **Buy Server Backup Vault** on the CBR console. If a message appears indicating that you do not have the permissions to perform the operation, the **CBR ReadOnlyAccess** policy has already taken effect.
  - Choose any other service in **Service List**. If a message appears indicating that you do not have the permissions to access the service, the **CBR ReadOnlyAccess** policy has already taken effect.

## 1.2 Creating a Custom Policy

You can create custom policies to supplement the system-defined policies of CBR. For the actions supported for custom policies, see [Permissions Policies and Supported Actions](#).

You can create custom policies in either of the following ways:

- Visual editor: Select cloud services, actions, resources, and request conditions. This does not require knowledge of policy syntax.
- JSON: Edit JSON policies from scratch or based on an existing policy.

For details about how to create custom policies, see [Creating a Custom Policy](#).

This section provides examples of common CBR custom policies.

## Example Custom Policies

- Example 1: Allowing users to create, modify, and delete vaults

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

- Example 2: Denying users to delete vaults and backups

A policy with only "Deny" permissions must be used in conjunction with other policies to take effect. If the permissions assigned to a user contain both "Allow" and "Deny", the "Deny" permissions take precedence over the "Allow" permissions.

If you need to assign permissions of the **CBR FullAccess** policy to a user but want to prevent the user from deleting vaults and backups, create a custom policy for denying vault and backup deletion, and attach both policies to the group to which the user belongs. In this way, the user can perform all operations on CBR except deleting vaults or backups. The following is an example deny policy:

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

- Example 3: Defining permissions for multiple services in a policy

A custom policy can contain the actions of multiple services that are of the global or project-level type. The following is an example policy containing actions of multiple services:

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
```



```

    "Action": [
      "cbr:vaults:create",
      "cbr:vaults:update",
      "cbr:vaults:delete"
    ]
  },
  {
    "Effect": "Allow",
    "Action": [
      "sfs:shares:createShare"
    ]
  }
]
}

```

## 1.3 Configuring Forcible Backup Policies

Forcible backup policies allow IAM users to forcibly back up data to ensure user data accuracy and security and service security.

You can configure forcible backup policies to grant permissions to IAM users to force backup, specifically:

1. [Grant permission to always enable a backup policy when it is created.](#)
2. [Grant permission to prohibit disabling of backup policies when they are modified.](#)
3. [Grant permission to force backup policy application during vault creation.](#)

### NOTICE

To ensure forcible backup, you are advised to configure all the three preceding policies.

### NOTE

You can create custom policies in either of the following ways:

- Visual editor: Select cloud services, actions, resources, and request conditions. This does not require knowledge of policy syntax.
- JSON: Create a JSON policy or edit an existing one.

For details about how to create custom policies, see [Creating a Custom Policy](#).

1. Grant permission to always enable a backup policy when it is created.

```

{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": ["cbr:policies:create"],
      "Condition": {
        "Bool": {
          "cbr:EnabledPolicy": "false"
        }
      }
    }
  ]
}

```

2. Grant permission to prohibit disabling of backup policies when they are modified.

```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": ["cbr:policies:update"],
      "Condition": {
        "Bool": {
          "cbr:EnabledPolicy": "false"
        }
      }
    }
  ]
}
```

3. Grant permission to force backup policy application during vault creation.

```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "cbr:vaults:create"
      ],
      "Condition": {
        "Null": {
          "cbr:PolicyId": [
            "true"
          ]
        }
      }
    }
  ]
}
```

# 2 Vault Management

---

## 2.1 Overview

### What Is a Vault?

CBR stores backups in vaults. Before creating a backup, you need to create at least one vault and associate the resources you want to back up with the vaults. Then the resources can be backed up to the associated vaults.

- The backups of different types of resources must be stored in different types of vaults.

### Vault Types

Vaults can be either backup vaults or replication vaults.

- Backup vaults store backups of a variety of resources, including servers and disks, and are classified into the following types:
  - **Server backup vaults:** store backups of non-database servers or database servers. You can associate servers with a server backup vault and apply a backup or replication policy to schedule automatic backups or replications.
  - **Disk backup vaults:** store only disk backups. You can associate disks with a disk backup vault and apply a backup policy to schedule automatic backups.
  - **SFS Turbo backup vaults:** store only backups of SFS Turbo file systems. You can associate file systems with an SFS Turbo backup vault and apply a backup policy to schedule automatic backups.
  - **Desktop backup vaults:** store only backups of Workspace desktops. You can associate desktops with a desktop backup vault and apply a backup policy to schedule automatic backups.
- Replication vaults: store only backups replicas. Replicas cannot be replicated again. Replication vaults for server backups include those that store only replicas of common backups and those that store replicas of application-consistent backups.

 NOTE

The protection type of a purchased vault cannot be changed. You need to delete or unsubscribe from the vault and then create a new one.

## Supported Operations

You can perform the following operations.

Table 2-1

Operation	Description
<b>Querying a vault</b>	You can set search criteria for querying desired vaults in the vault list.
<b>Deleting a vault</b>	You can delete or unsubscribe from unwanted vaults to reduce storage space usage and costs.
<b>Associating resources to a vault</b>	After a vault is created, you can associate servers, file systems, or disks with the vault to back up these resources.
<b>Dissociating resources from a vault</b>	If you no longer need to back up an associated resource, dissociate it from your vault.
<b>Migrating resources from a vault</b>	Migrating a resource means that you dissociate a resource from a vault and then associate it to another vault. All backups of the resource will be migrated to the destination vault.
<b>Expanding vault capacity</b>	You can expand the size of a vault if its total capacity is insufficient.
<b>Changing from pay-per-use to yearly/monthly</b>	If you want to use a vault for a long time, you can change its billing mode from pay-per-use to yearly/monthly to reduce cost.
<b>Changing vault specifications</b>	Server backup vaults have two specifications: those for server backups and those for application-consistent backups. If you need to back up database servers, change the specifications of the target vault from server backup to application-consistent backup.
<b>Replicating a vault across regions</b>	CBR allows you to replicate server backup vaults, SFS Turbo backup vaults, and hybrid cloud backup vaults entirely to replication vaults in a different region. Replicas of server backups can be used to create images and provision servers. Replicas of SFS Turbo backups in the destination region can be used to create file systems.
<b>Managing vault tags</b>	You can add, edit, or delete tags of a vault. Vault tags are used to filter and manage vaults only.

Operation	Description
<a href="#">Managing the enterprise projects of vaults</a>	If you need to modify the enterprise project of a vault, go to the <b>Enterprise Management</b> page to move the vault from the original enterprise project to a new one.
<a href="#">Enabling backup locking</a>	To prevent the backup data from being deleted by mistake or maliciously, you can enable backup locking for vaults to improve data security.  Once enabled, all backups in the vault enter the WORM (write once, read many) status. No one can delete the backups that are in their retention periods.

## 2.2 Viewing a Vault



You can set search criteria for querying desired vaults in the vault list.

### Prerequisites

A vault has been created.

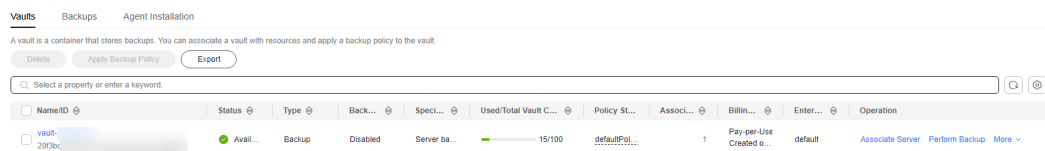
### Viewing Vault Details

**Step 1** Log in to the CBR console.

1. [Log in to the management console.](#)
2. Click  in the upper left corner and select a region.
3. Click  and choose **Storage > Cloud Backup and Recovery**. Select a backup type from the left navigation pane.

**Step 2** On the **Vaults** tab, view basic information about all vaults. Related parameters are described in the following table.

**Figure 2-1** Vault list



**Table 2-2** Basic information parameters

Parameter	Description
Name/ID	Name and ID of the vault. Click the vault name to view details about the vault.

Parameter	Description
Type	<p>Vault type, which can be backup vault or replication vault</p> <ul style="list-style-type: none"> <li>• A backup vault stores backups of servers, file systems, and disks.</li> <li>• A replication vault stores replicas of backups.</li> </ul>
Status	<p>Vault status. <a href="#">Table 2-3</a> describes the vault statuses.</p>
Backup Locking	<p>Whether backup locking is enabled for the vault.</p> <ul style="list-style-type: none"> <li>• Enabled: If backup locking is enabled, it cannot be disabled.</li> <li>• Disabled: Backup locking is disabled for the vault.</li> </ul>
Specifications	<p>Vault specifications, which can be server backup or application-consistent backup</p> <ul style="list-style-type: none"> <li>• A server backup vault stores backups of non-database servers.</li> <li>• An application-consistent backup vault stores backups of database servers.</li> </ul>
Backup Data Redundancy	<p>Redundancy policy for the backup data storage</p> <ul style="list-style-type: none"> <li>• <b>Single-AZ:</b> Backup data is stored in a single AZ, with lower costs.</li> <li>• <b>Multi-AZ:</b> Backup data is stored in multiple AZs to achieve higher reliability.</li> </ul>
Used/Total Vault Capacity (GB)	<p>Capacity used by the backups in the vault. It shows the space used by backups and the total vault capacity.</p> <p>For example: If <b>20/100</b> is displayed, 20 GB has been used out of the 100 GB vault capacity.</p>
Associated Servers/ File Systems/Disks	<p>Number of servers, file systems, and disks associated with the vault. You can click the number to view details of associated resources. The associated capacity shown on the details page is the total capacity of all the resources that have been associated with this vault.</p>
Billing Mode	<p>Billing mode of the vault, which can be <b>Yearly/Monthly</b> or <b>Pay-per-use</b>.</p> <ul style="list-style-type: none"> <li>• Yearly/monthly is a prepaid billing mode. You are billed based on the subscription duration you specify. This mode is ideal when the resource use duration is predictable. A longer subscription often means a lower cost.</li> <li>• Pay-per-use is a postpaid billing mode. You are billed based on your resource usage and you can increase or delete resources anytime. Fees are deducted from your account balance.</li> </ul>

**Step 3** On the **Vaults** tab page, set filter criteria to view specific vaults.

- Select a value from the status drop-down list to query vaults by status. [Table 2-3](#) describes the vault statuses.

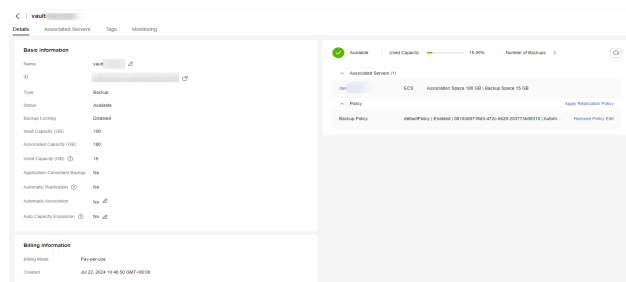
**Table 2-3** Vault statuses

Status	Attribute	Description
All statuses	--	All vaults are displayed if this value is selected.
Available	A stable state	A stable state after a vault task is complete. This state allows most of the operations.
Locked	An intermediate state	An intermediate state displayed when a capacity expansion, billing mode change, or specifications change is in progress.  If a vault is in this state, you can perform operations, such as applying a policy and associating servers, file systems, or disks. However, the following operations are not allowed on such a vault: expanding the vault capacity, changing the billing mode, and changing the vault specifications. Once those operations are complete, the vault status will become <b>Available</b> .
Deleting	An intermediate state	An intermediate state displayed when a vault is being deleted.  In this state, a progress bar is displayed indicating the deletion progress. If the progress bar remains unchanged for an extended time, an exception has occurred. Contact customer service.
Frozen	A stable state	If your resources enter a pending deletion period in the case that your subscription has expired or your account is in arrears, or if the resources do not meet security requirements, your vault is put in the <b>Frozen</b> state.  If the resources are frozen due to arrears, the state will become <b>Available</b> after you pay off the outstanding balance, and the resources can then be used normally. If you do not pay off the outstanding balance in time, the system automatically deletes the frozen resources after the retention period expires. If the resources are frozen due to security reasons, contact customer service.

Status	Attribute	Description
Error	A stable state	A vault enters the <b>Error</b> state when an exception occurs during task execution. You can click <b>Tasks</b> in the navigation pane on the left to view the error cause. If the error persists, contact customer service.

- Search a vault by its name or ID.
- Click **Search by Tag** in the upper right corner to search for vaults by tag.
  - On the displayed **Search by Tag** page, enter an existing tag key and value and click **+**. The added tag search criteria are displayed under the text boxes. Click **Search** in the lower right corner.
  - You can add a maximum of 10 tags by clicking **+**. They will be applied together for a combination search.
  - You can click **Reset** in the lower right corner to reset the search criteria.

**Step 4** Click the name of a specific vault to view vault details.



**NOTE**

- The values of used capacity and backup space are rounded off to integers. CBR will display 0 GB for any backup space less than 1 GB. For example, there may be 200 MB backup space used, but it will be displayed as 0 GB on the console.
- After changing the name of the resource associated with the vault, you need to perform an automatic or manual backup again to synchronize the change.

----End

## 2.3 Deleting a Vault

You can delete unwanted vaults to reduce storage space usage and costs.

Once you delete a vault, all backups stored in the vault will be deleted.

Only pay-per-use vaults can be deleted. Yearly/monthly vaults need to be unsubscribed by following instructions in [How Do I Unsubscribe from a Vault?](#)

### Prerequisites



- There is at least one vault.



- The vault is in the **Available** or **Error** state.
- To delete a hybrid cloud backup vault, ensure that corresponding backups have been deleted from both on premises and the cloud.

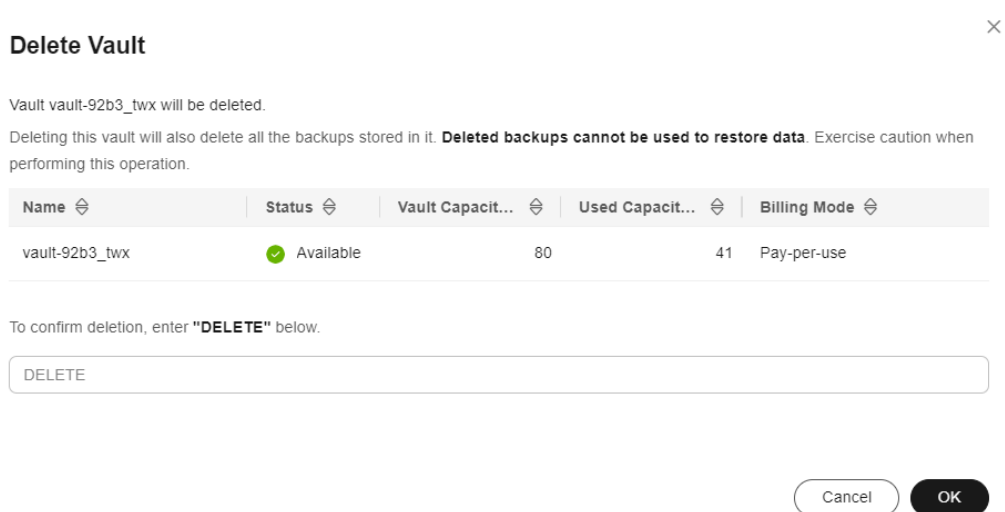
## Procedure

**Step 1** Log in to the CBR console.

1. [Log in to the management console.](#)
2. Click  in the upper left corner and select a region.
3. Click  and choose **Storage > Cloud Backup and Recovery**. Select a backup type from the left navigation pane.

**Step 2** Find the target vault and choose **More > Delete** in the **Operation** column. See [Figure 2-2](#). All backups stored in the vault will be deleted once you delete a vault.

**Figure 2-2** Deleting a vault



**Step 3** Click **OK**.

----End

## Unsubscribing from a Vault (Yearly/Monthly)

If you no longer need a vault billed in yearly/monthly mode to store backups, you can unsubscribe from the vault in either of the following methods. For details about the unsubscription rules, see [Unsubscription Rules](#).

### Method 1

- Step 1** Log in to the CBR console.
- Step 2** Click the **Vaults** tab and locate the target vault. Click **More** > **Unsubscribe** in the **Operation** column.
- Step 3** Complete the unsubscription operations as prompted.

----End

#### Method 2

- Step 1** Log in to the CBR console.
- Step 2** Click **Billing** in the top navigation bar to go to the **Billing Center** page.
- Step 3** In the left navigation pane, choose **Orders** > **Unsubscriptions** to view the yearly/monthly vaults you purchased.
- Step 4** Select an unwanted vault and click **Unsubscribe**. See [Figure 2-3](#).

**Figure 2-3** Unsubscribing from a resource package

Unsubscribe from In-Use Resources (1)		Unsubscribe from Inactive Resources (0)		Unsubscribe from Renewal Period (0)			
Conditional Unsubscription (1)		5-Day Unconditional Unsubscription (0)		Unsubscription Not Allowed (0)			
Batch Unsubscribe							
<input type="checkbox"/>	Name/ID	Service T...	Current Configurati...	Region	Effective Time	Expiration TI...	Operation
<input checked="" type="checkbox"/>	vault-ec1b 25406745-9548-4c36-a11a-...	Cloud Backup and ...	Cloud Server Backup Vau...	br-iaas-odin1	Aug 03, 2021 17:37:19 ...	24 days Sep 03, 2021 23:59:59 ...	<a href="#">Unsubscribe from Resource</a>

----End

## 2.4 Associating Resources to a Vault

If you have already associated servers, file systems, or disks when purchasing a vault, skip this step. If you need to enable automatic association, see [Automatic Association](#).

After a server backup vault, SFS Turbo backup vault, or disk backup vault is created, you can associate servers, file systems, or disks with the vault to back up these resources.

After a hybrid cloud backup vault is created, servers and disks cannot be associated with the vault, but you can synchronize backups of on-premises servers and storage systems to the cloud. For details, see [Hybrid Cloud Backup](#).

New resources cannot be associated with vaults in AZ2 of the CN North-Beijing1 region to perform backups. Resources already associated are not affected, and backups can still be performed.

### Prerequisites

- A vault can be associated with a maximum of 256 resources.
- The servers you plan to associate with a vault must have at least one disk attached.
- The vault and the resources you plan to associate with it must be in the same region.
- The total size of the resources to be associated cannot be greater than the vault capacity.



- Resources can be associated only when they are in the statuses in the table below.

**Table 2-4** Resource statuses available for association

Resource Type	Status
Cloud server	Running or Stopped
Cloud disk	Available or In-use
SFS Turbo file system	Available

## Procedure

**Step 1** Log in to the CBR console.

- Log in to the management console.**
- Click  in the upper left corner and select a region.
- Click  and choose **Storage > Cloud Backup and Recovery**. Select a backup type from the left navigation pane.

**Step 2** On a backup page, locate the target vault and click **Associate Server/Associate Disk/Associate File System**.

**Step 3** In the resource list, select the resources you want to associate with the vault. After resources are selected, they are added to the list of selected resources. See [Figure 2-4](#).


**Figure 2-4** Associating servers

### Associate Server

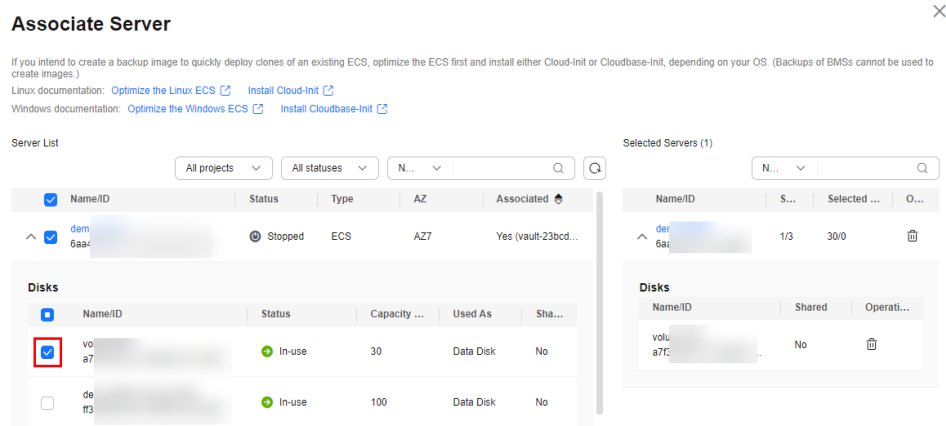
If you intend to create a backup image to quickly deploy clones of an existing ECS, optimize the ECS first and install either Cloud-Init or Cloudbase-Init, depending on your OS. (Backups of BMSs cannot be used to create images.)

Linux documentation: [Optimize the Linux ECS](#) [Install Cloud-Init](#)

Windows documentation: [Optimize the Windows ECS](#) [Install Cloudbase-Init](#)

Server List						Selected Servers (1)		
Name/ID	Status	Type	AZ	Associated	Name/ID	Selected Di...	Operati...	
<input checked="" type="checkbox"/> ecs-4137 7fac0f84-172d-46e3-a158-a05b...	<span style="color: green;">●</span> Running	ECS	AZ3	Yes (vault-8a58)	<input checked="" type="checkbox"/> ecs-4137 7fac0f84-172d-46e3-a158-...	1/1		

If you only want to associate some disks of an ECS, click the drop-down arrow on the left of the ECS name and select the disks you desire.



**Step 4** Click **OK**. In the vault list, you can view the number of associated servers/disks/file systems in the **Associated Servers/Associated Disks/Associated File Systems** column.

**NOTE**

If a new disk is attached to an associated server, CBR automatically identifies the new disk and includes the new disk in subsequent backup tasks.

----End


## Automatic Association

If you enable automatic association for a backup vault, the vault will automatically associate the unprotected resources and back them up according to the backup policy applied to the vault.

- The vault's remaining capacity should be greater than both 40 GB and the associated capacity. The vault will automatically scan and associate unprotected servers in the next backup cycle and perform backup. Remaining capacity of a vault = Total capacity of the vault - Capacity of resources associated with the vault. You can obtain the vault's total capacity and associated capacity in the **Basic Information** area on the details page of the vault. For example, if you have an 800-GB server backup vault and it has been associated with two 100-GB servers, its remaining capacity is 600 GB (800 GB - 200 GB). In this case, the vault will automatically associate unprotected servers in the next backup cycle and perform backup.
- If multiple vaults are enabled with automatic association, CBR scans their backup policies and associates resources with the vault whose next scheduled backup time is the earliest.
- If the capacity of the first selected vault is used up, resources will be associated with the vault whose next scheduled backup time is the second earliest.
- If a backup policy with the earliest scheduled backup time is applied to more than one vault, CBR randomly associates the resources with one of these vaults.

- If a vault has automatic association enabled but has no backup policy applied, no resources will be automatically associated with this vault. You can manually associate unprotected resources.
- After automatic association is disabled for a vault, the vault stops automatically scanning for unprotected resources. Associated resources are not affected.

**Step 1** Log in to the CBR console.

1. Log in to the management console.
2. Click  in the upper left corner and select a region.
3. Choose **Storage > Cloud Backup and Recovery**.

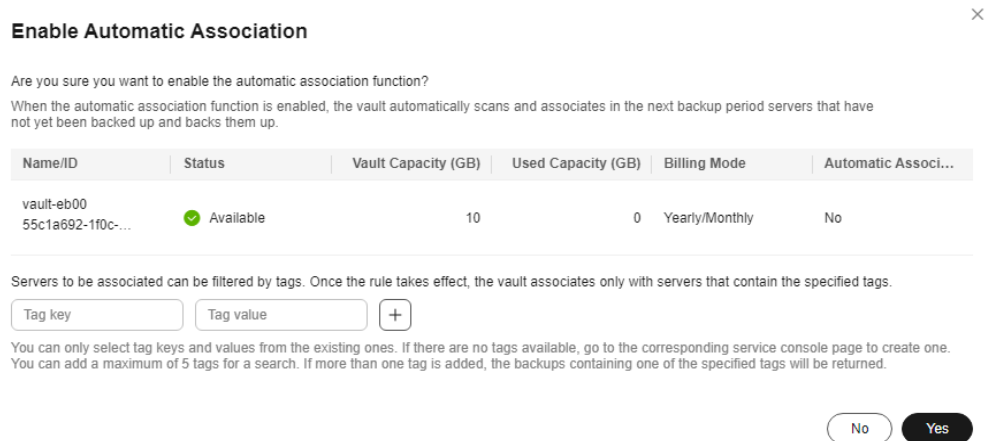
**Step 2** On any backup page, locate the target vault.

**Step 3** Choose **More > Enable Automatic Association** in the **Operation** column of the vault.

You can filter unprotected resources by tag. If a tag is selected, only unprotected resources with the specified tag will be associated with the vault. Or, all unprotected resources will be associated.

If no tag is available, you can create tags on the corresponding resource page. You can search for vaults by specifying a maximum of 5 tags at a time. If you select more than one tag, the vaults with any of the specified tags will be returned.

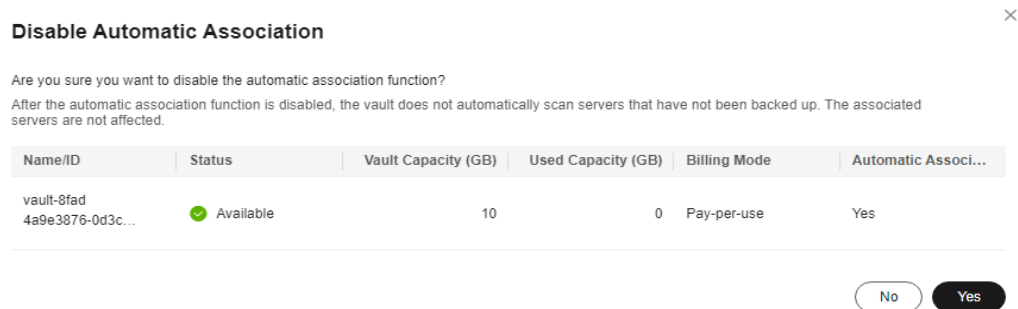
**Figure 2-5** Enabling automatic association



**Step 4** Check that **Automatic association** is displayed in the **Associated Servers** column of the vault list.

**Step 5** (Optional) If automatic association is not required, choose **More > Disable Automatic Association** in the **Operation** column of the vault. See [Figure 2-6](#).

**Figure 2-6** Disabling automatic association



----End

## 2.5 Dissociating Resources from a Vault



If you no longer need to back up an associated resource, dissociate it from your vault.

After a resource is dissociated, the vault's backup or replication policy no longer applies to the resource. In addition, all manual and automatic backups of this resource will be deleted. Deleted backups cannot be used to restore data.

Dissociating a resource from a vault does not affect the performance of services on the resource.

### Procedure

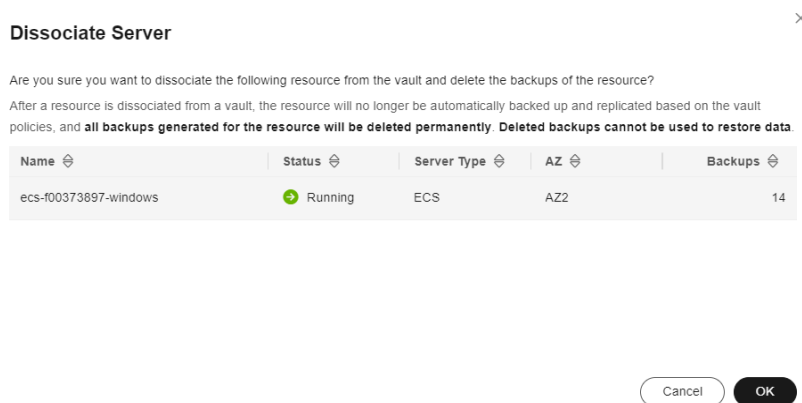
**Step 1** Log in to the CBR console.

1. [Log in to the management console.](#)
2. Click  in the upper left corner and select a region.
3. Click  and choose **Storage > Cloud Backup and Recovery**. Select a backup type from the left navigation pane.

**Step 2** Find the target vault and click its name.

**Step 3** In this example, we will be using the **Cloud Server Backups** page to illustrate the process. Click the **Associated Servers** tab. Find the target server and click **Dissociate** in the **Operation** column. See [Figure 2-7](#).

**Figure 2-7** Dissociating a server



**Step 4** Confirm the information and click **Yes**.

----End

## 2.6 Migrating Resources from a Vault



Migrating a resource means that you dissociate a resource from a vault and then associate it to another vault. All backups of the resource will be migrated to the destination vault.

### Notes and Constraints

- Resources can be migrated only when the source and destination vaults are in the **Available** or **Locked** state.
- Resources can be migrated only when no task is being executed in the source and destination vaults.
- The remaining capacity of the destination vault must be greater than the size of resource backups to be migrated.
- Cross-account resource migration is currently not supported.
- The source and destination vaults must be in the same region.
- The source and destination vaults for resource migration must be of the same types. For example, resources in a server backup vault can be migrated to another server backup vault, but cannot be migrated to another disk backup vault.

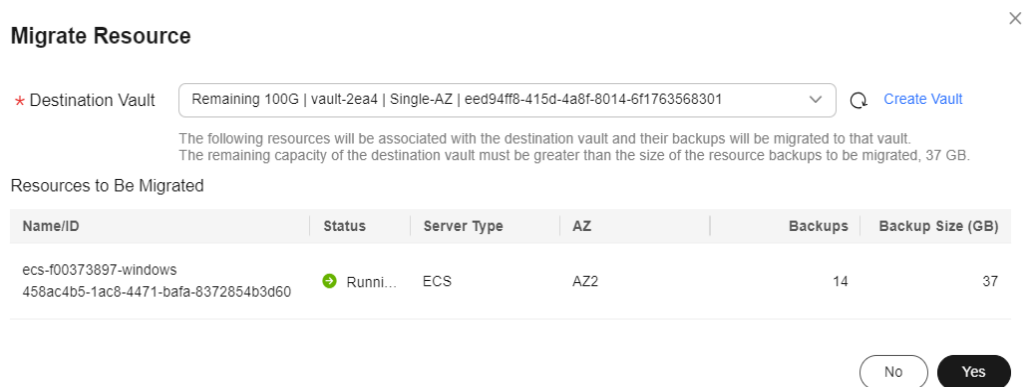
### Procedure

**Step 1** Log in to the CBR console.

1. [Log in to the management console](#).
2. Click  in the upper left corner and select a region.
3. Click  and choose **Storage > Cloud Backup and Recovery**. Select a backup type from the left navigation pane.

- Step 2** Find the target vault and click its name. In this example, we will be using the **Cloud Server Backups** page to illustrate the process.
- Step 3** Click the **Associated Servers** tab. Find the target server and click **Migrate** in the **Operation** column. See [Figure 2-8](#).

**Figure 2-8** Migrating a resource





- Step 4** Select the destination vault and click **Yes**.
- Step 5** View the migration progress on the **Tasks** page. If **Status** changes to **Successful**, the resource has been migrated.
- Step 6** Go to the destination vault to confirm that the resource has been associated and all its backups have been migrated.

----End

## 2.7 Expanding Vault Capacity

You can expand the size of a vault if its total capacity is insufficient.

### Procedure

- Step 1** Log in to the CBR console.
1. [Log in to the management console](#).
  2. Click  in the upper left corner and select a region.
  3. Click  and choose **Storage > Cloud Backup and Recovery**. Select a backup type from the left navigation pane.
- Step 2** Find the target vault and choose **More > Expand Capacity** in the **Operation** column. See [Figure 2-9](#).



**Figure 2-9** Expanding vault capacity

< | **Expand Server Backup V...**

---

Current Configuration

Vault Name	vault-8a58	Region	CN-Hong Kong
Vault ID	0711d0e0-1ee5-49ff-91e0-82c6d4804cdb	Backup Type	Server backup

---

Billing Mode

Pay-per-use(Current Price:\$0.0045 USD/hour)

Current Capacity (GB)

80

Used Capacity (GB)

0

Add Capacity (GB)

New Capacity (GB)

90

**Step 3** Enter the capacity to be added. The minimum value is 1.

**Step 4** Click **Next**. Confirm the settings and click **Submit**.

**Step 5** Return to the vault list and check that the capacity of the vault has been expanded.

----End

## Auto Capacity Expansion

If you want a vault to be automatically expanded when its capacity is used up, enable auto capacity expansion.

If this function is enabled, the vault capacity will be automatically expanded to 1.25 times its current capacity when its capacity is used up.


Auto capacity expansion does not take effect if it is enabled after the vault is full.


Yearly/Monthly vaults do not support auto capacity expansion.

### NOTE

Auto capacity expansion does not take effect if it is enabled after the vault is full.

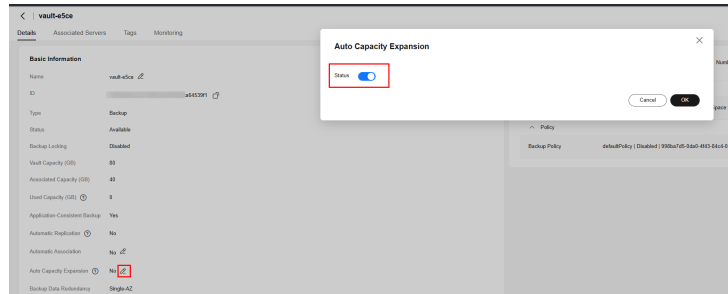
**Step 1** Log in to the CBR console.

1. [Log in to the management console](#).
2. Click  in the upper left corner and select a region.

3. Click  and choose **Storage > Cloud Backup and Recovery**. Select a backup type from the left navigation pane.

**Step 2** Find the target vault and click its name.

**Step 3** On the vault details page, enable **Auto Capacity Expansion**.



**Step 4** (Optional) Disable **Auto Capacity Expansion** if you no longer need this function.



----End

## 2.8 Reducing Vault Capacity

You can reduce the size of a vault if its total capacity is too much for you. Only pay-per-use vaults can have their capacity reduced.

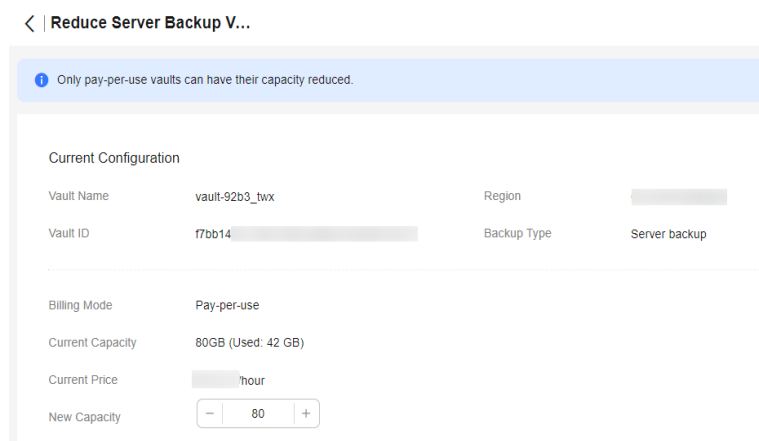
### Procedure

**Step 1** Log in to the CBR console.

1. [Log in to the management console](#).
2. Click  in the upper left corner and select a region.
3. Click  and choose **Storage > Cloud Backup and Recovery**. Select a backup type from the left navigation pane.

**Step 2** Find the target vault and choose **More > Reduce Capacity** in the **Operation** column. See [Figure 2-10](#).

**Figure 2-10** Reducing vault capacity



- Step 3** Enter the new capacity. Ensure that the new capacity is greater than 125% of the used capacity. Or, the capacity reduction will fail.
- Step 4** Click **Next**. Confirm the settings and click **Submit**.
- Step 5** Return to the vault list and check that the capacity of the vault has been reduced.
- End

## 2.9 Changing from Pay-per-Use to Yearly/Monthly



- Yearly/monthly is a prepaid billing mode. You are billed based on the subscription duration you specify. This mode is ideal when the resource use duration is predictable. A longer subscription often means a lower cost.
- Pay-per-use is a postpaid billing mode. You are billed based on your resource usage and you can increase or delete resources anytime. Fees are deducted from your account balance.

If you want to use a vault for a long time, you can change its billing mode from pay-per-use to yearly/monthly to reduce cost.

### Prerequisites

The vault's billing mode is pay-per-use.

### Procedure

- Step 1** Log in to the CBR console.
1. [Log in to the management console](#).
  2. Click  in the upper left corner and select a region.
  3. Click  and choose **Storage > Cloud Backup and Recovery**. Select a backup type from the left navigation pane.
- Step 2** Find the target vault and choose **More > Change Billing Mode** in the **Operation** column.
- Step 3** Select the required duration for the vault, confirm information, and click **Pay**.
- Step 4** Return to the vault list. You can see that the vault's **Billing Mode** has changed to **Yearly/Monthly**.
- End

## 2.10 Changing Vault Specifications

Server backup vaults have two specifications: those for server backups and those for application-consistent backups.



- Server backups are backups of non-database servers.
- Application-consistent backups are backups of database servers.

If you need to back up database servers, change the specifications of the target vault from server backup to application-consistent backup.

You can only change the specifications of a vault from server backup to application-consistent backup, but not the other way around.

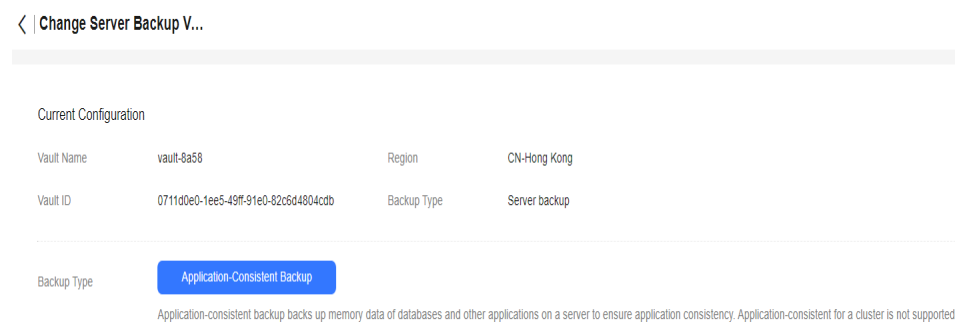
## Procedure

**Step 1** Log in to the CBR console.

1. [Log in to the management console](#).
2. Click  in the upper left corner and select a region.
3. Click  and choose **Storage > Cloud Backup and Recovery**. Select a backup type from the left navigation pane.

**Step 2** On the **Cloud Server Backups** page, find the target vault. Choose **More > Change Specifications** in the **Operation** column of the vault. See [Figure 2-11](#).

**Figure 2-11** Changing specifications



**Step 3** **Application-Consistent Backup** is preset for **Backup Type**. Click **Next**.

**Step 4** Click **Pay** and complete the payment. The system automatically changes the vault specifications.

----End

## 2.11 Replicating a Vault Across Regions

### Scenarios

CBR allows you to **replicate all backups** in a server backup vault and an SFS Turbo backup vault **to replication vaults in other regions of the same account**. Replicas of server backups in the destination region can be used to create images and provision servers. Replicas of SFS Turbo backups in the destination region can be used to create file systems to quickly deploy services across regions.

There are two methods available for replicating a vault.

- Manual replication: Select a backup vault and manually replicate it.
- Policy-based replication: Configure a replication policy to periodically replicate backups that have not been replicated or failed to be replicated to the destination region.

## Constraints

- Disk backup vaults cannot be replicated to other regions.
- Backup data can be replicated to vaults in different regions. Any traffic costs associated with this operation will be attributed to the source region. Backup replicas occupy the replication vault space.
- A server backup vault can be replicated only when it contains at least one backup that meets all the following conditions:
  - a. The backup is an ECS backup.
  - b. The backup contains system disk data.
  - c. The backup is in the **Available** state.
- An SFS Turbo backup can be replicated only when it meets all the following conditions:
  - a. It is generated for an SFS Turbo file system.
  - b. It is in the **Available** state.
- Only backup vaults of the same type can be replicated. Replicated vaults cannot be replicated again but their replicas can be used to create images or SFS Turbo file systems.
- A backup vault can be replicated to different destination regions. For manual and policy-based vault replication, a vault can only be replicated to a destination region once. It cannot be replicated to that region again, even if its backups have been deleted.
- Only vaults of the same type can be selected as destination vaults. For example, if you want to replicate server backups to a different region, select a server backup vault (**Protection Type** set to **Replication (cross-region)**) in that region.
- Only replication-supported regions can be selected as destination regions. For details, see [Table 2-5](#)



**Table 2-5** Replication-supported regions

Source Region	Destination Region	Description
CN North-Ulanqab1	CN North-Beijing4, CN East-Shanghai1, and CN South-Guangzhou	-
CN South-Shenzhen	CN North-Beijing4	-
CN Southwest-Guiyang1	CN North-Beijing 4 and CN East-Shanghai1	-

Source Region	Destination Region	Description
CN North-Beijing1	CN North-Beijing4, CN East-Shanghai2, CN East-Shanghai1, and CN South-Guangzhou	-
CN North-Beijing4	CN North-Ulanqab1, CN South-Shenzhen, CN Southwest-Guiyang1, CN North-Beijing1, CN East-Shanghai2, CN East-Shanghai1, and CN South-Guangzhou	-
CN East-Shanghai2	CN North-Beijing1, CN North-Beijing4, CN East-Shanghai1, and CN South-Guangzhou	-
CN East-Shanghai1	CN North-Ulanqab1, CN Southwest-Guiyang1, CN North-Beijing1, CN North-Beijing4, CN East-Shanghai2, and CN South-Guangzhou	-
CN South-Guangzhou	CN North-Ulanqab1, CN North-Beijing1, CN North-Beijing4, CN East-Shanghai2, and CN East-Shanghai1	-
CN-Hong Kong, AP-Bangkok, and AP-Singapore	CN-Hong Kong, AP-Bangkok, and AP-Singapore	Vaults can be replicated from one region to another.
LA-Mexico City2	LA-Sao Paulo1	
LA-Sao Paulo1	LA-Mexico City2, LA-Santiago	
LA-Santiago	LA-Sao Paulo1, LA-Lima1	
LA-Lima1	LA-Santiago	

## Procedure

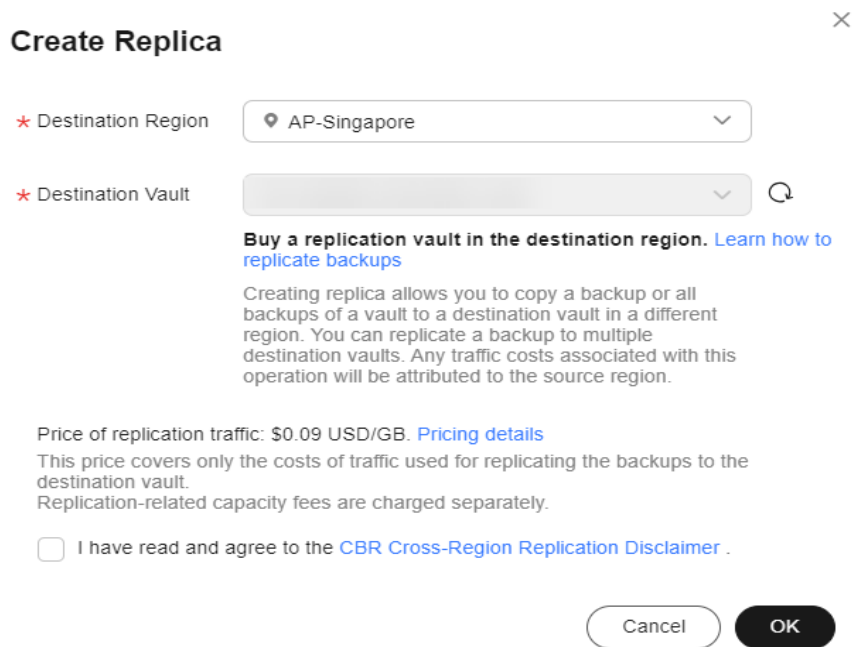
**Step 1** Log in to the CBR console.

1. [Log in to the management console](#).
2. Click  in the upper left corner and select a region.
3. Click  and choose **Storage > Cloud Backup and Recovery**. Select a backup type from the left navigation pane.

**Step 2** On the **Vaults** tab, find the target backup vault.

**Step 3** Choose **More > Create Replica** in the **Operation** column of the vault. See [Figure 2-12](#).

**Figure 2-12** Creating a replica



**Step 4** In the displayed dialog box, configure the parameters as described in [Table 2-6](#).

**Table 2-6** Parameter description

Parameter	Description
Destination Region	<p>Region to which the vault is replicated</p> <p>Only the regions that support replication will be displayed.</p> <ul style="list-style-type: none"> <li>• If the selected region contains only one project, you can directly select the region name.</li> <li>• If the selected region has multiple projects, the default project of the region is selected. You can select another project if needed.</li> </ul>
Destination Vault	A replication vault in the destination region

**Step 5** Click **OK**.

**Step 6** After the replication is complete, you can switch to the destination region to view generated replicas. For details, see [Viewing a Vault](#). You can then use replicas to create images.

----End

## 2.12 Managing Vault Tags



You can add, edit, or delete tags of a vault. Vault tags are used to filter and manage vaults only.

### Constraints

If your organization has enabled the tag policy type for CBR and has a tag policy attached, you must comply with the tag policy rules when creating vaults, otherwise vaults may fail to be created. Contact the organization administrator to learn more about tag policies.

### Procedure

**Step 1** Log in to the CBR console.

1. [Log in to the management console.](#)
2. Click  in the upper left corner and select a region.
3. Click  and choose **Storage > Cloud Backup and Recovery**. Select a backup type from the left navigation pane.

**Step 2** On the **Vaults** tab, click the name of the target vault and then select the **Tags** tab.

- Adding a tag
  - a. Click **Add Tag** in the upper left corner.
  - b. In the displayed dialog box, enter the key and value of the new tag.  
Tags are key-value pairs, which are used to identify, classify, and search for vaults. You can add a maximum of tags for a vault, and vault tags are only used for vault search and management.

[Table 2-7](#) describes the parameters of a tag.

**Table 2-7** Tag parameter description

Parameter	Description	Example Value
Key	Tag key. Each tag of a vault has a unique key. You can customize a key. A tag key: <ul style="list-style-type: none"> <li>▪ Can contain 1 to 36 Unicode characters.</li> <li>▪ Can contain only letters, digits, hyphens (-), and underscores (_).</li> </ul>	Key_0001



Parameter	Description	Example Value
Value	<p>A tag value can be repetitive or left blank. A tag value:</p> <ul style="list-style-type: none"> <li>▪ Can contain 0 to 43 Unicode characters.</li> <li>▪ Can contain only letters, digits, hyphens (-), and underscores (_).</li> </ul>	Value_000 1

- c. Click **OK**.
- Editing a tag
  - a. In the **Operation** column of the tag that you want to edit, click **Edit**.
  - b. In the displayed **Edit Tag** dialog box, enter a new tag value. [Table 2-7](#) describes the parameters.
  - c. Click **OK**.
- Deleting a tag
  - a. In the **Operation** column of the tag that you want to delete, click **Delete**.
  - b. In the displayed dialog box, confirm the deletion information.
  - c. Click **Yes**.

----End

## 2.13 Managing the Enterprise Projects of Vaults

If you need to modify the enterprise project of a vault, go to the **Enterprise Management** page to move the vault from the original enterprise project to a new one.

### Procedure

- Step 1** Click **Enterprise** on the upper right of console page. By default, the **Overview** page of Enterprise Management is displayed.
- Step 2** In the navigation pane of the **Enterprise Management** page, choose **Project Management**.
- Step 3** Locate the enterprise project from which the vault will be removed. Click **View Resources** in the **Operation** column. On the **Resources** tab page, view resources in the current enterprise project.
- Step 4** Select the resources to be removed and click **Remove**. On the displayed page, select **Independent resources** for **Mode**.
- Step 5** Select the destination enterprise project to which the vault is to be added and click **OK**.

After the vault is removed from the enterprise project, you can view it in the resource list of the destination enterprise project.

----End

## 2.14 Enabling Backup Locking

### Scenarios

To prevent the backup data from being deleted by mistake or maliciously, you can enable backup locking for vaults to improve data security.

Once enabled, all backups in the vault enter the WORM (write once, read many) status. No one can delete the backups that are in their retention periods.

This section describes how to enable backup locking for a vault. You can also enable it when purchasing a vault.

#### NOTE



- Backup locking does not affect normal backup, restoration, and replication operations.
- Manual backups are not affected by backup locking and can be manually deleted.
- If you enable backup locking, set **Type** of **Retention Rule** to **Time period**. In this way, even if you modify the retention rule of the policy, backups with the original policy applied will be automatically deleted based on the original expiration time, backups with the new policy applied will be retained based on the new retention rule.

### Constraints

- Backup locking cannot be disabled after it is enabled.
- After backup locking is enabled, associated resources cannot be dissociated and files cannot be migrated.
- After backup locking is enabled, policy-based backups can only be deleted after they expire. You cannot manually delete them.
- After backup locking is enabled, pay-per-use vaults cannot be deleted if they contain backups, but yearly/monthly vaults can be unsubscribed from.

### Enabling Backup Locking for an Existing Vault

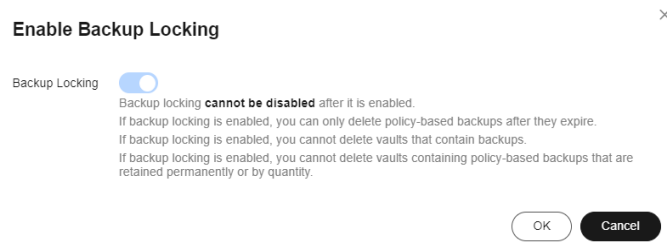
**Step 1** Log in to the CBR console.

1. [Log in to the management console](#).
2. Click  in the upper left corner and select a region.
3. Click  and choose **Storage > Cloud Backup and Recovery**. Select a backup type from the left navigation pane.

**Step 2** On any backup page, locate the target vault and choose **More > Enable Backup Locking** in the **Operation** column.

**Step 3** In the displayed dialog box, click **OK** to enable backup locking.

**Figure 2-13** Backup locking



**Step 4** Click **OK**.

The vault list is displayed, and you can see that the value in the **Back Locking** column is **Enabled**.

----**End**

# 3 Backup Management

---

## 3.1 Overview

### What Is a Backup?

A backup is a copy of a particular chunk of data and is usually stored elsewhere so that it may be used to restore the original data in the event of data loss. It can be generated either manually by a one-off backup task or automatically by a periodic backup task.

A one-off backup task is manually created and is executed only once. Periodic backup tasks are automatically executed based on a user-defined backup policy.

- A one-off backup is named **manualbk\_**xxxx and can be user- or system-defined.
- A periodic backup is named **autobk\_**xxxx by CBR.

### Cloud Backup Types

There are the following types of backups:

- Cloud disk backup: provides snapshot-based backups for EVS disks.
- Cloud server backup: uses the consistency snapshot technology to protect data for ECSs and BMSs. Backups of non-database servers are non-database server backups, and those of database servers are application-consistent backups.
- SFS Turbo backup: backs up data of SFS Turbo file systems.
- Desktop backup: backs up data of Workspace desktops.

**Table 3-1** Differences among the backup types

Item	Cloud Server Backup	Cloud Disk Backup	SFS Turbo Backup	Desktop Backup
What to back up	All disks (system and data disks) on a server or part of disks and cloud servers (with applications)	One or more specific disks (system or data disks)	SFS Turbo file systems	Entire Workspace desktop systems, including all disks
When to use	You want to back up entire cloud servers.	You want to back up only data disks.	You want to back up entire SFS Turbo file systems.	You want to back up entire Workspace desktops.
Advantages	All disks on a server are backed up at a time.	Only data of specific disks is backed up, which costs less than backing up an entire server.	File system data and their backups are stored separately, and the backups can be used to create new file systems.	Desktop data and their backups are stored separately, and the backups can be used to create new desktops.

## Backup Mechanism

CBR in-cloud backup offers block-level backup. The first backup is a full backup and backs up all used data blocks. For example, if a disk size is 100 GB and 40 GB has been used, only the 40 GB of data is backed up. An incremental backup backs up only the data changed since the last backup to save the storage space and backup time.

When a backup is deleted, data blocks will not be deleted if they are depended on by other backups, ensuring that other backups can still be used for restoration. Both a full backup and an incremental backup can be used to restore data to a given backup point in time.

When creating a backup of a disk, CBR also creates a snapshot for it. CBR keeps only the latest snapshot. Every time it creates a new snapshot during backup, it deletes the old snapshot.

CBR stores backups in OBS to ensure data security.

## Backup Options

CBR supports one-off backup and periodic backup. A one-off backup task is manually created and is executed only once. Periodic backup tasks are automatically executed based on a user-defined backup policy.

**Table 3-2** compares the two backup options.

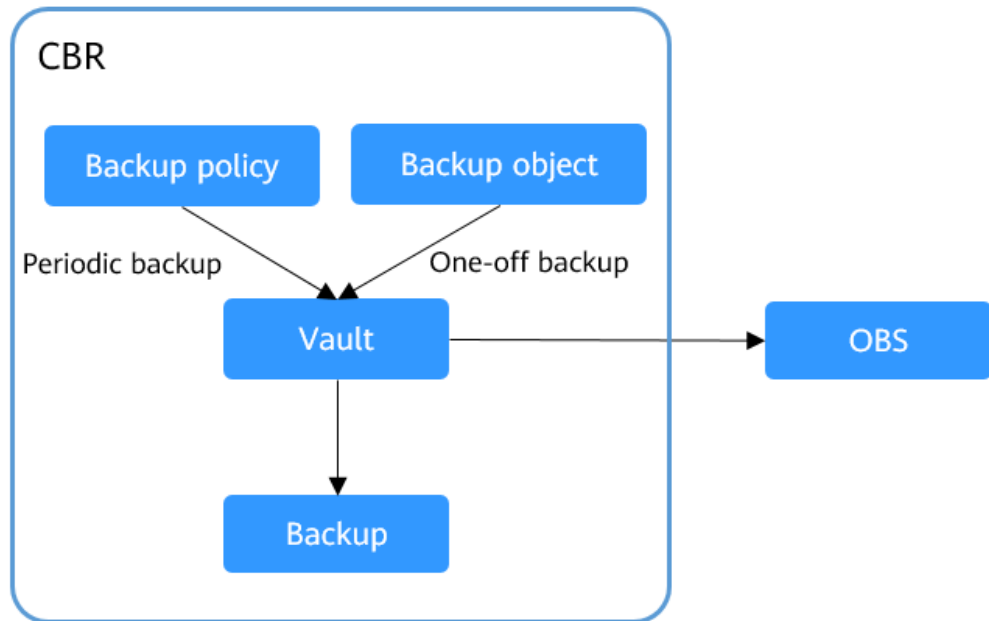
**Table 3-2** One-off backup and periodic backup

Item	One-Off Backup	Periodic Backup
Backup policy	Not required	Required
Number of backup tasks	One manual backup task	Periodic tasks triggered by a preset backup policy
Backup name	User-defined backup name, which is <b>manualbk_xxxx</b> by default	System-assigned backup name, which is <b>autobk_xxxx</b> by default
Backup mode	The first backup is a full backup and the consecutive backups are incremental.	The first backup is a full backup and the consecutive backups are incremental.
Application scenario	Executed before patching or upgrading the OS or upgrading an application. A one-off backup can be used for restoration if the patching or upgrading fails.	Executed for routine maintenance. The latest backup can be used for restoration if an unexpected failure or data loss occurs.

You can also use the two backup options together if needed. For example, you can associate resources with a vault and apply a backup policy to the vault to execute periodic backup for all the resources in the vault. Additionally, you can perform a one-off backup for the most important resources to enhance data security. **Figure 3-1** shows the use of the two backup options.

Theoretically, you can create as many backups for a resource as needed. This number is not limited.

**Figure 3-1** Use of the two backup options



### Supported Operations

You can perform the following operations.

**Table 3-3**

Operation	Description
<b>Viewing a backup</b>	In the backup list, you can set search criteria to filter backups and view their details. The results contain backup tasks that are running or have completed.
<b>Sharing a backup</b>	You can share a server or disk backup with projects of other accounts. Shared backups can be used to create servers or disks.
<b>Deleting a backup</b>	You can delete unwanted backups to reduce space usage and costs.
<b>Replicating a backup across regions</b>	CBR enables you to replicate backups of server backup vaults, SFS Turbo backup vaults, and hybrid cloud backup vaults from one region to another.

## 3.2 Viewing a Backup

### Scenario



In the backup list, you can set search criteria to filter backups and view their details. The results contain backup tasks that are running or have completed.

## Prerequisites

At least one backup task has been created.

## Procedure

**Step 1** Log in to the CBR console.

1. [Log in to the management console](#).
2. Click  in the upper left corner and select a region.
3. Click  and choose **Storage > Cloud Backup and Recovery**. Select a backup type from the left navigation pane.

**Step 2** Click the **Backups** tab and set filter criteria to view the backups.

The last active time displayed in the backup client list shows the last time the Agent was detected normal.

- You can search for backups by selecting a status from the **All statuses** drop-down list above the backup list. [Table 3-4](#) describes the backup statuses.

**Table 3-4** Backup statuses

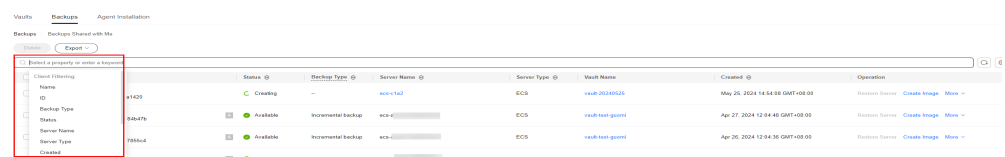
Status	Status Attribute	Description
All statuses	--	All backups are displayed if this value is selected.
Available	A stable state	A stable state of a backup after the backup is created, indicating that the backup is currently not being used. This state allows most of the operations.
Creating	An intermediate state	An intermediate state of a backup from the start of a backup job to the completion of this job. In the <b>Tasks</b> list, a progress bar is displayed for a backup task in this state. If the progress bar remains unchanged for an extended time, an exception has occurred. Contact customer service.
Restoring	An intermediate state	An intermediate state when using the backup to restore data. In the <b>Tasks</b> list, a progress bar is displayed for a restoration task in this state. If the progress bar remains unchanged for an extended time, an exception has occurred. Contact customer service.



Status	Status Attribute	Description
Deleting	An intermediate state	An intermediate state from the start of deleting the backup to the completion of deleting the backup. In the <b>Tasks</b> list, a progress bar is displayed for a deletion task in this state. If the progress bar remains unchanged for an extended time, an exception has occurred. Contact customer service.
Error	A stable state	A backup enters the <b>Error</b> state when an exception occurs. A backup in this state cannot be used for restoration, and must be deleted manually. If manual deletion fails, contact customer service.

- You can search for backups by clicking **Advanced Search** above the backup list.  
You can search by specifying a backup name, backup ID, backup status, server name, server ID, server type, protection type, whether the backup is a replica, or the creation date.

**Figure 3-2** Filtering backups



- You can search for backups by selecting a project from the **All projects** dropdown list in the upper right corner of the backup list.
- Click **Export** above the backup list to export the cloud backup list.

**Step 3** Click the backup name to view details about the backup.

----End

### 3.3 Changing a Backup Name



You can change the name of a created backup for identification purposes. Both the names of manual and automatic backups can be changed.

#### Prerequisites

There is at least one backup.


#### Procedure

**Step 1** Log in to the CBR console.

1. [Log in to the management console.](#)
2. Click  in the upper left corner and select a region.
3. Click  and choose **Storage > Cloud Backup and Recovery**. Select a backup type from the left navigation pane.





**Step 2** Click the **Backups** tab and set filter criteria to view the backups.

**Step 3** Click the name of the target backup to go to the backup details page.

**Step 4** Click  next to the backup name.


**Figure 3-3** Changing backup name

**Basic Information**

Name	<input type="text" value="autobk_test_001"/>  
ID	 
Status	Available
AZ	AZ1

 **NOTE**

- Duplicate backup names are allowed.
- CBR automatically adds the **autobk\_** prefix for you to differentiate automatic backups from manual backups. You are advised to retain the **autobk\_** prefix.
- If the name of a backup is changed and prefix deleted, you may find it difficult to distinguish automatic backups from manual backups.
- CBR can always differentiate automatic backups from manual backups no matter you delete the prefix or not. Automatic backups expire based on the retention rule of the backup policy.

**Step 5** Enter a name you want and click  .

----End

## 3.4 Sharing a Backup

### Scenarios

You can share server or disk backups with projects of other accounts. Shared backups can be used to create servers or disks.

### Context

#### Sharer

- Backups can only be shared among projects of accounts in the same region. They cannot be shared across regions.
- Backups cannot be shared across regions. Account to which a backup is shared must be in the same region as the backup.
- When a sharer deletes a shared backup, the backup will also be deleted from the recipient's account, but the disks or servers previously created using the backup will be retained.
- When an encrypted backup is shared, the encryption key must be shared with the recipient so that the recipient can use the shared backup.

---

#### NOTICE

- For details about how to share an encryption key, see [creating a grant](#) of Data Encryption Workshop (DEW) or the [creating a resource share](#) of Resource Access Manager (RAM). To obtain the recipient **Account ID**, hover over the username and choose **My Credentials**. On the **API Credentials** page that is displayed, the **Account ID** is shown,
- Cloud disk backup encryption depends on an agency created that grants KMS access permissions to EVS. If the disk to be backed up is encrypted, the disk backup generated will be an encrypted backup. The encryption attribute of backups cannot be changed.

---

#### Recipient



- A recipient must have at least one backup vault to store the accepted shared backup, and the vault's remaining space must be greater than the size of the backup to be accepted.
- A recipient can choose to accept or reject a backup. After accepting a backup, the recipient can use the backup to create new servers or disks.
- When a sharer deletes a shared backup, the backup will also be deleted from the recipient's account, but the disks or servers previously created using the backup will be retained.

#### NOTE

The retention rule of the backup shared to the recipient is the same as that of the original backup set the initiator.

## Procedure

**Step 1** Log in to the CBR console.

1. [Log in to the management console](#).
2. Click  in the upper left corner and select a region.
3. Click  and choose **Storage > Cloud Backup and Recovery**. Select a backup type from the left navigation pane.

**Step 2** Click the **Backups** tab and set filter criteria to view the backups.

**Step 3** Locate the target backup and choose **More > Share Backup** in the **Operation** column.

The backup name, server or disk name, backup ID, and backup type are displayed.

- Sharing a backup

**Figure 3-4** Share Backup

**Share Backup**

A backup that is shared with a project can be used in the project to create new disks.

Backup Name: autobk\_5a9a

Backup ID: [Redacted]

Server Name: [Redacted]

Backup Type: ECS

Region: [Redacted]

Type:  Share Backup  Cancel Sharing

Projects: Enter the project ID of a recipient. [Learn how to obtain a project ID.](#)

[Text Input Field]

[Add]

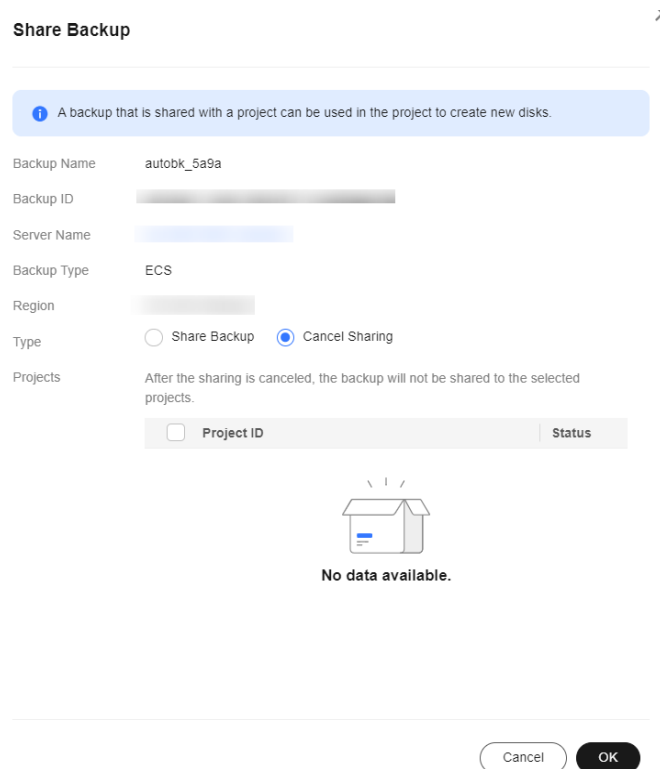
Added Projects: You can share the backup with 10 more projects.

Project ID	Operation

[Cancel] [OK]

1. Click the **Share Backup** tab.
  2. Enter the project ID of the recipient. A project ID indicates a tenant's resources. For details about how to obtain a project ID, see [Obtaining a Project ID](#).
  3. Click **Add**.  
The project ID to be added will be displayed in the list. You can add multiple project IDs. A backup can be shared to a maximum of 10 projects.
  4. Click **OK**.
- Canceling sharing
1. Select **Cancel sharing** for **Type**, select the projects you want to cancel sharing, and click **OK**. See [Figure 3-5](#).

**Figure 3-5** Cancel Sharing



----End

## Procedure

**Step 1** Log in to the CBR console.

1. **Log in to the management console.**
2. Click in the upper left corner and select a region.
3. Click and choose **Storage > Cloud Backup and Recovery**. Select a backup type from the left navigation pane.

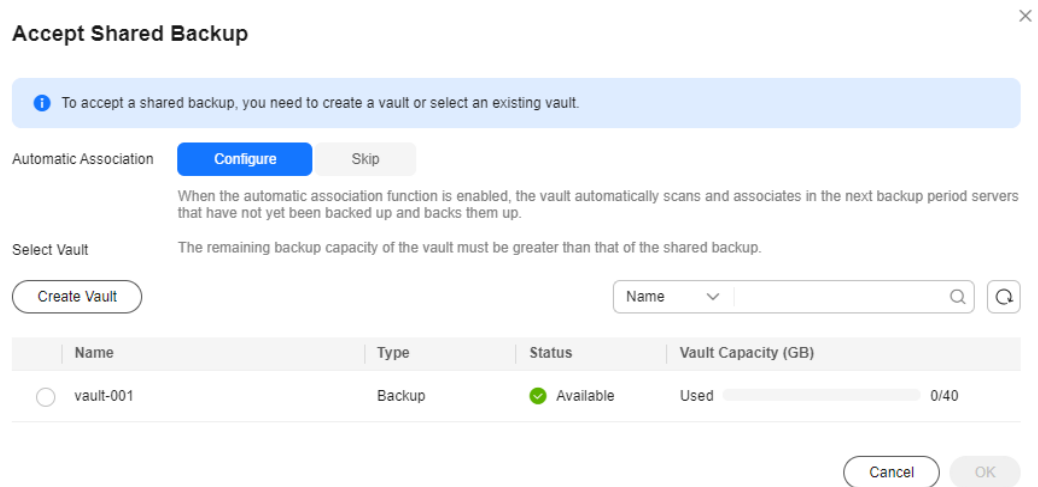
**Step 2** Click the **Backups** tab and then click **Backups Shared with Me**.

**Step 3** Ensure that the recipient has at least one backup vault before accepting the shared backup. For how to purchase a backup vault, see [Purchase a Vault](#).

**Step 4** Click **Accept**. On the displayed page, select the vault used to store the shared backup. Ensure that the vault's remaining capacity is greater than the backup size. See [Figure 3-6](#).

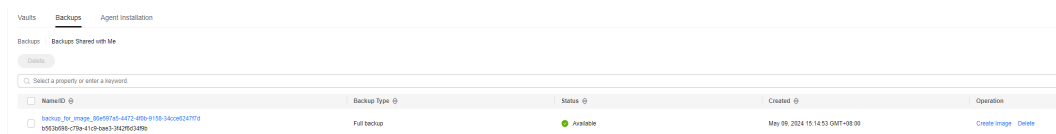
**Automatic Association:** Determine whether to enable automatic association for the vault. If you select **Configure**, the vault automatically scans and associates in the next backup period servers that have not been backed up and performs backup.

**Figure 3-6** Accepting a shared backup



**Step 5** View the shared backup you accepted in the backup list. See [Figure 3-7](#).

**Figure 3-7** Shared backup accepted



----End

## 3.5 Deleting a Backup

You can delete unwanted backups to reduce space usage and costs.

Deleting a backup from a hybrid cloud backup vault does not affect the corresponding backup on-premises, and vice versa.

If a backup has been used to create an image, the backup cannot be deleted. In this case, delete the image first based on the instructions in [Deleting Images](#).

CBR supports manual deletion of backups and automatic deletion of expired backups. The latter is executed based on the backup retention rule in the backup policy. For details, see [Creating a Backup Policy](#).

 NOTE



- Backups are not stored on a server. Deleting backups has no impact on the server performance.
- If a backup has been created and the next backup task is in progress, CBR will not allow you to delete the most recent backup created. You can delete the backup only after the backup task is complete.
- CBR automatically creates snapshots during backup and retains the latest snapshot for each disk.

### Prerequisites

- There is at least one backup.
- The backup to be deleted is in the **Available** or **Error** state.

### Procedure

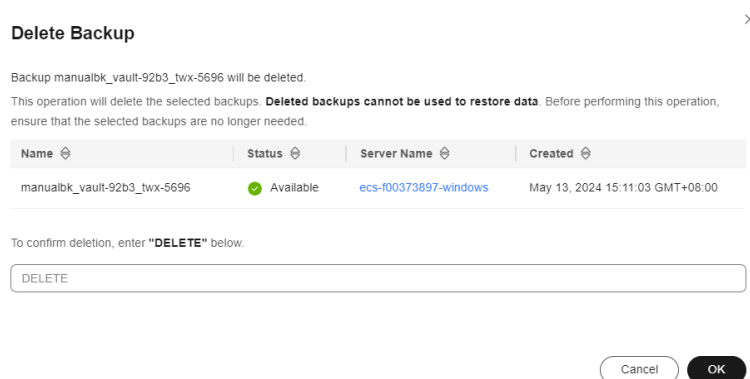
**Step 1** Log in to the CBR console.

1. [Log in to the management console.](#)
2. Click  in the upper left corner and select a region.
3. Click  and choose **Storage > Cloud Backup and Recovery**. Select a backup type from the left navigation pane.

**Step 2** Click the **Backups** tab and locate the desired backup. For details, see [Viewing a Backup](#).

**Step 3** Choose **More > Delete** from the **Operation** column. See [Figure 3-8](#). Alternatively, select the backups you want to delete in a batch and click **Delete** in the upper left corner to delete them.

**Figure 3-8** Deleting a backup



**Step 4** Click **OK**.

----End

## Follow-up Procedure

When you use CBR to back up a disk, all disk data including any invisible data will be backed up. If you frequently add, delete, or modify data on the disk before each backup task, a large amount of vault space will still be occupied even after some backups are deleted. For how to reduce occupied vault space, see [How Do I Reduce the Vault Space Occupied by Backups?](#)

## 3.6 Replicating a Backup Across Regions

### Scenarios

Cross-region replication of server backup vaults and SFS Turbo backup vaults allows you to **replicate backups from one region to another under the same account**.

Replicas of server backups can be used to create images and provision servers.

Replicas of SFS Turbo backups can be used to create file systems.

With cross-region replication, you can quickly deploy services in a different region. Data on the new resource in the destination region is the same as that on the original resource when you took the backup.

You can replicate backups in either of the following methods on the CBR console:

- Select a backup from the backup list and manually perform a replication.
- Select a backup vault and manually replicate it. Alternatively, you can configure a replication policy to periodically replicate backups that have not been replicated or failed to be replicated to the destination region.

This section uses the first method to describe how to replicate a backup. For details about the second method, see [Replicating a Vault Across Regions](#).

### Constraints

- A server backup can be replicated only when it meets all the following conditions:
  - a. It is an ECS backup.
  - b. It contains system disk data.
  - c. It is in the **Available** state.
- Only backups or backup vaults can be replicated. Replicated backups and vaults cannot be replicated again but their replicas can be used to create images or SFS Turbo file systems.
- A backup can be replicated to multiple regions but can have only one replica in each destination region. The replication rule varies with the replication method:

Manual replication: A backup can be manually replicated to the destination region as long as it has no replica in that region. A backup can be manually replicated again if its replica in the destination region has been deleted.





For manual and policy-based vault replication, a vault can only be replicated to a destination region once. It cannot be replicated to that region again, even if its backups have been deleted.

- Only replication-supported regions can be selected as destination regions. For details, see [Table 2-5](#)
- Only vaults of the same type can be selected as destination vaults. For example, if you want to replicate server backups to a different region, select a server backup vault (**Protection Type** set to **Replication (cross-region)**) in that region.

## Procedure

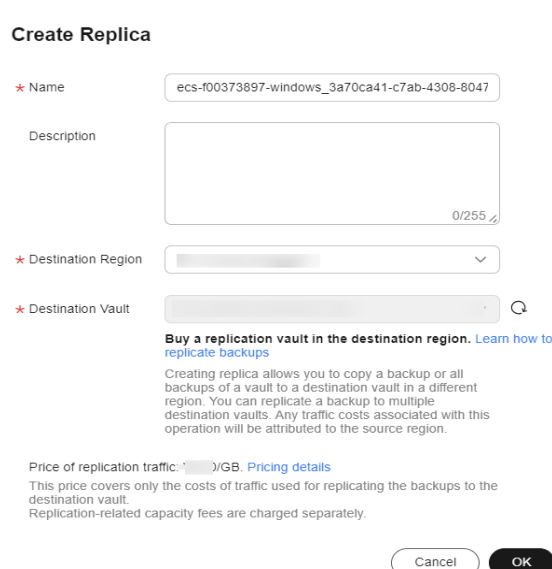
**Step 1** Log in to the CBR console.

1. [Log in to the management console.](#)
2. Click  in the upper left corner and select a region.
3. Click  and choose **Storage > Cloud Backup and Recovery**. Select a backup type from the left navigation pane.

**Step 2** Click the **Backups** tab and locate the desired backup. For details, see [Viewing a Backup](#).

**Step 3** Choose **More > Create Replica** in the **Operation** column of the backup. See [Figure 3-9](#).

**Figure 3-9** Creating a replica



**Create Replica** ×

★ Name

Description

★ Destination Region

★ Destination Vault

**Buy a replication vault in the destination region. [Learn how to replicate backups](#)**

Creating replica allows you to copy a backup or all backups of a vault to a destination vault in a different region. You can replicate a backup to multiple destination vaults. Any traffic costs associated with this operation will be attributed to the source region.

Price of replication traffic:  /GB. [Pricing details](#)

This price covers only the costs of traffic used for replicating the backups to the destination vault.  
Replication-related capacity fees are charged separately.

**Step 4** In the displayed dialog box, configure the parameters as described in [Table 3-5](#).

**Table 3-5** Parameter description

Parameter	Description
Name	<p>Replica name</p> <p>A name must contain 1 to 64 characters including digits, letters, underscores (_), or hyphens (-).</p>
Description	<p>Replica description</p> <p>It cannot exceed 255 characters.</p>
Destination Region	<p>Region to which the backup is replicated</p> <p>Only the regions that support replication will be displayed.</p> <ul style="list-style-type: none"> <li>• If the selected region contains only one project, you can directly select the region name.</li> <li>• If the selected region has multiple projects, the default project of the region is selected. You can select another project if needed.</li> </ul>
Destination Vault	<p>A replication vault in the destination region</p> <p>You can replicate backups to vaults in multiple destination regions. Creating replica will replicate all backups in the source vault to the destination vault.</p>

 **NOTE**

The traffic for cross-region replication is the size of the replicated backup.

**Step 5** Click **OK**.

**Step 6** After the replication is complete, you can switch to the destination region to view generated replicas. For details, see [Viewing a Backup](#). You can then use replicas to create images.

----**End**

# 4 Policy Management

## 4.1 Overview

There are backup policies and replication policies. A backup or replication policy allows CBR to automatically back up or replicate vaults at specified times or intervals. Periodic backups can be used to restore data quickly against data corruption or loss.

- **Backup policies:** To perform automatic backups, configure a backup policy by setting the execution times of backup tasks, the backup cycle, and retention rules, and then apply the policy to a vault. A backup policy takes effect after it is applied to a vault. If backup is not executed for a vault, verify that the policy is enabled.
- **Replication policies:** To automatically replicate backups or vaults, configure a replication policy by setting the execution times of replication tasks, the replication cycle, and retention rules, and then apply the policy to a vault. Backup replicas are stored in replication vaults.

## Supported Operations

You can perform the following operations.

Table 4-1



Operation	Description
<a href="#">Viewing the policy of a vault</a>	After a policy is applied to a vault, you can view the detailed policy information on the vault details page.
<a href="#">Creating a backup policy</a>	A backup policy allows CBR to automatically back up vaults at specified times or intervals. Periodic backups can be used to restore data quickly against data corruption or loss. You can use the default backup policy or create one as needed.
<a href="#">Creating a replication policy</a>	A replication policy allows CBR to periodically replicate backups that have not been replicated or failed to be replicated to the destination region.

Operation	Description
<b>Modifying a policy</b>	You can modify backup policies if needed.
<b>Deleting a policy</b>	You can delete backup and replication policies if they are no longer needed.
<b>Applying a policy to a vault</b>	You can apply a backup or replication policy to a vault to execute backup or replication tasks at specified times or intervals.
<b>Removing a policy from a vault</b>	If you no longer need automatic backup or replication for a vault, remove the policy from the vault.

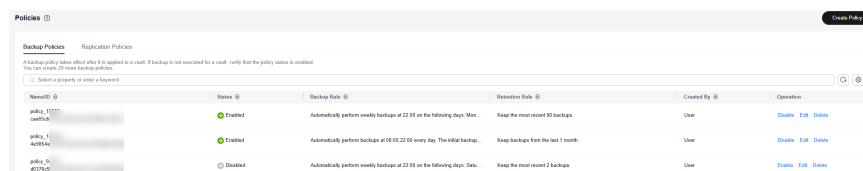
## 4.2 Viewing the Policy of a Vault

After a policy is created, you can view the policy in the policy list or on the vault details page.

**Step 1** Log in to the CBR console.

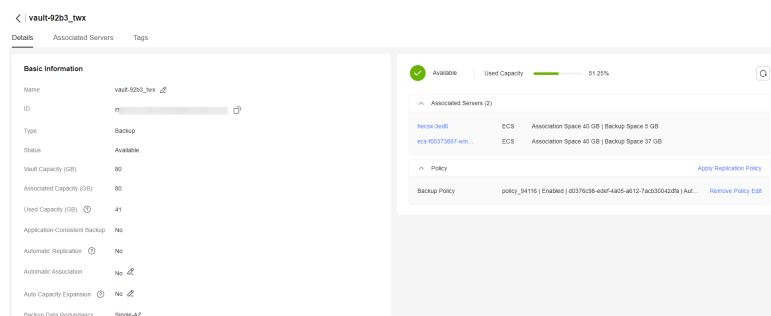
1. **Log in to the management console.**
2. Click  in the upper left corner and select a region.
3. Click  and choose **Storage > Cloud Backup and Recovery > Policies**.

**Step 2** View the created policy in the policy list. In the search box above the list, you can select an attribute or enter a keyword to search for policies.



**Step 3** After creating a policy and applying it to a vault, you can view the policy on the vault details page. Select a backup type on the left navigation pane. On the page displayed, locate the desired vault, click the vault name.

**Step 4** View the policy applied to the vault.



----End

## 4.3 Creating a Backup Policy

A backup policy allows CBR to automatically back up vaults at specified times or intervals. Periodic backups can be used to restore data quickly against data corruption or loss.

To implement periodic backups, you need a backup policy first. You can use the default backup policy or create one as needed.



Peak hours of the backup service are from 22:00 to 08:00, during which there may be delays. So you are advised to evaluate your service types and schedule backups in discrete time periods.

### Constraints

- Backup policies can be applied to the following types of vaults: server backup vaults, disk backup vaults, SFS Turbo backup vaults
- A backup policy must be enabled before it can be used for periodic backups.
- A maximum of 32 backup policies can be created in each account.
- When a backup time and a replication time are both configured, ensure that replication starts after backup is complete. Or, replication may fail.
- When expired backups are deleted, automatic backups will be deleted, but manual backups will not.
- Only servers in the **Running** or **Stopped** state and disks in the **Available** or **In-use** state can be backed up.
- CBR by default performs a full backup for a resource in the initial backup and incremental backups in subsequent backups.
- The minimum interval between two full backups is 1 day.

### Procedure

**Step 1** Log in to the CBR console.

1. [Log in to the management console](#).
2. Click  in the upper left corner and select a region.
3. Click  and choose **Storage > Cloud Backup and Recovery**.

**Step 2** Choose **Policies** in the left navigation pane and click the **Backup Policies** tab. In the upper right corner, click **Create Policy**. See [Figure 4-1](#).

**Figure 4-1** Creating a backup policy

The screenshot shows the 'Create Policy' interface with the following sections:

- Basic Information:**
  - Type: Backup policy (selected), Replication policy
  - Policy Name: policy\_165651
  - Status: Enable (selected), Disable
- Backup Rule:**
  - Current rule: Automatically perform weekly backups at 22:00 on the following days: Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday. The initial backup is a full backup. All subsequent backups are incremental backups.
  - Backup Frequency: Weekly (selected), Day-based
  - Automatically perform backups every: Mon, Tues, Wed, Thur, Fri, Sat, Sun
  - Execution Time: 00:00, 01:00, 02:00, 03:00, 04:00, 05:00, 06:00, 07:00, 08:00, 09:00, 10:00, 11:00, 12:00, 13:00, 14:00, 15:00, 16:00, 17:00, 18:00, 19:00, 20:00, 21:00, 22:00 (selected), 23:00
  - Full Backup:  Enable. Enabling full backup improves your data reliability, but they will use more storage space.
- Retention Rule:**
  - Current rule: Keep backups from the last 1 month.
  - Type: Backup quantity, Time period (selected), Permanent
  - Rule: Keep backups from the last 1 month. Older backups are automatically deleted.

Buttons: Cancel, Create Now

**Step 3** Set the backup policy parameters. [Table 4-2](#) describes the parameters.

**Table 4-2** Backup policy parameters

Parameter	Description	Example Value
Type	Select a policy type. In this section, we select the backup policy.	Backup policy
Name	Backup policy name A name must contain 1 to 64 characters including digits, letters, underscores (_), or hyphens (-).	backup_policy

Parameter	Description	Example Value
Status	Whether to enable the backup policy.	Only after a backup policy is enabled and applied will CBR automatically back up the vault resources and deletes expired backups.
Backup Frequency	Select a backup frequency. <ul style="list-style-type: none"><li>• <b>Weekly</b> Specifies on which days of each week the backup task will be executed. You can select multiple days.</li><li>• <b>Day based</b> Specifies the interval (every 1 to 30 days) for executing the backup task.</li></ul>	Every day If you select day-based backup, the first backup is supposed to be executed on the day when the backup policy is created. If the execution time on the day you create the backup policy has passed, the first backup will be executed in the next backup cycle.  It is recommended that backups be performed during off-peak hours or when no services are running.

Parameter	Description	Example Value
Execution Time	<p>Execution time</p> <p>Backups can be scheduled at the beginning of each hour, and you can select multiple hours.</p> <p><b>NOTICE</b></p> <ul style="list-style-type: none"> <li>There may be a time difference between the scheduled backup time and the actual backup time.</li> <li>If a large amount of data needs to be backed up, you are advised to make backup less frequent to prevent the system from skipping any execution time.</li> </ul> <p>For example, a disk is scheduled to be backed up at 00:00, 01:00, and 02:00. A backup task starts at 00:00. Because a large amount of incremental data needs to be backed up or a heap of backup tasks are executed at the same time, this backup task takes 90 minutes and completes at 01:30. CBR performs the next backup at 02:00. In this case, only two backups are generated in total, one at 00:00, and the other at 02:00.</p> <ul style="list-style-type: none"> <li>The execution times refer to the local times of clients, not the time zone and times of the region.</li> </ul>	<p>00:00, 02:00</p> <ul style="list-style-type: none"> <li>It is recommended that backups be performed during off-peak hours or when no services are running.</li> <li>Peak hours of the backup service are from 00:00 to 06:00, during which there may be scheduling delays. So you are advised to evaluate your service types and schedule backups outside of the backup peak hours.</li> </ul>



Parameter	Description	Example Value
Full Backup	<p>Whether to perform periodic full backups.</p> <ul style="list-style-type: none"> <li>• <b>Enable</b> Enabling full backup improves your data reliability, but full backups will use more storage space. Configure a full backup frequency. The value ranges from <b>0</b> to <b>100</b>. Value <b>0</b> means that a full backup will be performed in every backup task.</li> <li>• <b>Do not enable</b> CBR will perform incremental backups after the first backup.</li> </ul> <p><b>NOTICE</b></p> <ul style="list-style-type: none"> <li>- A full backup usually takes a long period of time. If a full backup of a resource is in progress, other policy or manual backups of this resource will not be performed. You can back up data during off-peak hours.</li> <li>- When backups are kept by quantity, full backups can be performed only when the full backup frequency configured is less than the number of retained backups.</li> <li>- If full backup is not enabled, to ensure data security, a full backup is performed after 365 incremental backups by default.</li> </ul>	7

Parameter	Description	Example Value
Retention Rule	<p>Rule that specifies how backups will be retained</p> <ul style="list-style-type: none"> <li>● <b>Time period</b> You can choose to retain backups for one month, three months, six months, one year, or for any desired number (2 to 99999) of days.</li> <li>● <b>Backup quantity</b> You can set the maximum number of backups to retain for each resource. The value ranges from 2 to 99999.</li> <li>● <b>Advanced Options</b> You can also set long-term retention rules with advanced options. Long-term retention rules and quantity-based retention rules will be both applied. <ul style="list-style-type: none"> <li>- <b>Day-based:</b> 0-100</li> <li>- <b>Weekly:</b> 0-100</li> <li>- <b>Monthly:</b> 0-100</li> <li>- <b>Yearly:</b> 0-100</li> </ul> </li> </ul> <p>A resource may be backed up multiple times in a day. If day-based backup is configured, only the most recent backup of that day is retained. If you set <b>Day-based</b> to <b>5</b>, the most recent backup of each of the last five days that have backups generated will be retained. That is, a total of five backups are retained. If there are more than five backup replicas, the system automatically deletes the earliest backup replicas. If day-based, weekly, monthly, and yearly retention rules are all configured, all the rules will apply and the union set of backups will be retained. For example, if <b>Day-based</b> is set to <b>5</b> and <b>Weekly</b> to <b>1</b>, five backups will be retained. The long-term retention rule and the quantity-based retention rule both apply.</p> <ul style="list-style-type: none"> <li>● <b>Permanent</b></li> </ul>	<p>Select <b>Backup quantity</b> and set to keep 3 backups. In addition, select <b>Advanced Options</b> and set to keep the most recent backup from each of the last two weeks. If today is the 30th of a month, see the execution of this policy in <a href="#">Figure 4-3</a>.</p> <ul style="list-style-type: none"> <li>● Dates with a time indicate the days that have backups generated</li> <li>● Dates with the time in gray indicate that the backups have been deleted.</li> <li>● Dates with the time in green indicate that the backups are retained.</li> </ul> <p>If the weekly retention rule in advanced options is not configured, only the backups generated on the 25th, 26th, and 29th are retained.</p>

Parameter	Description	Example Value
	<p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>- The system automatically deletes the earliest and expired backups every other day to avoid exceeding the maximum number of backups to retain or retaining any backup longer than the maximum retention period.</li> <li>- Expired backups are not deleted right after they are expired. They will be <b>deleted during 08:00 to 20:00 in batches</b>. For example, if a backup expired at 20:00 on November 23, 2024, it will be deleted during 08:00 to 20:00 on November 24, 2024. In this way, backup data can be deleted during off-peak hours.</li> <li>- The retention rules apply only to auto-generated backups, but not manual backups. Manual backups need to be deleted manually.</li> <li>- If a backup is used to create an image, the backup will not be deleted by the retention rule. It will be forcibly retained. If you delete the image created from the backup, the backup will be retained based on the original retention rule applied. (If the backup expires or is not within the most recent backups specified in the retention rule, CBR will automatically delete the backup.)</li> <li>- A maximum of 10 backups are retained for failed periodic backup tasks. They are retained for one month and can be deleted manually.</li> <li>- If a backup has been created and the next backup task is in progress, CBR will not allow you to delete the most recent backup created. You can delete the backup only after the backup task is complete.</li> </ul>	

**Figure 4-2** Retention rule with advanced options configured

**Retention Rule**

*Current rule: Keep the most recent 90 backups and execute advanced options.*

Type: **Backup quantity** | Time period | Permanent

Rule: Keep only the most recent  backups.

Advanced Options:  Configure now

*Quantity-based retention rules and advanced options do not conflict. They will both be applied. [Learn more](#)*

Day-Based: Keep the most recent backup from each of the last  days that have backups generated.

Weekly: Keep the most recent backup from each of the last  weeks.

Monthly: Keep the most recent backup from each of the last  months.

Yearly: Keep the most recent backup from each of the last  years.

**Figure 4-3** The execution of the retention rule

Sun	Mon	Tues	Wed	Thur	Fri	Sat
				<b>1</b> 23:00	2	3
<b>4</b> 23:00	<b>5</b> 23:00	6	7	<b>8</b> 23:00	9	10
<b>11</b> 23:00	<b>12</b> 23:00	13	14	<b>15</b> 23:00	16	17
<b>18</b> 23:00	<b>19</b> 23:00	20	21	<b>22</b> 23:00	23	24
<b>25</b> 23:00	<b>26</b> 23:00	27	28	<b>29</b> 23:00	30	31

**NOTE**

More frequent backups create more backups or retain backups for a longer time, protecting data to a greater extent but occupying more storage space. Set an appropriate backup frequency as needed.

**Step 4** Click **OK**.

**NOTE**

You can locate the desired vault and choose **More > Apply Backup Policy** to apply the policy to the vault. Then you can view the applied policy on the vault details page. After the policy is applied, data will be periodically backed up to the vault based on the policy.

----End

## Example

At 10:00 a.m. on Monday, a user sets a backup policy for their vault to instruct CBR to execute a backup task at 02:00 a.m. every day and retain a maximum of three backups. As of 11:00 a.m. on Saturday, three backups will be retained, which are generated on Thursday, Friday, and Saturday. The backups generated at 02:00 a.m. on Tuesday and Wednesday have been automatically deleted.

## 4.4 Creating a Replication Policy

A replication policy allows CBR to periodically replicate backups that have not been replicated or failed to be replicated to the destination region.



When a backup time and a replication time are both configured, ensure that replication starts after backup is complete. Or, replication may fail.

### Constraints

- You can only apply replication policies to server backup vaults, SFS Turbo backup vaults, and hybrid cloud backup vaults.

### Procedure

**Step 1** Log in to the CBR console.

1. [Log in to the management console.](#)
2. Click  in the upper left corner and select a region.
3. Click  and choose **Storage > Cloud Backup and Recovery**.

**Step 2** Choose **Policies** in the left navigation pane and click the **Replication Policies** tab. In the upper right corner, click **Create Policy**. Select **Replication Policy** for **Type**. See [Figure 4-4](#).

**Figure 4-4** Creating a replication policy

The screenshot shows the 'Create Policy' configuration page. It includes sections for 'Basic Information' (Type: Replication policy, Policy Name: policy\_165651, Status: Enable), 'Replication Rule' (Frequency: Weekly, Execution Time: 22:00, Destination Region: AP-Bangkok), and 'Retention Rule' (Type: Time period, Rule: Keep backups from the last 1 month). Buttons for 'Cancel' and 'Create Now' are at the bottom.

**Step 3** Set the replication policy parameters. [Table 4-3](#) describes the parameters.

**Table 4-3** Replication policy parameters

Parameter	Description	Example Value
Type	Select a policy type. In this section, we select the replication policy.	Replication policy
Name	Replication policy name A name must contain 1 to 64 characters including digits, letters, underscores (_), or hyphens (-).	replication_policy
Status	Whether to enable the replication policy	Only after a replication policy is enabled and applied will CBR automatically replicates the backups in the vaults and deletes expired backup replicas.

Parameter	Description	Example Value
Execution Time	<p>Execution times of the replication policy in a day</p> <p>Replication tasks can be scheduled at the beginning of each hour, and you can select multiple hours.</p>	<p>00:00, 02:00</p> <p>It is recommended that replication be performed during off-peak hours or when no services are running.</p>
Replication Frequency	<p>Select a replication frequency.</p> <ul style="list-style-type: none"> <li>● <b>Weekly</b> Specifies on which days of each week the replication task will be executed. You can select multiple days.</li> <li>● <b>Day based</b> Specifies the interval (every 1 to 30 days) for executing the replication task.</li> </ul>	<p>Every day</p> <p>If you select day-based replication, the first replication is supposed to be executed on the day when the replication policy is created. If the execution time on the day you create the replication policy has passed, the first replication will be performed in the next replication cycle.</p>

Parameter	Description	Example Value
Retention Rule	<p>Rule that specifies how backup replicas will be retained in the destination region</p> <ul style="list-style-type: none"> <li>● <b>Replica quantity</b> You can set the maximum number of backup replicas to retain for each resource. The value ranges from 2 to 99999. <p>You can also set long-term retention rules with advanced options. Long-term retention rules and quantity-based retention rules will be both applied.</p> <ul style="list-style-type: none"> <li>- <b>Day-based:</b> 0-100</li> <li>- <b>Weekly:</b> 0-100</li> <li>- <b>Monthly:</b> 0-100</li> <li>- <b>Yearly:</b> 0-100</li> </ul> <p>A resource may be replicated multiple times in a day. If day-based replication is configured, only the most recent backup replica of that day is retained. If you set <b>Day-based</b> to <b>5</b>, the most recent backup replica of each of the last five days that have backup replicas generated will be retained and the earliest backup replicas will be deleted automatically. If day-based, weekly, monthly, and yearly retention rules are all configured, all the rules will apply and the union set of backup replicas will be retained. For example, if <b>Day-based</b> is set to <b>5</b> and <b>Weekly</b> to <b>1</b>, five backup replicas will be retained. The long-term retention rule and the quantity-based retention rule both apply.</p> <ul style="list-style-type: none"> <li>● <b>Time period</b> You can choose to retain backup replicas for one month, three months, six months, one year, or for any desired number (2 to 99999) of days.</li> <li>● <b>Permanent</b></li> </ul> </li> </ul>	6 months



Parameter	Description	Example Value
	<p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>- The system automatically deletes the earliest and expired backup replicas every other day to avoid exceeding the maximum number of backup replicas to retain or retaining any backup replica longer than the maximum retention period.</li> <li>- There will be delays for CBR to delete expired backup replicas, but normally these delays will not be over 24 hours.</li> <li>- The retention rules apply only to auto-generated backup replicas, but not manual ones. Manual backup replicas need to be deleted manually.</li> <li>- After a backup replica is used to create an image, the replica will not be deleted by the retention rule.</li> </ul>	
Destination Region	<p>Region to which backups are replicated</p> <p>Only the regions that support replication will be displayed.</p> <ul style="list-style-type: none"> <li>• If the selected region contains only one project, you can directly select the region name.</li> <li>• If the selected region has multiple projects, the default project of the region is preselected. You can select another project if needed.</li> </ul>	AP-Bangkok

**Step 4** Click **Create Now**.

**Step 5** Locate the desired vault and choose **More > Apply Replication Policy** to apply the replication policy to the vault. Then you can view the applied policy on the vault details page.

After the policy is applied, backups will be periodically replicated to the destination vault based on the policy.

----End

## Example

A user applies a replication policy to a vault in a given region at 11:00 a.m. on Thursday. According to this policy, backups will be replicated to the destination region on 02:00 a.m. everyday, and only two backup replicas will be retained. According to this vault's backup policy, two backups are automatically generated at 00:00 everyday. At 12:00 p.m. on Saturday, the replication vault will contain two backup replicas, which are replicated on Saturday. Backup replicas generated at

02:00 a.m. on Friday have been automatically deleted according to the replication policy.

## 4.5 Modifying a Policy



You can modify backup policies if needed.

### Prerequisites

At least one policy has been created.

### Procedure

**Step 1** Log in to the CBR console.

1. [Log in to the management console](#).
2. Click  in the upper left corner and select a region.
3. Click  and choose **Storage > Cloud Backup and Recovery**. Select a backup type from the left navigation pane.

**Step 2** Find the target vault and click the vault name to view its details.

**Step 3** In the **Policies** area, click **Edit** in the row of the policy to be edited. See [Figure 4-5](#).

**Figure 4-5** Editing a backup policy

### Edit Policy

---

**Basic Information**

Policy Name

Status Enabled Disabled

---

**Backup Rule**

**i** Current rule: Automatically perform backups at 00:00,22:00 every day. The initial backup is a full backup. After that, a full backup will be performed after every 1 incremental backups.

Backup Frequency Weekly Day-based

Automatically perform backups every  days.

Execution Time Select All Invert Selection

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

Full Backup ?  Enable  
Enabling full backup improves your data reliability, but they will use more storage space.

Full Backup Frequency Perform a full backup after every  incremental backups.  
Based on your current settings, the minimum interval between two full backups is less than 7 days. You are advised to keep this interval greater than 7 days.

---

**Retention Rule**

**i** Current rule: Keep backups from the last 1 month.

Type Backup quantity Time period Permanent

After the retention time period is changed, the new retention rule will be applied only to new backups, but not those generated before this change. [Learn more](#)

Rule Keep backups from the last  . Older backups are automatically deleted.

Cancel
OK

Related parameters are described in [Table 4-2](#) and [Table 4-3](#).

**Step 4** Click **OK**.

If the retention rule is modified, the new rule does not necessarily apply to existing backups. For details, see [Why Does the Retention Rule Not Take Effect After Being Changed?](#)

**Step 5** Alternatively, select **Policies** from the navigation pane on the left and edit the desired policy.

----End

## 4.6 Deleting a Policy



You can delete policies if they are no longer needed.

### Prerequisites

At least one policy has been created.

### Procedure

**Step 1** Log in to the CBR console.

1. [Log in to the management console.](#)
2. Click  in the upper left corner and select a region.
3. Click  and choose **Storage > Cloud Backup and Recovery.**

**Step 2** Click the **Backup Policies** tab, locate the row that contains the policy you want to delete, and click **Delete**.

#### NOTE

Deleting a policy will not delete the backups generated based on the policy. You can manually delete unwanted backups.

**Step 3** Confirm the information and click **OK**.

----End

## 4.7 Applying a Policy to a Vault



You can apply a backup or replication policy to a vault to execute backup or replication tasks at specified times or intervals.

### Constraints

You can create multiple policies, but a can apply only one backup or replication policy to a vault.

### Procedure

**Step 1** Log in to the CBR console.

1. [Log in to the management console.](#)
2. Click  in the upper left corner and select a region.
3. Click  and choose **Storage > Cloud Backup and Recovery.** Select a backup type from the left navigation pane.

**Step 2** Find the target vault and choose **More > Apply Backup Policy** or **More > Apply Replication Policy**. See [Figure 4-6](#).

**Figure 4-6** Setting a backup policy

**Step 3** Select an existing backup policy from the drop-down list or create a new one. For how to create a policy, see [Creating a Backup Policy](#) and [Creating a Replication Policy](#).

**Step 4** After the policy is successfully applied, view details in the **Policies** area of the vault details page.

----End

## 4.8 Removing a Policy from a Vault

### Scenarios



If you need to cancel auto backup or replication of a vault, remove the policy from the vault, or disable the policy. This section describes how to remove a policy from a vault.

### Prerequisites

A policy has been applied to the vault.

### Procedure

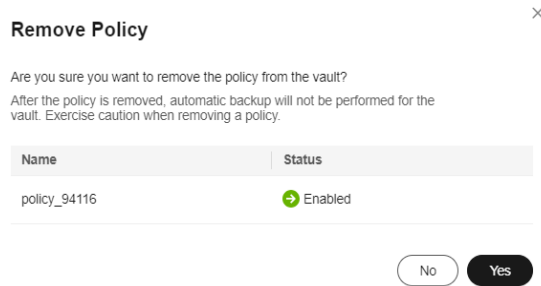
**Step 1** Log in to the CBR console.

1. [Log in to the management console](#).
2. Click  in the upper left corner and select a region.
3. Click  and choose **Storage > Cloud Backup and Recovery**. Select a backup type from the left navigation pane.

**Step 2** Find the target vault and click the vault name to view its details.

**Step 3** In the **Policies** area, click **Remove Policy**. See [Figure 4-7](#).

**Figure 4-7** Removing a policy



 **NOTE**

- You can remove a policy from a vault when the vault resources are being backed up. In this case, backup tasks will continue, and backups will be generated.
- After a policy is removed, backups retained by **Time period** will expire based on the retention rule, but backups retained by **Backup quantity** will not. You need manually delete unwanted backups.

**Step 4** Click **Yes**.

Tasks will no longer be executed based on this policy for the vault.

----**End**

# 5 Organizational Policy Management

---

## 5.1 Overview

You can manage backup policies for a given organization. The organization administrator or delegated CBR administrator can centrally create and configure organizational policies for member accounts in the organization. All member accounts in the organization can use the created organizational policies.

CBR will be enabled as a trusted service when a management account creates organizational policies. After CBR is enabled as a trusted service for Organizations, CBR can obtain information about OUs and member accounts to provide organization-level management and backup services for the entire organization.

There are organizational backup policies and organizational replication policies.

- **Organizational backup policies:** An enterprise can use an organization's management account to configure organizational backup policies for all the member accounts in the organization. All member accounts in the organization can use the created organizational backup policies.
- **Organizational replication policies:** An enterprise can use an organization's management account to configure organizational replication policies for all the member accounts in the organization. All member accounts in the organization can use the created organizational replication policies.

## 5.2 Creating an Organizational Backup Policy

An enterprise can use an organization's management account to configure organizational backup policies for all the member accounts in the organization. All member accounts in the organization can use the created organizational backup policies.

This section describes how to create an organizational backup policy.



### Constraints

- Backup policies can be applied to the following types of vaults: server backup vaults, disk backup vaults, SFS Turbo backup vaults

- A backup policy must be enabled before it can be used for periodic backups.
- A maximum of 32 backup policies can be created in each account.
- When a backup time and a replication time are both configured, ensure that replication starts after backup is complete. Or, replication may fail.
- When expired backups are deleted, automatic backups will be deleted, but manual backups will not.
- Only servers in the **Running** or **Stopped** state and disks in the **Available** or **In-use** state can be backed up.
- CBR by default performs a full backup for a resource in the initial backup and incremental backups in subsequent backups.
- The minimum interval between two full backups is 1 day.

## Procedure

**Step 1** Log in to the CBR console.

1. [Log in to the management console](#).
2. Click  in the upper left corner and select a region.
3. Click  and choose **Storage > Cloud Backup and Recovery**. Select a backup type from the left navigation pane.

**Step 2** Choose **Organizational Policies** in the left navigation pane and click the **Organizational Backup Policies** tab. In the upper right corner, click **Create Organizational Policy**. See [Figure 5-1](#).



**Figure 5-1** Create Organizational Policy

**Create Organizational Policy**

---

**Basic Information**

Organizational Policy Name

Organizational Policy Description

Organizational Policy Type  
 Backup     Replication

Policy Name

Status  
 Enable     Disable

**Backup Rule**

**i** Current rule: Automatically perform weekly backups at 22:00 (UTC+08:00) on the following days: Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday. The initial backup is a full backup. All subsequent backups are incremental backups.

Backup Frequency  
 Weekly     Day-based

Automatically perform backups every

Execution Time  

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

[Select All](#) [Invert Selection](#)

Timezone

Full Backup **i**  
 Enable  
Enabling full backup improves your data reliability, but they will use more storage space.

**Retention Rule**

**i** Current rule: Keep backups from the last 1 month.

Type  
 Backup quantity     Time period     Permanent

**Step 3** Set the backup policy parameters. [Table 5-1](#) describes the parameters.

**Table 5-1** Backup policy parameters

Parameter	Description	Example Value
Organizational Policy Name	Organizational policy name A name must contain 1 to 64 characters including digits, letters, underscores (_), or hyphens (-).	org_policy
Organizational Policy Description	Description that can help the organization members to understand the usage of the policy.	/

Parameter	Description	Example Value
Organizational Policy Type	Select a policy type. In this section, we select the backup policy.	Backup policy
Policy Name	Backup policy name A name must contain 1 to 64 characters including digits, letters, underscores (_), or hyphens (-).	backup_policy
Status	Whether to enable the backup policy.	Only after a backup policy is enabled and applied will CBR automatically back up the vault resources and deletes expired backups.
Backup Frequency	Select a backup frequency. <ul style="list-style-type: none"> <li>• <b>Weekly</b> Specifies on which days of each week the backup task will be executed. You can select multiple days.</li> <li>• <b>Day based</b> Specifies the interval (every 1 to 30 days) for executing the backup task.</li> </ul>	Every day If you select day-based backup, the first backup is supposed to be executed on the day when the backup policy is created. If the execution time on the day you create the backup policy has passed, the first backup will be executed in the next backup cycle.  It is recommended that backups be performed during service off-peak hours or when no services are running.

Parameter	Description	Example Value
Execution Time	<p>Execution times of the backup policy in a day</p> <p>Backups can be scheduled at the beginning of each hour, and you can select multiple hours.</p> <p><b>NOTICE</b></p> <ul style="list-style-type: none"> <li>• There may be a time difference between the scheduled backup time and the actual backup time.</li> <li>• If a large amount of data needs to be backed up, you are advised to make backup less frequent to prevent the system from skipping any execution time. For example, a disk is scheduled to be backed up at 00:00, 01:00, and 02:00. A backup task starts at 00:00. Because a large amount of incremental data needs to be backed up or a heap of backup tasks are executed at the same time, this backup task takes 90 minutes and completes at 01:30. CBR performs the next backup at 02:00. In this case, only two backups are generated in total, one at 00:00, and the other at 02:00.</li> <li>• The execution times refer to the local times of clients, not the time zone and times of the region.</li> </ul>	<p>00:00, 02:00</p> <ul style="list-style-type: none"> <li>• It is recommended that backups be performed during service off-peak hours or when no services are running.</li> <li>• Peak hours of the backup service are from 00:00 to 06:00, during which there may be scheduling delays. So you are advised to evaluate your service types and schedule backups outside of the backup peak hours.</li> </ul>

Parameter	Description	Example Value
Full Backup	<p>Whether to perform periodic full backups.</p> <ul style="list-style-type: none"> <li>• <b>Enable</b> Enabling full backup improves your data reliability, but full backups will use more storage space. Configure a full backup frequency. The value ranges from <b>0</b> to <b>100</b>. Value <b>0</b> means that a full backup will be performed in every backup task.</li> <li>• <b>Do not enable</b> Periodic full backup will not be performed. Instead, CBR will always perform incremental backups after the first backup.</li> </ul> <p><b>NOTICE</b></p> <ul style="list-style-type: none"> <li>- A full backup usually takes a long period of time. If a full backup of a resource is in progress, other backups of this resource will not be performed. For example, any policy-based backups planned to be executed during a full backup will be skipped.</li> <li>- When backups are kept by quantity, full backups can be performed only when the full backup frequency configured is less than the number of retained backups.</li> </ul>	7

Parameter	Description	Example Value
Retention Rule	<p>Rule that specifies how backups will be retained</p> <ul style="list-style-type: none"> <li>● <b>Time period</b> You can choose to retain backups for one month, three months, six months, one year, or for any desired number (2 to 99999) of days.</li> <li>● <b>Backup quantity</b> You can set the maximum number of backups to retain for each resource. The value ranges from 2 to 99999.</li> <li>● <b>Advanced Options</b> You can also set long-term retention rules with advanced options. Long-term retention rules and quantity-based retention rules will be both applied. <ul style="list-style-type: none"> <li>- <b>Day-based:</b> 0-100</li> <li>- <b>Weekly:</b> 0-100</li> <li>- <b>Monthly:</b> 0-100</li> <li>- <b>Yearly:</b> 0-100</li> </ul> <p>A resource may be backed up multiple times in a day. If day-based backup is configured, only the most recent backup of that day is retained. If you set <b>Day-based</b> to 5, the most recent backup of each of the last five days that have backups generated will be retained and the earliest backups will be deleted automatically. If day-based, weekly, monthly, and yearly retention rules are all configured, all the rules will apply and the union set of backups will be retained. For example, if <b>Day-based</b> is set to 5 and <b>Weekly</b> to 1, five backups will be retained. The long-term retention rule and the quantity-based retention rule both apply.</p> </li> <li>● <b>Permanent</b></li> </ul>	6 months

Parameter	Description	Example Value
	<p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>- The system automatically deletes the earliest and expired backups every other day to avoid exceeding the maximum number of backups to retain or retaining any backup longer than the maximum retention period.</li> <li>- Expired backups are not deleted right after they are expired. They will be deleted from 12:00 to 00:00 in batches.</li> <li>- The retention rules apply only to auto-generated backups, but not manual backups. Manual backups need to be deleted manually.</li> <li>- If a backup is used to create an image, the backup will not be deleted by the retention rule.</li> <li>- A maximum of 10 backups are retained for failed periodic backup tasks. They are retained for one month and can be deleted manually.</li> </ul>	

 **NOTE**

More frequent backups create more backups or retain backups for a longer time, protecting data to a greater extent but occupying more storage space. Set an appropriate backup frequency as needed.

**Step 4** Click **Create Now**.

 **NOTE**

After the backup policy is created, it will automatically appear in each member account's policy list.

----End

**Follow-Up Operations**

- [Modifying a Policy](#)
- [Deleting a Policy](#)

## 5.3 Creating an Organizational Replication Policy

An enterprise can use an organization's management account to configure organizational replication policies for all the member accounts in the organization. All member accounts in the organization can use the created organizational replication policies.



This section describes how to create an organizational replication policy.

## Constraints

- You can only apply replication policies to server backup vaults, SFS Turbo backup vaults, and hybrid cloud backup vaults.

## Procedure

**Step 1** Log in to the CBR console.

1. [Log in to the management console](#).
2. Click  in the upper left corner and select a region.
3. Click  and choose **Storage > Cloud Backup and Recovery**. Select a backup type from the left navigation pane.

**Step 2** Choose **Organizational Policies** in the left navigation pane and click the **Organizational Replication Policies** tab. In the upper right corner, click **Create Organizational Policy**. Select **Replication** for **Organizational Policy Type**. See [Figure 5-2](#).

**Figure 5-2** Creating an organizational policy

**Step 3** Set the replication policy parameters. [Table 5-2](#) describes the parameters.

**Table 5-2** Replication policy parameters

Parameter	Description	Example Value
Organizational Policy Name	Organizational policy name A name must contain 1 to 64 characters including digits, letters, underscores (_), or hyphens (-).	org_policy
Organizational Policy Description	Description that can help the organization members to understand the usage of the policy.	/
Organizational Policy Type	Select a policy type. In this section, we select the replication policy.	Replication policy



Parameter	Description	Example Value
Policy Name	Replication policy name A name must contain 1 to 64 characters including digits, letters, underscores (_), or hyphens (-).	replication_policy
Status	Whether to enable the replication policy	Only after a replication policy is enabled and applied will CBR automatically replicates the backups in the vaults and deletes expired backup replicas.
Execution Time	Execution times of the replication policy in a day Replication tasks can be scheduled at the beginning of each hour, and you can select multiple hours.	00:00, 02:00 It is recommended that replication be performed during off-peak hours or when no services are running.
Replication Frequency	Select a replication frequency. <ul style="list-style-type: none"> <li>• <b>Weekly</b> Specifies on which days of each week the replication task will be executed. You can select multiple days.</li> <li>• <b>Day based</b> Specifies the interval (every 1 to 30 days) for executing the replication task.</li> </ul>	Every day If you select day-based replication, the first replication is supposed to be executed on the day when the replication policy is created. If the execution time on the day you create the replication policy has passed, the first replication will be performed in the next replication cycle.

Parameter	Description	Example Value
Retention Rule	<p>Rule that specifies how backup replicas will be retained in the destination region</p> <ul style="list-style-type: none"> <li>• <b>Backup quantity</b> You can set the maximum number of backup replicas to retain for each resource. The value ranges from 2 to 99999. <p>You can also set long-term retention rules with advanced options. Long-term retention rules and quantity-based retention rules will be both applied.</p> <ul style="list-style-type: none"> <li>- <b>Day-based:</b> 0-100</li> <li>- <b>Weekly:</b> 0-100</li> <li>- <b>Monthly:</b> 0-100</li> <li>- <b>Yearly:</b> 0-100</li> </ul> <p>A resource may be replicated multiple times in a day. If day-based replication is configured, only the most recent backup replica of that day is retained. If you set <b>Day-based</b> to <b>5</b>, the most recent backup replica of each of the last five days that have backups generated will be retained and the earliest backup replicas will be deleted automatically. If day-based, weekly, monthly, and yearly retention rules are all configured, all the rules will apply and the union set of backup replicas will be retained. For example, if <b>Day-based</b> is set to <b>5</b> and <b>Weekly</b> to <b>1</b>, five backup replicas will be retained. The long-term retention rule and the quantity-based retention rule both apply.</p> <ul style="list-style-type: none"> <li>• <b>Time period</b> You can choose to retain backup replicas for one month, three months, six months, one year, or for any desired number (2 to 99999) of days.</li> <li>• <b>Permanent</b></li> </ul> </li> </ul>	6 months

Parameter	Description	Example Value
	<p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>- The system automatically deletes the earliest and expired backup replicas every other day to avoid exceeding the maximum number of backup replicas to retain or retaining any backup replica longer than the maximum retention period.</li> <li>- There will be delays for CBR to delete expired backup replicas, but normally these delays will not be over 24 hours.</li> <li>- The retention rules apply only to auto-generated backup replicas, but not manual ones. Manual backup replicas need to be deleted manually.</li> <li>- After a backup replica is used to create an image, the replica will not be deleted by the retention rule.</li> </ul>	
Destination Region	<p>Region to which backups are replicated</p> <p>Only the regions that support replication will be displayed.</p> <ul style="list-style-type: none"> <li>• If the selected region contains only one project, you can directly select the region name.</li> <li>• If the selected region has multiple projects, the default project of the region is preselected. You can select another project if needed.</li> </ul>	AP-Bangkok

**Step 4 Click Create Now.**

 **NOTE**

After the replication policy is created, it will automatically appear in each member account's policy list.

----End

**Follow-Up Operations**

- [Modifying a Policy](#)
- [Deleting a Policy](#)

# 6 Application-Consistent Backup

---

## 6.1 Application-Consistent Backup

### Overview

There are three types of backups in terms of backup consistency:

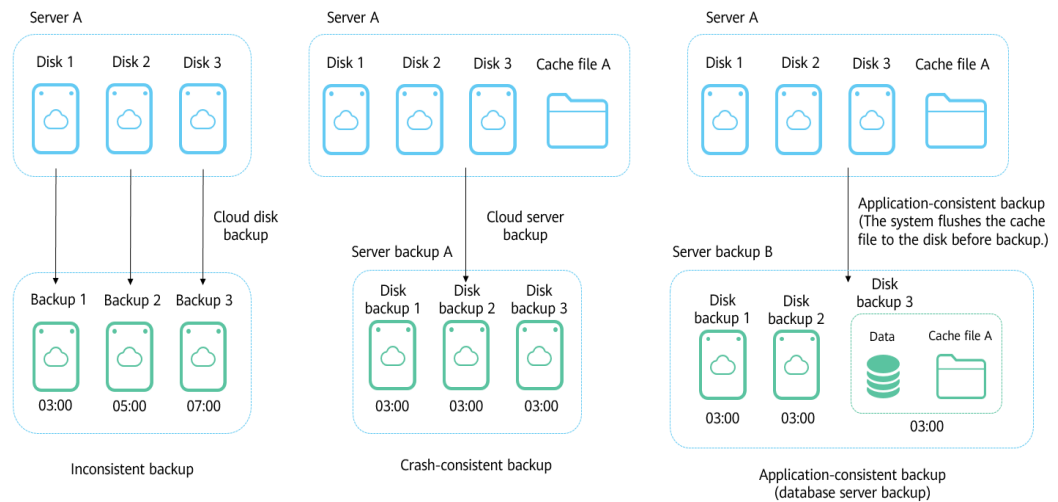
- Inconsistent backup: An inconsistent backup contains data taken from different points in time. This typically occurs if changes are made to your files or disks during the backup. CBR cloud server backup uses the consistency snapshot technology for disks to protect data of ECSs and BMSs. If you back up multiple EVS disks separately, the backup time points of the EVS disks are different. As a result, the backup data of the EVS disks is inconsistent.
- Crash-consistent backup: A crash-consistent backup captures all data on disks at the time of the backup and does not capture data in memory or any pending I/O operations. Although it cannot ensure application consistency, disks are checked by **chkdsk** upon operating system restart to restore damaged data and undo logs are used by databases to keep data consistent.
- Application-consistent backup: An application-consistent backup captures data in memory or any pending I/O operations and allows applications to achieve a quiescent and consistent state.

**Figure 6-1** compares these backup types in detail.

CBR supports both crash-consistent backup (also called cloud server backup) and application-consistent backup.

Crash-consistent backup does not back up data in memory or pending I/O operations and cannot be used to restore applications. If your server is running a MySQL or SAP HANA database, you can use application-consistent backup. An application-consistent backup capture application information both in memory and in pending I/O operations and can be used to quickly restore applications.

**Figure 6-1 Backup consistency**



## Differences Between Application-Consistent Backup and Cloud Server Backup

Item	Application-Consistent Backup	Cloud Server Backup
Object	Cloud servers with MySQL or SAP HANA database deployed	Cloud servers without databases
Granularity	Cloud server	Cloud server
Vault	Server backup vault	Server backup vault
Recommended scenario	Data of cloud servers and their databases such as MySQL or SAP HANA database needs to be backed up. All data and application configurations need to be restored in case of an error.	Only data of cloud servers needs to be backed up. Such data needs to be restored in case of an error.  If cloud server backup is used to back up database servers, some database configurations may fail to be restored from the backups and issues may occur when the database is restarted.

### NOTICE

There are two types of vaults to store server backups. Those store backups of non-database servers are server backup vaults, and those store backups of database servers are database server backup vaults.

## Application Scope

**Table 6-1** lists the OSs that support the installation of Agent.

**Table 6-1** OSs that support installation of the Agent

Database	OS	Version
SQL Server 2008/2012/2019	Windows	Windows Server 2008, 2008 R2, 2012, 2012 R2, and 2019 for x86_64
SQL Server 2014/2016/Enterprise Edition	Windows	Windows Server 2014, 2014 R2, and 2016 Datacenter for x86_64
MySQL 5.5/5.6/5.7	Red Hat	Red Hat Enterprise Linux 6 and 7 for x86_64
	SUSE	SUSE Linux Enterprise Server 11, 12, 15 SP1, 15 SP2 for x86_64
	CentOS	CentOS 6 and 7 for x86_64
	EulerOS	EulerOS 2.2 and 2.3 for x86_64
HANA 1.0/2.0	SUSE	SUSE Linux Enterprise Server 12 for x86_64

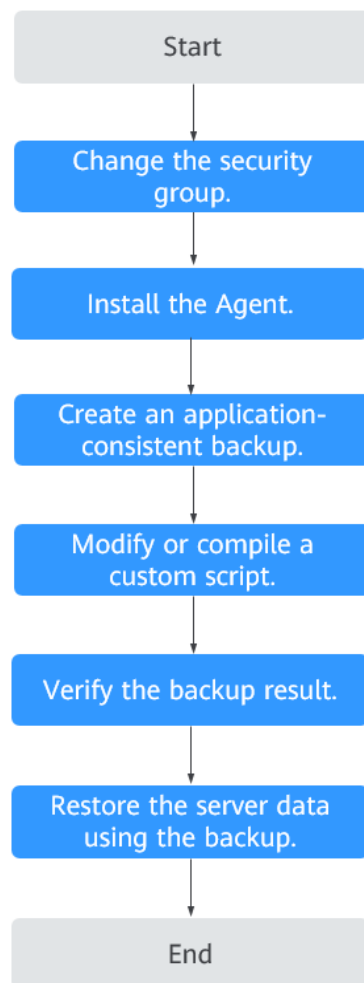
 **NOTE**

For Windows servers, ensure that Volume Shadow Copy is installed and can run properly.

For databases that are not in the compatibility list, you can create a custom script to back up the database server by referring to [Using a Custom Script to Implement Application-Consistent Backup](#) in the *Cloud Backup and Recovery Best Practices*.

## Process

[Figure 6-2](#) shows the application-consistent backup process.

**Figure 6-2** Application-consistent backup process

- Step 1** Change the security group: Before performing an application-consistent backup task, change the security group of the server you want to back up.
- Step 2** Install the agent: Change the security group and install the agent in any sequence. Ensure that the two operations are completed before backing up the desired server.
- Step 3** Create an application-consistent backup: After creating a server backup vault for storing application-consistent backups, associate it with the desired database server and then create an application-consistent backup.
- Step 4** Modify or compile a custom script: After backing up a database server on the CBR console, modify or compile a custom script on the database of the server. For details, see [Using a Custom Script to Implement Application-Consistent Backup](#).
- Step 5** Verify the backup result: After the backup is performed, verify that the backup succeeds. For details, see [Verifying the Application-Consistent Backup Result](#).
- Step 6** Use the backup to restore server data: Use the application-consistent backup to restore server data. The restored database applications and data are the same as

those at the backup point in time. For details, see [Restoring from a Cloud Server Backup](#).

----End

## 6.2 Changing a Security Group

### Context

A security group is a collection of access control rules for ECSs that have the same security protection requirements and are mutually trusted in a VPC. After a security group is created, you can create different access rules for the security group to protect the ECSs that are added to this security group. The default security group rule allows all outgoing data packets. ECSs in a security group can access each other without the need to add rules. The system creates a security group for each cloud account by default. You can also create custom security groups by yourself.


When creating a security group, you must add the inbound and outbound access rules and enable the ports required for application-consistent backup to prevent application-consistent backup failures.

### Operation Instructions

Before using the application-consistent backup function, you need to change the security group. To ensure network security, CBR has not set the inbound direction of a security group, so you need to manually configure it.

In the outbound direction of the security group, ports 1 to 65535 on the 100.125.0.0/16 network segment must be configured. In the inbound direction, ports 59526 to 59528 on the 100.125.0.0/16 network segment must be configured. The default outbound rule is 0.0.0.0/0, that is, all data packets are permitted. If the default rule in the outbound direction is not modified, you do not need to configure the outbound direction.

### Procedure

- Step 1** Log in to the ECS console.
  1. Log in to the management console.
  2. Click  in the upper left corner and select a region.
  3. Under **Computing**, click **Elastic Cloud Server**.
- Step 2** In the navigation pane on the left, choose **Elastic Cloud Server** or **Bare Metal Server**. On the page displayed, select the target server. Go to the server details page.
- Step 3** Click the **Security Groups** tab and select the target security group. On the right of the ECS page, click **Modify Security Group Rule** for an ECS. Click **Change Security Group** for a BMS. In the displayed dialog box, click **Manage Security Group**.
- Step 4** On the **Security Groups** page, click the **Inbound Rules** tab, and then click **Add Rule**. The **Add Inbound Rule** dialog box is displayed, as shown in [Figure 6-3](#).



Select **TCP** for **Protocol/Application**, enter **59526-59528** in **Port & Source**, select **IP address** for **Source** and enter **100.125.0.0/16**. After supplementing the description, click **OK** to complete the setting of the inbound rule.

**Figure 6-3** Adding an inbound rule

**Step 5** Click the **Outbound Rules** tab, and then click **Add Rule**. The **Add Outbound Rule** dialog box is displayed, as shown in **Figure 6-4**. Select **TCP** for **Protocol/ Application**, enter **1-65535** in **Port & Source**, select **IP address** for **Destination** and enter **100.125.0.0/16**. After supplementing the description, click **OK** to complete the setting of the outbound rule.

**Figure 6-4** Adding an outbound rule

----End

## 6.3 Installing the Agent

Before enabling application-consistent backup, change the security group and successfully install the Agent on your ECSs.

If application-consistent backup is enabled but Agent is not installed on servers, application-consistent backup will fail, and a common server backup will be performed instead. To ensure that application-consistent backup is properly executed, download and install the Agent first.

## Operation Instructions

- Application-consistent backup supports only x86-based ECSs, not Kunpeng-based ECSs.
- During the Agent installation, the system requires the **rdadmin** user's permissions to run the installation program. To improve O&M security, change the user **rdadmin**'s password of the Agent OS regularly and disable this user's remote login permission. For details, see [Changing the Password of User rdadmin](#).
- [Table 6-2](#) lists OSs that support installation of the Agent.

**Table 6-2** OSs that support installation of the Agent

Database	OS	Version
SQL Server 2008/2012/2019	Windows	Windows Server 2008, 2008 R2, 2012, 2012 R2, and 2019 for x86_64
SQL Server 2014/2016/Enterprise Edition	Windows	Windows Server 2014, 2014 R2, and 2016 Datacenter for x86_64
MySQL 5.5/5.6/5.7	Red Hat	Red Hat Enterprise Linux 6 and 7 for x86_64
	SUSE	SUSE Linux Enterprise Server 11, 12, 15 SP1, 15 SP2 for x86_64
	CentOS	CentOS 6 and 7 for x86_64
	EulerOS	EulerOS 2.2 and 2.3 for x86_64
HANA 1.0/2.0	SUSE	SUSE Linux Enterprise Server 12 for x86_64

### NOTE

For Windows servers, ensure that Volume Shadow Copy is installed and can run properly.

- [Table 6-3](#) lists the supported SHA256 values.

**Table 6-3** SHA256 values

Package Name	SHA256 Value
Cloud Server Backup Agent-CentOS6-x86_64.tar.gz	f0c59ccb4443bcb6e874bf6e3c574914f9f8b27f3f7379e2d81956a9972802f3
Cloud Server Backup Agent-CentOS7-x86_64.tar.gz	2d3028cb794e1699bae9f65746a60ae99be17d5c4c5e7ebe6b45ff261db9c3c7
Cloud Server Backup Agent-EulerOS2-x86_64.tar.gz	4fb4cf9cb6f5b0e6c13d8ad8bf928754cb95332ee645a97fd0bb3fcbcb53d003
Cloud Server Backup Agent-RedHat6-x86_64.tar.gz	6ae3838fb5644f0f47282c211fe20c6b57a7c5c1d683cd5a1f55860d259b2054
Cloud Server Backup Agent-RedHat7-x86_64.tar.gz	40fa68a808d9da04672678b2773e3345ea6c9dee3c17d598acb66a023cc5cacc
Cloud Server Backup Agent-SuSE11-x86_64.tar.gz	346cc9f1fc0a41a817abb2db61e657a4d615449e13bc46f1c1cfbadc0b281f47
Cloud Server Backup Agent-SuSE12-x86_64.tar.gz	625279b9c9d17ddcc4210b78242efebacd73f808b86754659d243ece85a400
Cloud Server Backup Agent-WIN64.zip	b7b2067ac89f1fec635d82e3fe2ea794ce6482f9880838f34924b383be44ac4e

**NOTICE**



To install the Agent, the system will open the firewall of a port from 59526 to 59528 of the ECS. When port 59526 is occupied, the firewall of port 59527 is enabled, and so on.

**Prerequisites**

- The username and password for logging in to the console have been obtained.
- The security group has been configured.
- The **Agent Status** of the ECS is **Not installed**.
- If you use Internet Explorer, you need to add the websites you will use to trusted sites.

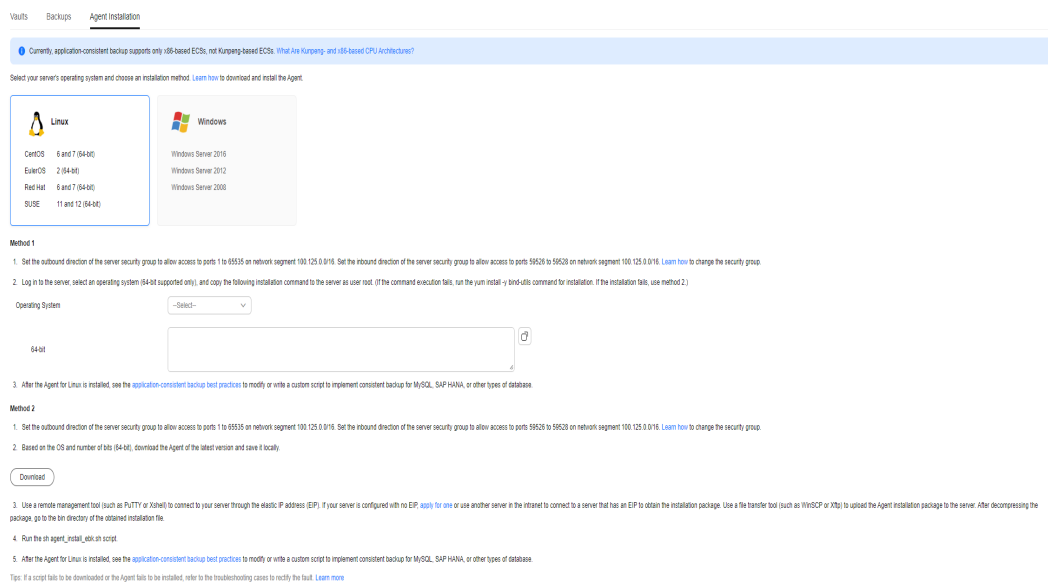
## Installing the Agent for a Linux OS (Method 1)

**Step 1** Log in to the CBR console.

1. [Log in to the management console.](#)
2. Click  in the upper left corner and select a region.
3. Click  and choose **Storage > Cloud Backup and Recovery**. Select a backup type from the left navigation pane.

**Step 2** Click the **Agent Installation** tab.

**Figure 6-5** Installation page for Linux



**Step 3** In method 1, select the corresponding Agent version as required, and copy the installation command in step 2.

**Step 4** On the ECS page, select the target server and click **Remote Login** in the **Operation** column to log in to the ECS.

### NOTE

Ensure that the package's SHA256 value is the same as that listed in [Table 6-3](#).

For how to obtain the software package, go to method 2. Specifically, click **Download**, and then on the displayed page, select a version based on the target ECS OS and click **OK**.

**Step 5** Paste the installation command in step 2 to the ECS and run the command as user **root**.

If the execution fails, run the **yum install -y bind-utils** command to install the dig module. If the installation still fails, use method 2 to install the Agent for a Linux OS.



**Step 6** After the installation is complete, Agent is running properly. To implement application-consistent backup for MySQL, SAP HANA, or other types of databases,

modify or compile a custom script by referring to the *Cloud Backup and Recovery Best Practices*.

----End

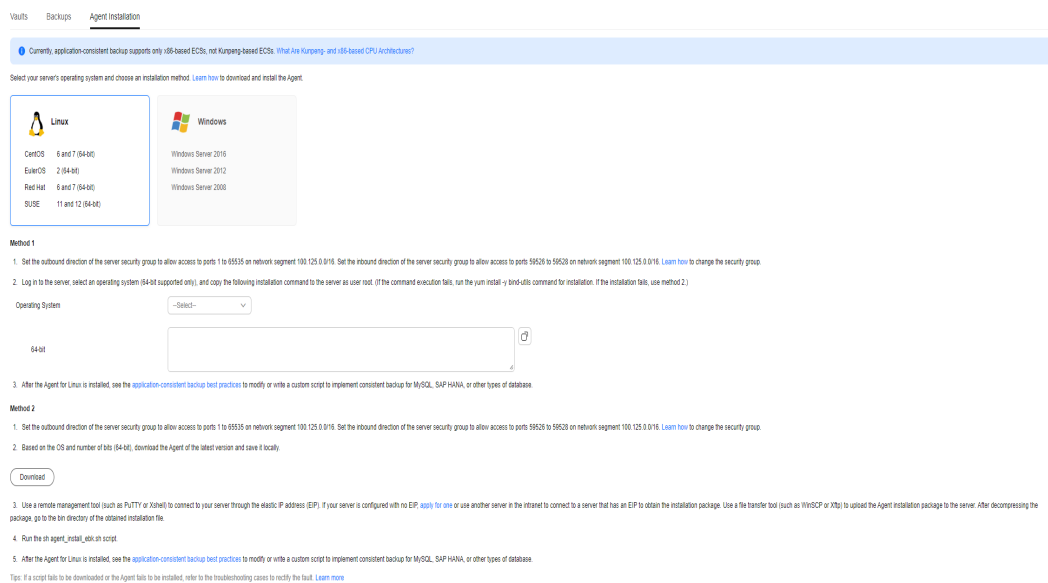
## Installing the Agent for a Linux OS (Method 2)

**Step 1** Log in to the CBR console.

1. [Log in to the management console](#).
2. Click  in the upper left corner and select a region.
3. Click  and choose **Storage > Cloud Backup and Recovery**. Select a backup type from the left navigation pane.

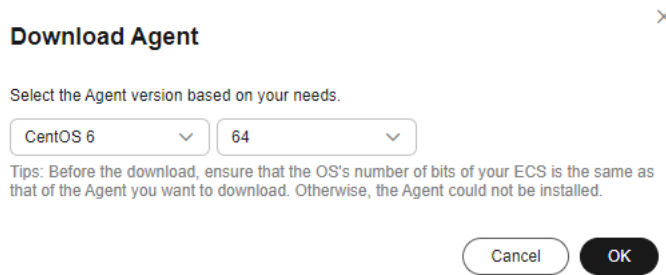
**Step 2** Click the **Agent Installation** tab.

**Figure 6-6** Installation page for Linux



**Step 3** In method 2, click **Download**. On the displayed download page, select the version to be downloaded based on the OS of the target ECS, and click **OK**. See [Figure 6-7](#).

**Figure 6-7** Downloading the Agent



- Step 4** After downloading the Agent to a local directory, check that the package's SHA256 value is the same as that listed in [Table 6-3](#).
- Step 5** Use a file transfer tool, such as Xftp, SecureFX, or WinSCP, to upload the Agent installation package to your ECS.
- Step 6** After the upload, go to the ECS page. Select the target server and click **Remote Login** in the **Operation** column to log in to the ECS.
- Step 7** Run the **tar -zxvf** command to decompress the Agent installation package to any directory and run the following command to go to the **bin** directory:  
**cd bin**
- Step 8** Run the following command to run the installation script:  
**sh agent\_install\_ebk.sh**
- Step 9** The system displays a message indicating that the client is installed successfully. See [Figure 6-8](#).

**Figure 6-8** Successful client installation for Linux

```



sus02@hona:~$ cd bin
sus02@hona:~/bin$ sh agent_install_ebk.sh
Begin to install Cloud Server Backup Service Agent.
Get address of Cloud Server Backup Service Agent.
The address listened by rcagent is 127.0.0.1:8051.
The address listened by rcagent is 0.0.0.0:8026.
Start Cloud Server Backup Service Agent.
Cloud Server Backup Service Agent was installed successfully.
*****
Important:
1. After the installation is successful, use the agentcli command to change the password of user sumit.
2. If the MySQL or SAP HANA database is installed, change the database login passwords in the scripts under directory /home/rdadmin/Agent/bin/thirdparty/ebk_user/.
For details, see the Database Backup Best Practices.
*****
sus02@hona:~/bin$
  
```

- Step 10** If the MySQL or SAP HANA database has been installed on the ECS, run the following command to encrypt the password for logging in to the MySQL or SAP HANA database:  
**/home/rdadmin/Agent/bin/agentcli encpwd**
- Step 11** Use the encrypted password in [previous step](#) to replace the database login password in the script in **/home/rdadmin/Agent/bin/thirdparty/ebk\_user/**.
- Step 12** After the installation is complete, Agent is running properly. To implement application-consistent backup for MySQL, SAP HANA, or other types of databases, modify or compile a custom script by referring to the *Cloud Backup and Recovery Best Practices*.

----End

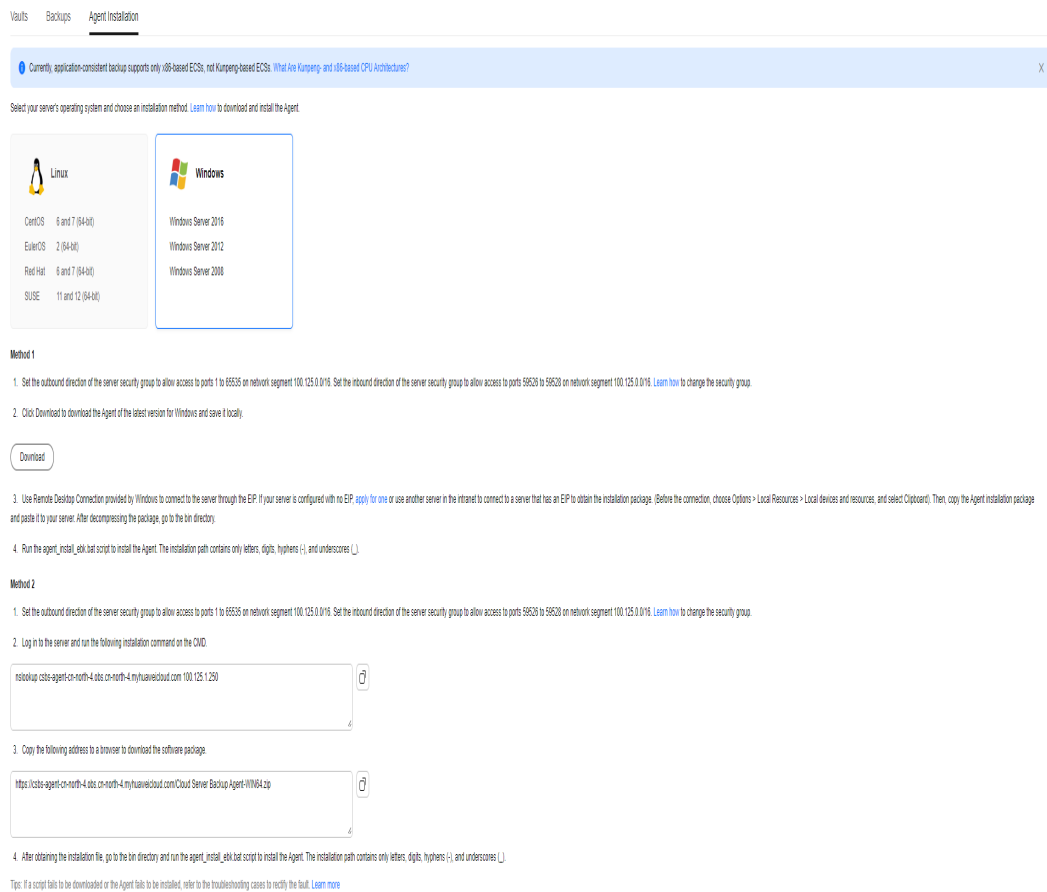
## Installing the Agent for a Windows OS (Method 1)

**Step 1** Log in to the CBR console.

1. [Log in to the management console.](#)
2. Click  in the upper left corner and select a region.
3. Click  and choose **Storage > Cloud Backup and Recovery**. Select a backup type from the left navigation pane.

**Step 2** Click the **Agent Installation** tab.

**Figure 6-9** Installation page for Windows



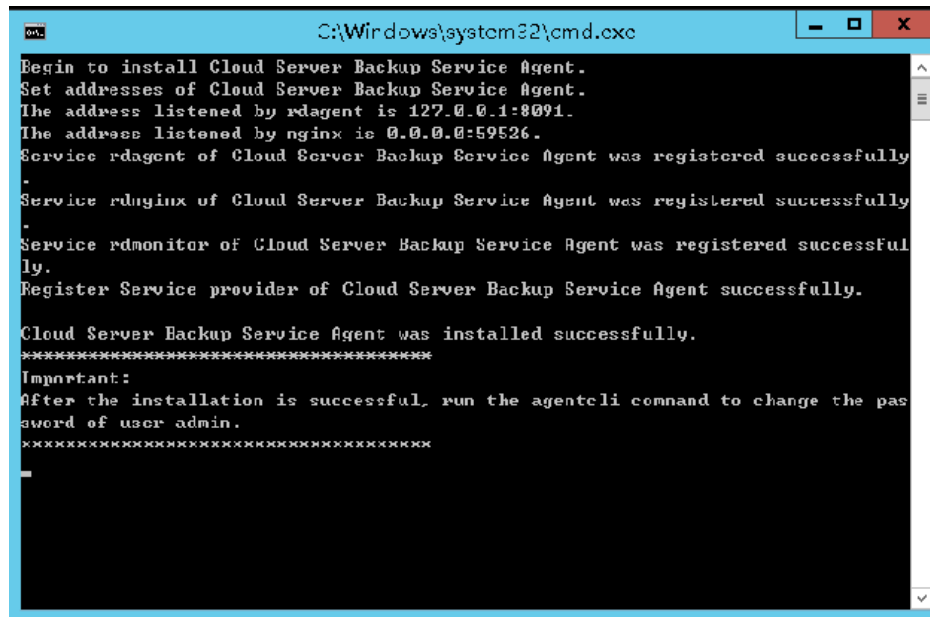
**Step 3** In method 1, click **Download**. Save the downloaded installation package to a local directory.

**Step 4** After downloading the Agent to a local directory, check that the package's SHA256 value is the same as that listed in [Table 6-3](#).

**Step 5** Use a file transfer tool, such as Xftp, SecureFX, or WinSCP, to upload the Agent installation package to your ECS.



- Step 6** Log in to the console and then log in to the ECS as the administrator.
- Step 7** Decompress the installation package to any directory and go to the *Installation path*\bin directory.
- Step 8** Double-click the **agent\_install\_ebk.bat** script to start the installation.
- Step 9** The system displays a message indicating that the client is installed successfully. See [Figure 6-10](#).

**Figure 6-10** Successful client installation for Windows



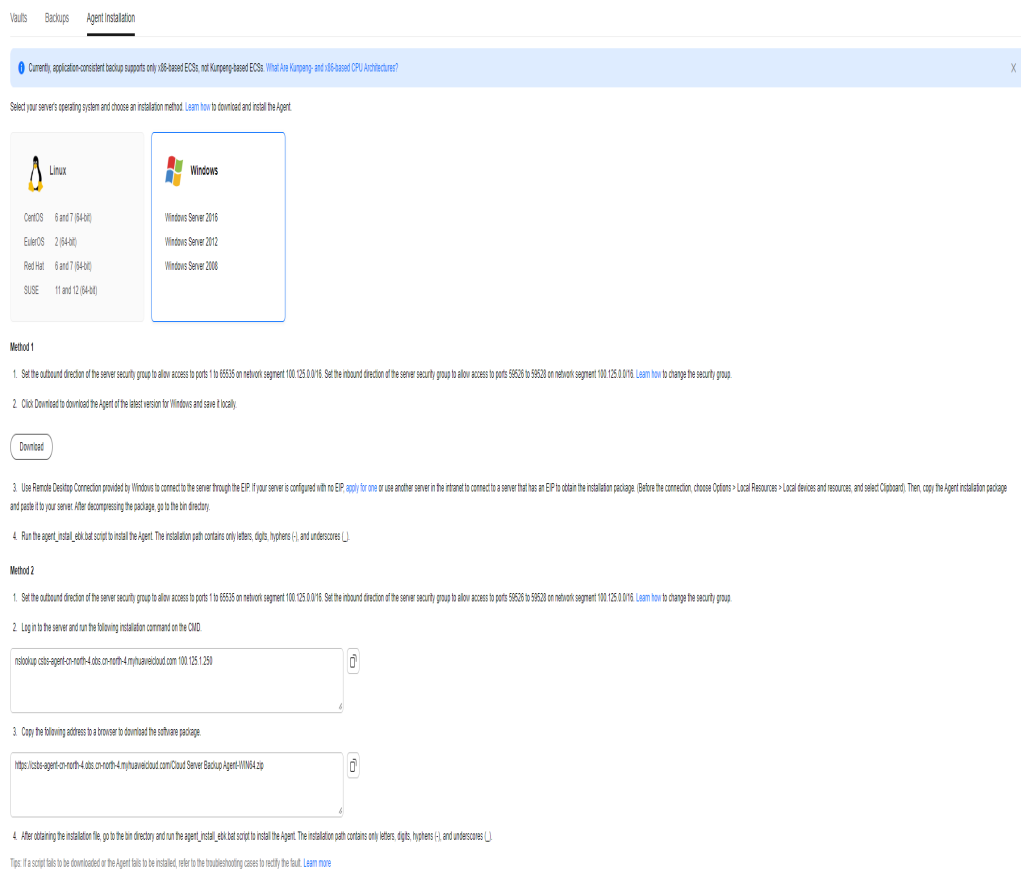
----End

## Installing the Agent for a Windows OS (Method 2)

- Step 1** Log in to the CBR console.
  1. [Log in to the management console](#).
  2. Click  in the upper left corner and select a region.
  3. Click  and choose **Storage > Cloud Backup and Recovery**. Select a backup type from the left navigation pane.
- Step 2** Click the **Agent Installation** tab.

**Figure 6-11** Installation page for Windows





**Step 3** On the ECS page, select the target server and click **Remote Login** in the **Operation** column to log in to the ECS as the administrator.

**Step 4** Copy the installation commands in step 2 of method 2 to the server and run the command in the Command Prompt.

**Step 5** Copy the installation command in step 3 of method 2 to the browser. The following uses **ap-southeast-1** as the example region. Then press **Enter** to download the installation package.

**https://csbs-agent-ap-southeast-1.obs.ap-southeast-1.myhwclouds.com/Cloud Server Backup Agent-WIN64.zip**

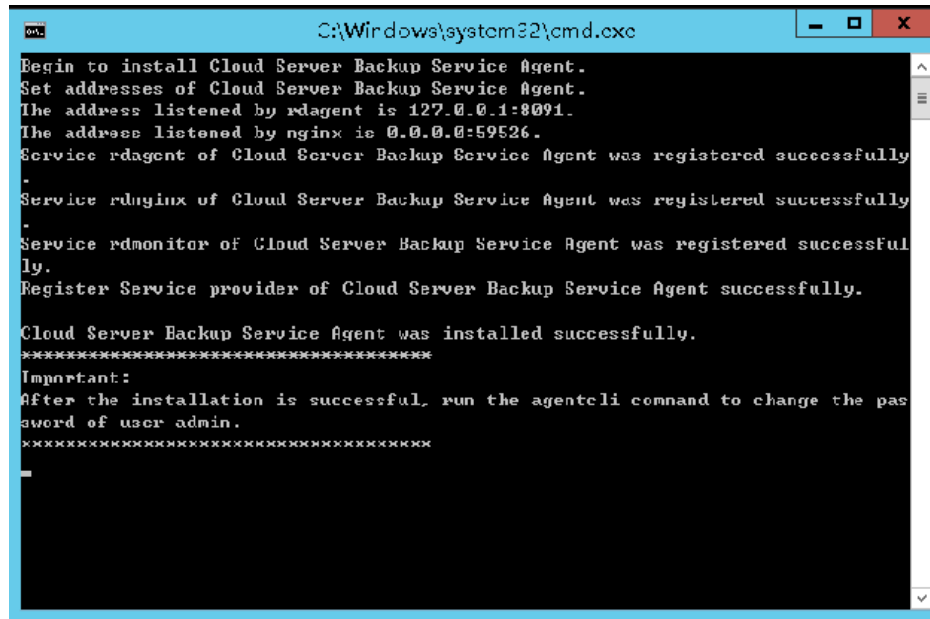
**Step 6** After downloading the Agent to a local directory, check that the package's SHA256 value is the same as that listed in **Table 6-3**.

**Step 7** Decompress the file to obtain the installation file. Decompress the installation package to any directory and go to the *Installation path*\bin directory.

**Step 8** Double-click the **agent\_install\_ebk.bat** script to start the installation.

**Step 9** The system displays a message indicating that the client is installed successfully. See **Figure 6-12**.

Figure 6-12 Successful client installation for Windows



----End

## 6.4 Creating an Application-Consistent Backup



Cloud server backup supports application-consistent backup in addition to crash-consistent backup. You can use cloud server backup to back up ECSs running MySQL or SAP HANA databases, because application-consistent backup ensures that the backed-up data is transactionally consistent.

### Constraints

- Application-consistent backup is currently not supported for cluster applications, such as, MySQL Cluster. It is supported only for applications on standalone servers.
- You are advised to perform application-consistent backup in off-peak hours.

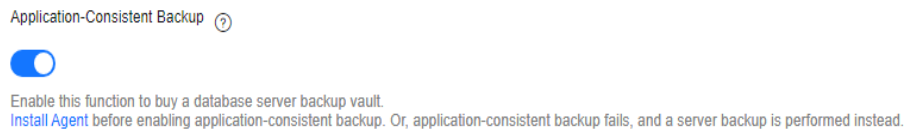
### Procedure

**Step 1** Log in to the CBR console.

1. [Log in to the management console.](#)
2. Click  in the upper left corner and select a region.
3. Click  and choose **Storage > Cloud Backup and Recovery**. Select a backup type from the left navigation pane.

**Step 2** Create a vault for application-consistent backups by referring to "Purchasing a Server Backup Vault" in [Creating a Cloud Server Backup](#). Select **Enable** for **Application-Consistent Backup**.

**Figure 6-13** Enabling Application-Consistent Backup



**Step 3** Associate the cloud servers with the created vault. Ensure that the Agent has been installed on the servers.

**Step 4** Create a cloud server backup by referring to [Creating a Cloud Server Backup](#).

- If an application-consistent backup is created successfully, a blue letter "A" is displayed next to the backup name in the backup list.
- If an application-consistent backup fails to be created, the system automatically creates a cloud server backup instead and stores the backup in the vault, and a gray letter "A" is displayed next to the backup name in the backup list. You can view the failure cause in the **Management Information** area on the backup details page. See [Figure 6-14](#).

**Figure 6-14** Application-consistent backup status

Name/ID	Status	Backup...
<input type="checkbox"/> autobk_7440 88b0717f-6127-4034-8fb6-123a3784b47b	Application-consistent backup failed. <span style="border: 1px solid gray; padding: 2px;">A</span>	Available Incremental ...
<input type="checkbox"/> autobk_f3e1 be2f8491-3d82-4b23-a4f2-7162ec7855c4	Application-consistent backup succeeded. <span style="border: 1px solid blue; padding: 2px;">A</span>	Available Incremental ...

**Step 5** Return to the cloud server backup page as prompted. If the backup execution fails, rectify the fault based on the failure details shown on the page.

----End

## Follow-up Procedure

If data is lost due to virus attacks or database faults, you can restore the data by following instructions in [Restoring Data Using a Cloud Server Backup](#) and [Using a Backup to Create an Image](#).

## 6.5 Uninstalling the Agent

### Scenarios

This section describes how to uninstall the Agent when application-consistent backup is no longer needed.

### Prerequisites

The username and password for logging in to an ECS have been obtained.

## Uninstalling the Agent for Linux

- Step 1** Log in to the ECS and run the `su -root` command to switch to user `root`.
- Step 2** In the `home/rdadmin/Agent/bin` directory, run the following command to uninstall the Agent. [Figure 6-15](#) displays an example. If the word **successfully** in green is displayed, the Agent is uninstalled successfully.

```
sh agent_uninstall_ebk.sh
```

**Figure 6-15** Agent uninstalled successfully from Linux

```

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

----End

## Uninstalling the Agent for Windows

- Step 1** Log in to the ECS.
- Step 2** In the `Installation path/bin` directory, double-click `agent_uninstall_ebk.bat`. The window for uninstalling the Agent is displayed.

After the uninstallation is complete and successful, the window will be automatically closed. See [Figure 6-16](#).

**Figure 6-16** Agent uninstalled successfully from Windows

```

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

----End

# 7 File Backup (Supported Conditionally)

## 7.1 File Backup

 NOTE

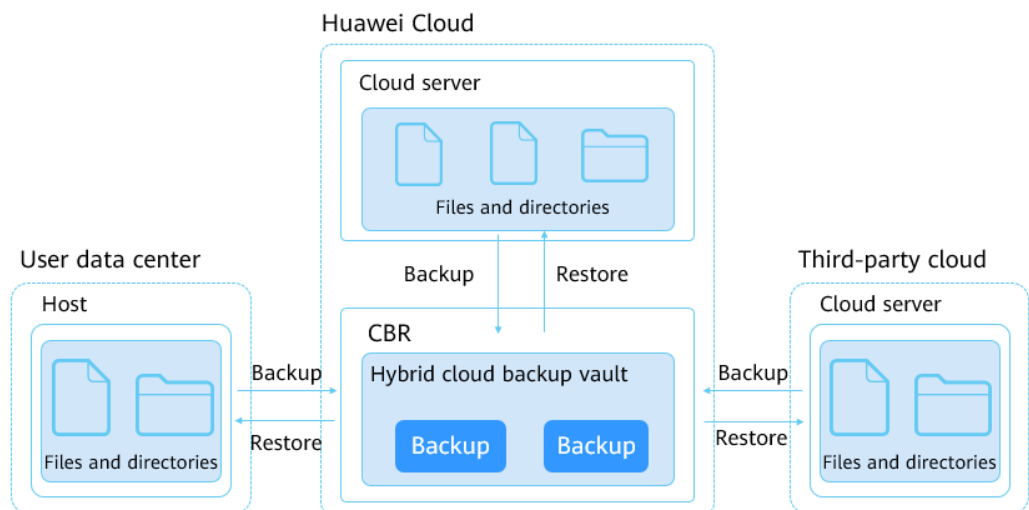
File backup is **supported conditionally**.

### Overview

CBR provides file backup which allows you to back up files and directories on your cloud servers and on-premises hosts, so you do not have to back up your entire servers or disks. Cloud servers that file backup supports can be servers on Huawei Cloud or a third-party cloud. If an accidental deletion or error occurred on your file, you can restore data to any time in the past when a backup was created.

[Figure 7-1](#) shows the file backup architecture.

**Figure 7-1** File backup architecture



## File Backup Scope

**Table 7-1** lists the supported OSs for on-premises hosts.

**Table 7-1** OSs that support file backup

OS	Supported Version
Windows Server	Windows Server 2019 for x86_64 Windows Server 2016 for x86_64 Windows Server 2012 for x86_64
Windows	Windows 10 Windows 7
CentOS	CentOS 7
EulerOS	EulerOS 2.5

## Differences Between SFS Turbo Backup and File Backup

Item	SFS Turbo Backup	File Backup
Backup and restore object	SFS Turbo file systems	One or more files on cloud servers and on-premises hosts
Backup unit	SFS Turbo file system	File
Vault type	SFS Turbo backup vault	Hybrid cloud backup vault
Recommended scenario	Data in the SFS Turbo file systems needs to be protected. The backup data is not stored in the file system and can be used to create new file systems when needed.	One or more files on cloud servers and on-premises hosts need to be protected, and data can be quickly backed up and restored on the cloud.

## File Backup Constraints

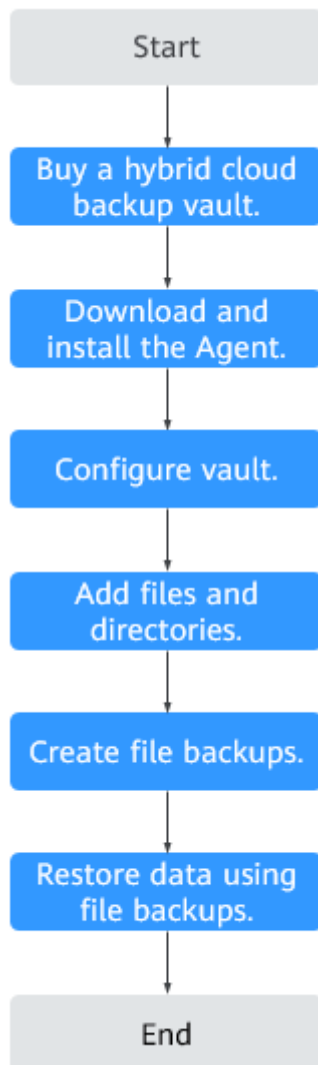
- Before backing up a file, ensure that the file is not being used or changed by an application, and the backup client has the read permissions on this file. Otherwise, the backed-up data will be incomplete.
- Before backing up a file, ensure that the file is not being used or changed by a process, and the backup client has the read permissions on this file. Otherwise, the backed-up data will be incomplete.
- You are advised not to restore file backups when applications are running. Stop the applications and then restore files.
- One backup client can have a maximum of 8 files and directories added.

- Each resource can only have one Agent installed.
- The number of resources where the Agent can be installed is not limited.
- A single directory can contain a maximum of 500,000 files, and you are advised to reserve at least 4 GB of memory on each backup client to perform file backups.
- One path can contain a maximum of 200 characters.
- The maximum bandwidth allowed for file backup data transmission is 16 Gbit/s. If the maximum bandwidth is reached, flow control will be triggered.
- File backup cannot back up the files stored in SFS file systems that are mounted to cloud servers.
- Backup may fail on directories with frequent file writes in Windows.
- At least 50 Mbit/s network bandwidth is required in cross-cloud or cross-region scenarios.
- Root directories of Windows hosts or servers, such as **C:\** and **D:\** cannot be backed up.

## 7.2 File Backup Process

[Figure 7-2](#) shows the file backup process.

**Figure 7-2** File backup process



1. Create a hybrid cloud backup vault.  
Before installing the file backup Agent, create a vault. The created vault will be used to store generated file backups.
2. Download and install the Agent.  
Install the Agent on target servers. After the Agent is successfully installed, the servers automatically appear as backup clients in the backup client list.
3. Configure a vault.  
Configure a vault for the backup clients. Generated file backups will be stored in this vault.
4. Add files and directories.  
Add the files and directories you want to back up.
5. Create file backups.  
Manually perform backups or have the system automatically create backups. Generated backups will be stored in the vault.



6. Restore data from file backups.



Restore data by referring to [Restoring from a File Backup](#). You can restore data to source servers or different servers.

## 7.3 Creating a Hybrid Cloud Backup Vault

This section describes how to purchase a hybrid cloud backup vault for storing file backups.

### Procedure

**Step 1** Log in to the CBR console.

1. Log in to the management console.
2. Click  in the upper left corner and select a region.
3. Click  and choose **Storage > Cloud Backup and Recovery > File Backups**.

**Step 2** In the upper right corner of the page, click **Buy Hybrid Cloud Backup Vault**.

**Step 3** Select a billing mode.

- Yearly/monthly is a prepaid billing mode. You are billed based on the subscription duration you specify. This mode is ideal when the resource use duration is predictable. A longer subscription often means a lower cost.
- Pay-per-use is a postpaid billing mode. You are billed based on your resource usage and you can increase or delete resources anytime.

**Step 4** Specify a vault capacity ranging from 1 to 10,240 TB.

Properly plan the vault capacity, which must be at least the same as the size of the files you want to back up. Check the file size on your local hosts. As the vault's used space grows, you can expand the vault capacity if it becomes insufficient.

**Step 5** Configure auto backup.

- If you select **Configure**, you must then select an existing backup policy or create a new policy. After the vault is created, CBR will apply the policy to this vault, and all files associated with this vault will be automatically backed up based on this policy.
- If you select **Skip**, files associated with this vault will not be automatically backed up until you apply a backup policy to the vault.

**Step 6** (Optional) Add tags to the vault.

Tags are key-value pairs, which are used to identify, classify, and search for vaults. You can add a maximum of 10 tags for a vault, and vault tags are only used for vault search and management.

[Table 7-2](#) describes the parameters of a tag.

**Table 7-2** Tag parameter description

Parameter	Description	Example Value
Key	<p>Each tag has a unique key. You can customize a key or select the key of an existing tag created in TMS.</p> <p>A tag key:</p> <ul style="list-style-type: none"> <li>• Can contain 1 to 36 Unicode characters.</li> <li>• Can contain only letters, digits, hyphens (-), and underscores (_).</li> </ul>	Key_0001
Value	<p>A tag value can be repetitive or left blank.</p> <p>A tag value:</p> <ul style="list-style-type: none"> <li>• Can contain 0 to 43 Unicode characters.</li> <li>• Can contain only letters, digits, hyphens (-), and underscores (_).</li> </ul>	Value_0001

**Step 7** Specify a name for the vault.

The name must contain 1 to 64 characters including digits, letters, underscores (\_), or hyphens (-), for example, **vault-f61e**.

 **NOTE**

You can also use the default name **vault\_xxxx**.

**Step 8** Specify the required duration if you select yearly/monthly billing. The validity period ranges from 1 month to 5 years.

Determine whether to enable auto renewal. If you select **Auto Renewal**:

- Your subscription will be renewed each month for monthly billing.
- Your subscription will be renewed each year for yearly billing.

**Step 9** Complete the payment as prompted.

**Step 10** Go back to the **File Backups** page and view the created vault in the vault list.

----End

## 7.4 Downloading and Installing the Agent



### Scenarios

Before backing up files, you need to change the security group of the target servers or VMs, and install the Agent on them. This section describes how to download and install the Agent.

Currently, only hosts running 64-bit OSs are supported.

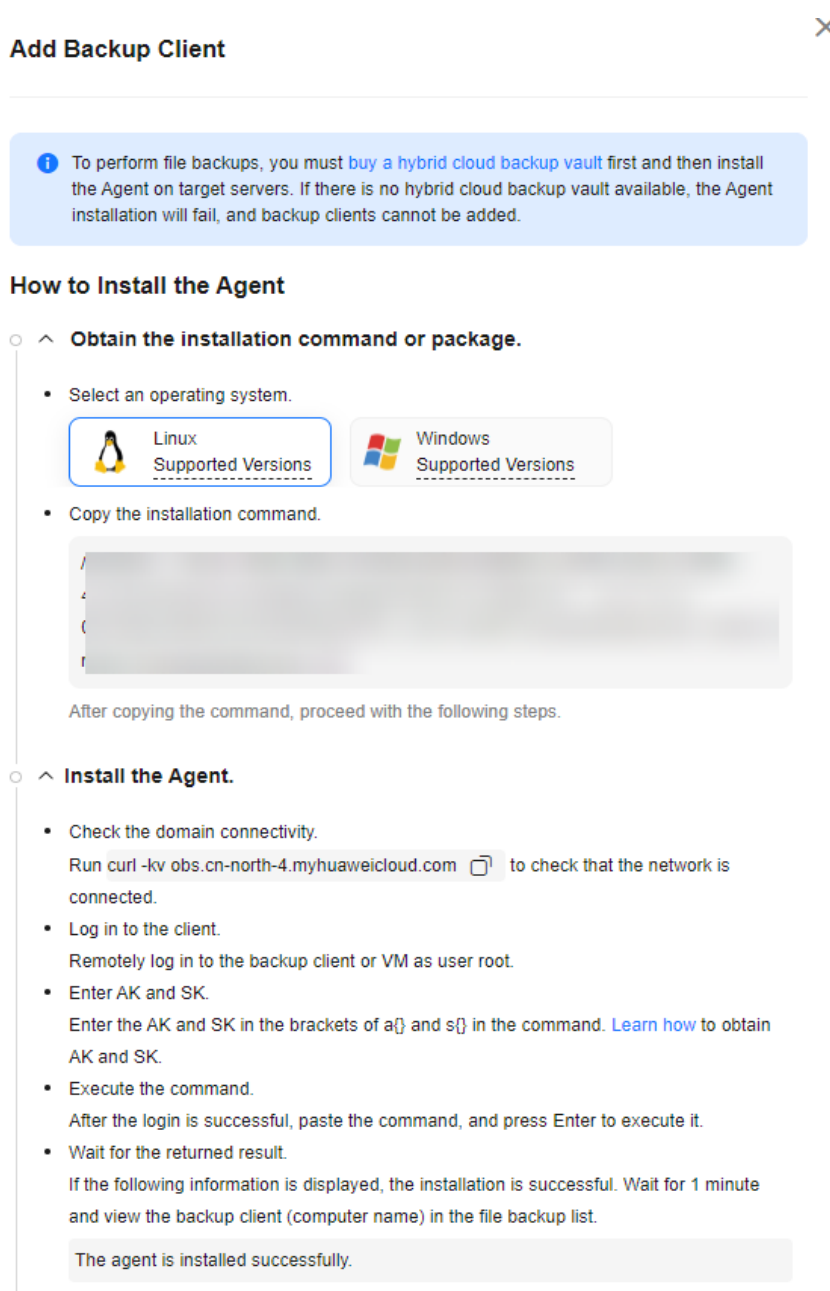
## Procedure for Downloading and Installing the Agent in Linux

**Step 1** Log in to the CBR console.

1. Log in to the management console.
2. Click  in the upper left corner and select a region.
3. Click  and choose **Storage > Cloud Backup and Recovery > File Backups**.

**Step 2** Click the **Backup Clients** tab and locate the target backup client. Click **Add Backup Client**. On the displayed page, select Linux.

Figure 7-3 Linux



- Step 3** Log in to the target host as user **root**.
- Step 4** On the host, run **curl -kv obs.Region ID.myhuaweicloud.com** to check that the network is connected. Replace *Region ID* with the ID of the region you select.
- Step 5** Complete the wget **https://obs.region1.myhuaweicloud.com/cbr/deploy/cbragent/install\_cbr\_agent.sh** command and run the command on the server to download the sh script. Then check that the script's SHA256 value is the same as that listed in [Table 7-3](#).

**Table 7-3** SHA256 values

Package/Script Name	SHA256 Value	OS
cbragent_WIN64.zip	6ebf82287550e25c765c92bc9212e21e2d65e0ddb508bc91448735b68d2cb62f	Windows
cbragent_linux_x86_64.tar.gz	c79e0345c3e0d6da632beaf722221c6eae7b7ec1f867095575d27988f1224d	Linux
install_cbr_agent.sh	17347eaa21bfbffbbba2a5c25006d779977aea8c2df63127fc7887f42a6ba139f	Linux

- Step 6** Complete the installation command provided on the CBR console.

```
/bin/bash -c "$(curl -kfsSL https://cbr-files-backup-agents-cn-north-7.obs.cn-north-7.myhuaweicloud.com/deploy/cbragent/install_cbr_agent.sh)" -- -a {} -s {} -p 3bdb0a1c35d64fe9a68235c53bed4a86 -c cbr.cn-north-7.myhuaweicloud.com -o obs.cn-north-7.myhuaweicloud.com
```

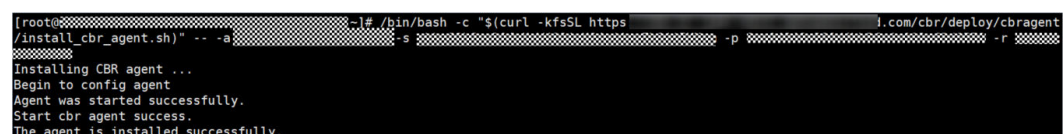
- Copy the region ID from the installation page to replace variable *region id*.
- Enter the AK and SK in the brackets of **a {}** and **s {}** in the command. [How to obtain an AK/SK?](#)

**NOTE**

Delete the brackets after entering the AK and SK.

- Step 7** Run the obtained command on the host to install the Agent.
- Step 8** If information similar to the following is displayed, the Agent is successfully installed.

**Figure 7-4** Executing the installation command





- Step 9** Wait for about 1 minute, and view the backup client in the backup client list. If the Agent status is **Normal**, the system successfully detects the client, and the Agent is running properly.

----End

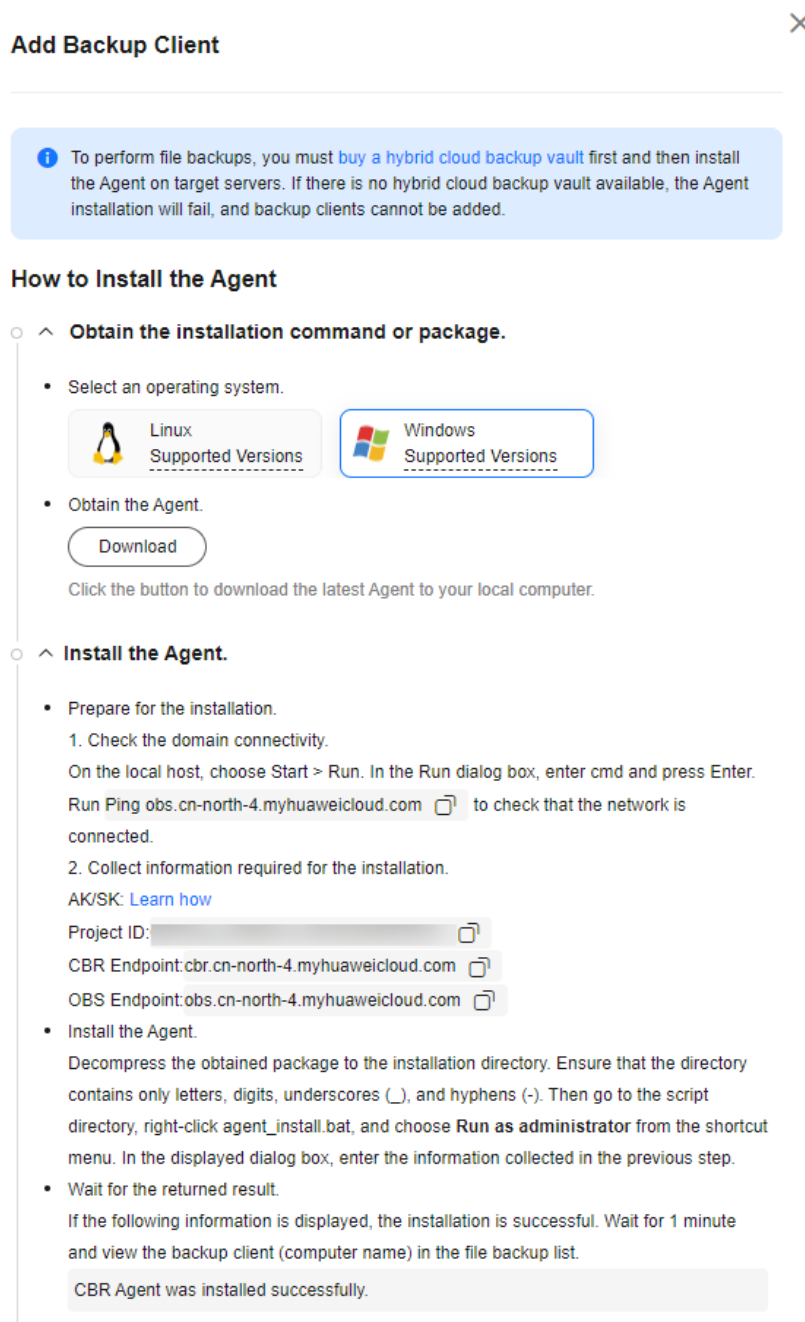
## Procedure for Downloading and Installing the Agent in Windows

**Step 1** Log in to the CBR console.

1. Log in to the management console.
2. Click  in the upper left corner and select a region.
3. Click  and choose **Storage > Cloud Backup and Recovery > File Backups**.

**Step 2** Click the **Backup Clients** tab and locate the target backup client. Click **Add Backup Client**. On the displayed page, select Windows.

Figure 7-5 Windows



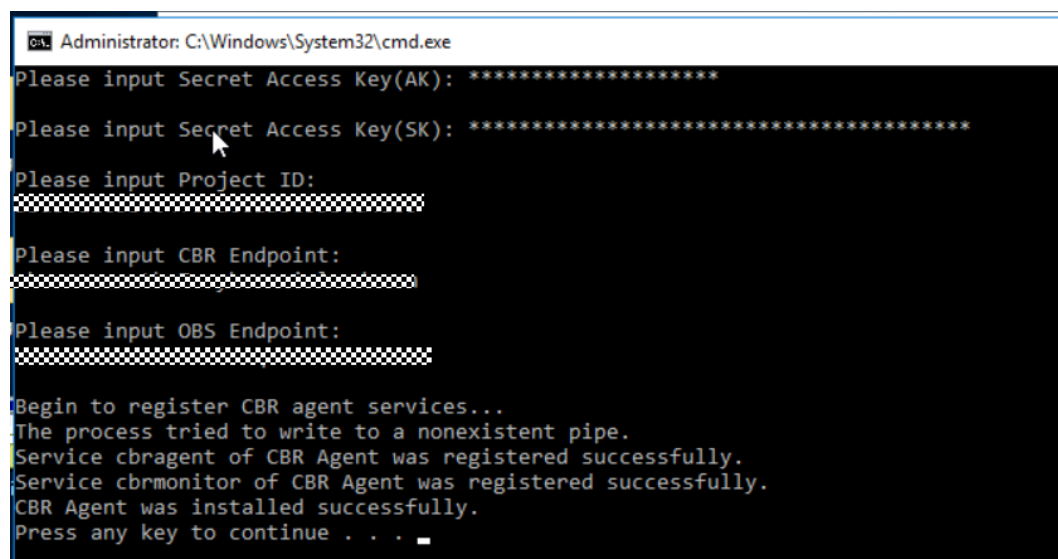
**Step 3** Click **Download** to download the latest Agent installation package to the local computer. Ensure that the package's SHA256 value is the same as that listed in [Table 7-3](#).

**Step 4** On the local host, choose **Start > Run**. In the **Run** dialog box, enter **cmd** and press **Enter**.

On the host, run **ping obs.Region ID.myhuaweicloud.com** to check that the network is connected. Replace *Region ID* with the ID of the region you select. For example, if you select CN North-Beijing4, replace it with **cn-north-4**.

- Step 5** Decompress the obtained package to the installation directory. Then go to the **script** directory, right-click **agent\_install.bat**, and choose **Run as administrator** from the shortcut menu. In the displayed dialog box, enter the following information.
- Step 6** Ensure that the installation path contains only letters, digits, underscores (\_), or hyphens (-). See [Figure 7-6](#).
- **access\_key**: Enter your AK. [How to obtain an AK/SK?](#)
  - **secret\_key**: Enter your SK. [How to obtain an AK/SK?](#)
  - **project\_id**: Copy the project ID from the installation page.
  - **CBR Endpoint**: Copy the CBR endpoint from the installation page.
  - **OBS Endpoint**: Copy the OBS endpoint from the installation page.

**Figure 7-6** Executing the installation command





- Step 7** After "CBR Agent was installed successfully" is returned, wait for about 1 minute, go back to the backup client list, and find the backup client. If its Agent status is **Normal**, the Agent has been installed successfully.

----End

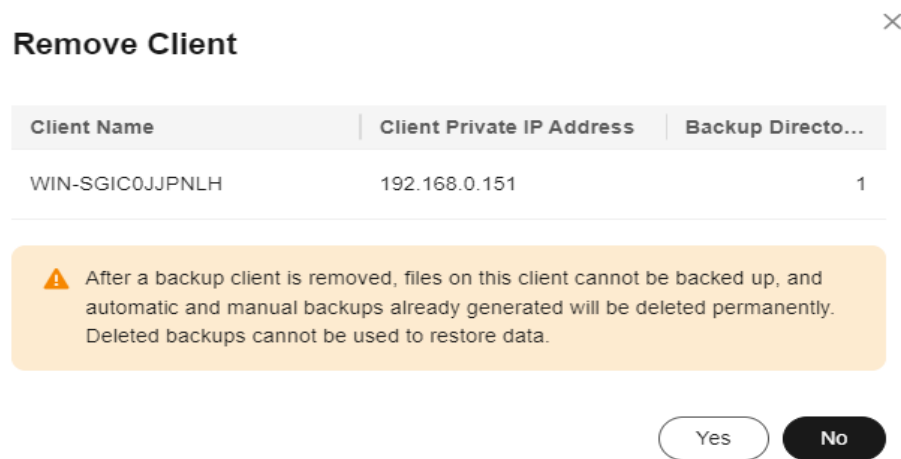
## Removing a Client

If a backup client is no longer needed, you can remove it.

- Step 1** Log in to the CBR console.
1. Log in to the management console.
  2. Click  in the upper left corner and select a region.
  3. Click  and choose **Storage > Cloud Backup and Recovery > File Backups**.
- Step 2** Click the **Backup Clients** tab and locate the target backup client. Locate the row that contains the target backup client, click **More** in the **Operation** column, and choose **Remove Client**. See [Figure 7-7](#).

After a backup client is removed, files on this client cannot be backed up, and automatic and manual backups already generated will be deleted permanently. Deleted backups cannot be used to restore data.

**Figure 7-7** Remove Client



**Step 3** Click **Yes**.

----End



## 7.5 Configuring a File Backup Vault

### Scenarios

After the system discovers backup clients, configure a vault for each client to have the backups automatically stored to the vault.

### Procedure

**Step 1** Log in to the CBR console.

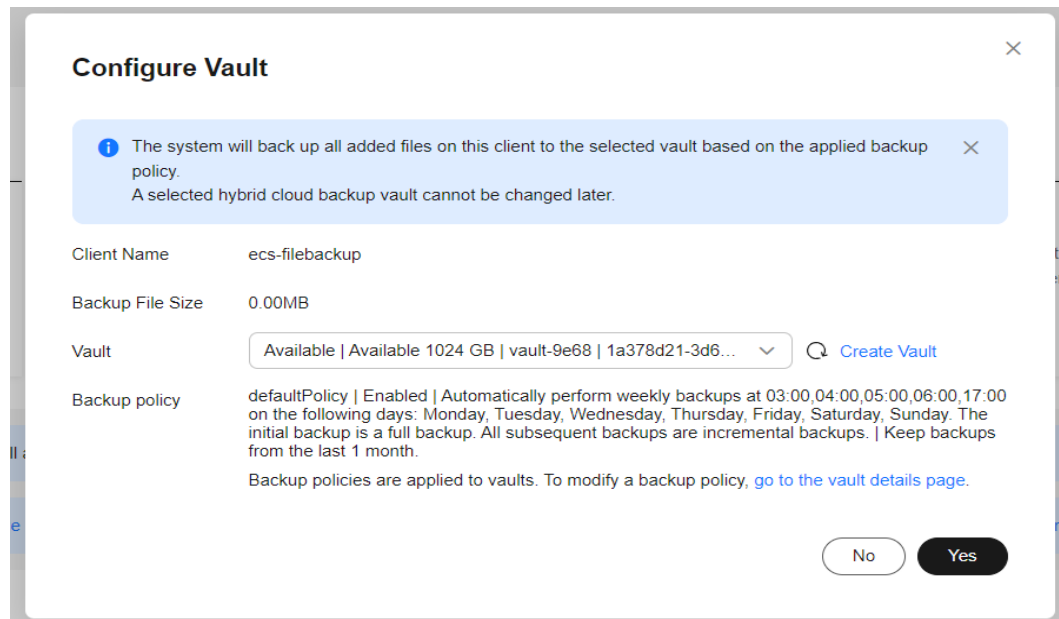
1. Log in to the management console.
2. Click  in the upper left corner and select a region.
3. Click  and choose **Storage > Cloud Backup and Recovery > File Backups**.

**Step 2** Click the **Backup Clients** tab and locate the target backup client. Then, click **Configure Vault** in the **Backup Configuration** column.

**Step 3** On the displayed page, select a vault. See [Figure 7-8](#).



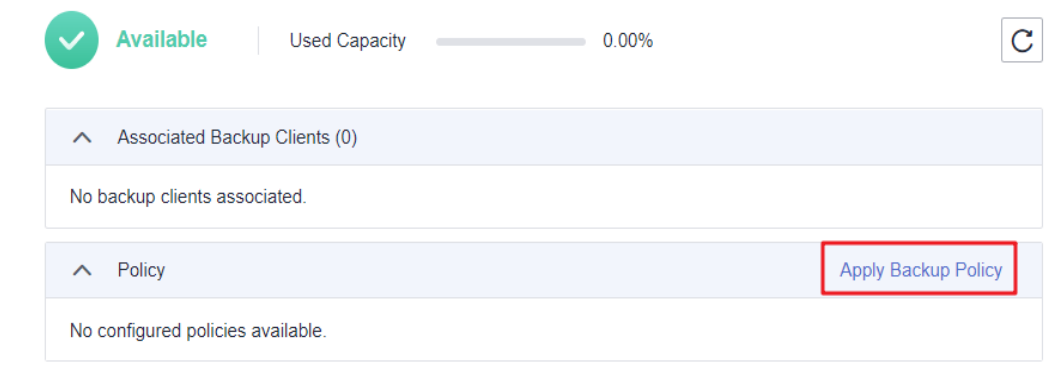
Figure 7-8 Configure Vault



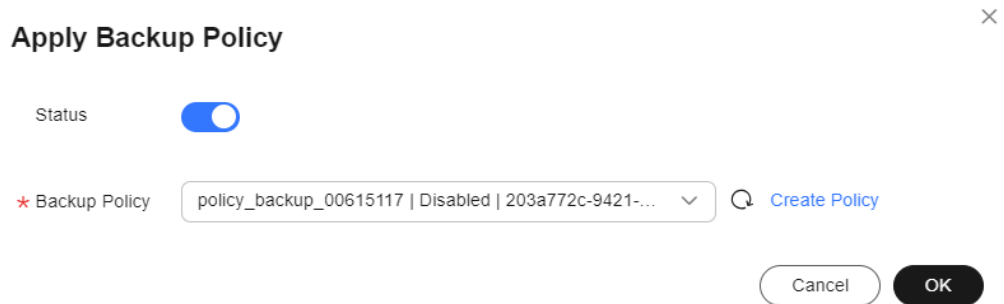
**Step 4** Click **Yes**. View the configured vault in the **Backup Configuration** column of the backup client list.

**Step 5** (Optional) If a backup policy is not applied when you create the hybrid cloud backup vault and now you want to configure auto backup for backup clients, click the vault name in the **Backup Configuration** column and apply a backup policy to the vault. See [Figure 7-9](#).

Figure 7-9 Apply Policy



**Step 6** (Optional) Click **Apply Backup Policy**. Select an existing backup policy or create a new one. See [Figure 7-10](#).

**Figure 7-10** Apply Policy

**Step 7** (Optional) Click **OK**. The policy is successfully applied to the hybrid cloud backup vault.

----End

## 7.6 Adding Directories

### Scenarios



After the Agent is installed on target servers, CBR will automatically detect and show the servers as backup clients in the backup client list under **Cloud Backup and Recovery > File Backups > Backup Clients**. You need to add the paths of the files and directories you want to back up.

### Constraints

- A backup client can have a maximum of 100 directories added.
- A single directory can contain a maximum of 500,000 files, and you are advised to reserve at least 4 GB of memory on each backup client to perform file backups.
- A path must be an absolute path, for example, a path starting with /, C:\, or D:\.
- Root directories of Windows hosts or servers, such as **C:\** and **D:\** cannot be backed up.

### Procedure

**Step 1** Log in to the CBR console.

1. Log in to the management console.
2. Click  in the upper left corner and select a region.
3. Click  and choose **Storage > Cloud Backup and Recovery > File Backups**.

**Step 2** Locate the target backup client and click its name to go to the details page.

**Step 3** Click **Add Backup Directory**. See [Figure 7-11](#).

**Figure 7-11 Add Backup Directory**

**Step 4** Paste the paths to the text box and click **OK**.


**Step 5** The file paths will be displayed in the lower part of the page.

----End

## Removing Directories

If backup is no longer required for a directory or the maximum number of directories allowed has been reached, you can remove directories.

**Step 1** Log in to the ECS console.

1. Log in to the management console.
2. Click  in the upper left corner and select a region.
3. Choose **Storage > Cloud Backup and Recovery > File Backups**.

**Step 2** Locate the target backup client and click its name to go to the details page.

**Step 3** Locate the target directory and click **Remove Directory**. See [Figure 7-12](#).

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

**Figure 7-12 Remove Directory**

Backup Directory	Client Name	Private IP Address
C:\Users\Administrator\Desktop\c...	WIN-SGIC0JJPNLH	192.168.0.151

**Step 4** Click **Yes**.

----End

## 7.7 Creating File Backups

### Scenarios

This section describes how to manually create file backups.


To implement automatic backup, create a policy and apply it to a vault by referring to [Creating a Backup Policy](#). Then, CBR will automatically perform backups at the time points specified in the policy.

### Constraints

Only backup clients whose Agent status is **Normal** can be backed up.

### Procedure

**Step 1** Log in to the CBR console.

1. Log in to the management console.
2. Click  in the upper left corner and select a region.
3. Choose **Storage > Cloud Backup and Recovery > File Backups**.

**Step 2** Click the **Backup Clients** tab and locate the target backup client.

**Step 3** Click **Perform Backup** in the **Operation** column. CBR automatically creates backups for the files.

**Step 4** On the **Backup Clients** tab page, click the name of the target backup client. In the **Backup Details** area of the displayed page, if the statuses of all generated backups are **Available**, the backup task is successful.

#### NOTE

If you delete data from the files during the backup, the deleted files may fail to be backed up. Therefore, to ensure data integrity, delete the target data after the backup is complete, and then perform the backup.

After the backup task is complete, you can restore file data by referring to [Restoring from a File Backup](#) as needed.

----End

## 7.8 Restoring from a File Backup


You can use a file backup to restore individual files of a server to its state when the backup was created.

## Constraints

- The Agent on the server must be **Normal**.
- You are advised not to restore file backups when applications are running. Stop the applications and then restore files.

## Method 1

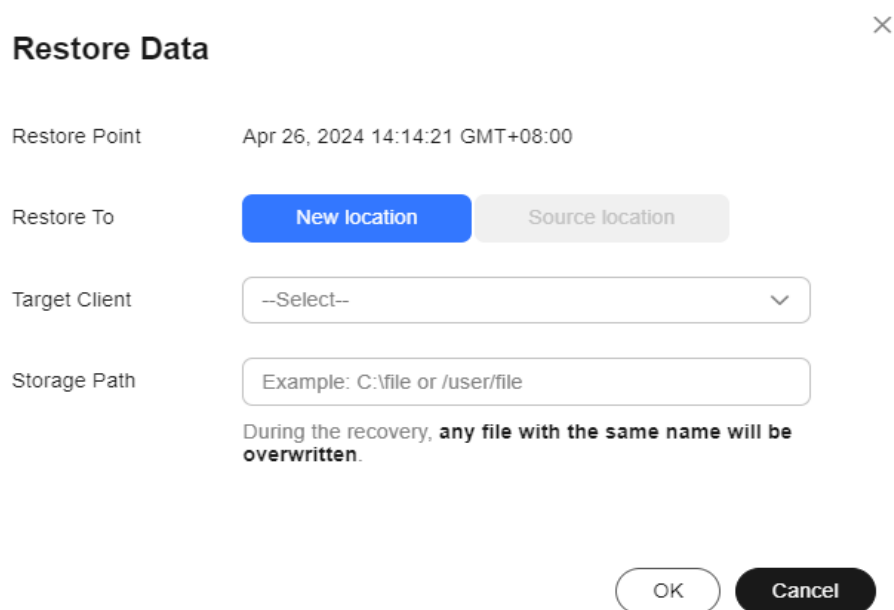
**Step 1** Log in to the CBR console.

1. Log in to the management console.
2. Click  in the upper left corner and select a region.
3. Choose **Storage > Cloud Backup and Recovery > File Backups**.

**Step 2** On the **Backup Clients** tab page, click the name of the target backup client.

**Step 3** Find the desired backup and click **Restore Data**. See [Figure 7-13](#).

**Figure 7-13** Restoring files



**Restore Data** ×

Restore Point Apr 26, 2024 14:14:21 GMT+08:00

Restore To New location Source location

Target Client --Select-- ▼

Storage Path Example: C:\file or /user/file

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

OK Cancel

**Step 4** Select a restore location.

- **Source location:** Data will be restored to the original file path, and any file with the same name will be overwritten. This option is available only for Linux backup clients.
- **New location:** Data will be restored to a different server you select. You can only choose from the backup clients whose Agent status is **Normal**. If your target server is not on the list, install the Agent on the server and try again.

### NOTE

The storage path cannot contain spaces.


**Step 5** Click **OK**. You can check whether data is successfully restored in the **Backup Details** area of the client details page or on the local host.

When the status of the backup changes to **Available**, the restoration is successful.

----End

## Method 2

**Step 1** Log in to the CBR console.

1. Log in to the management console.
2. Click  in the upper left corner and select a region.
3. Choose **Storage > Cloud Backup and Recovery > File Backups**.

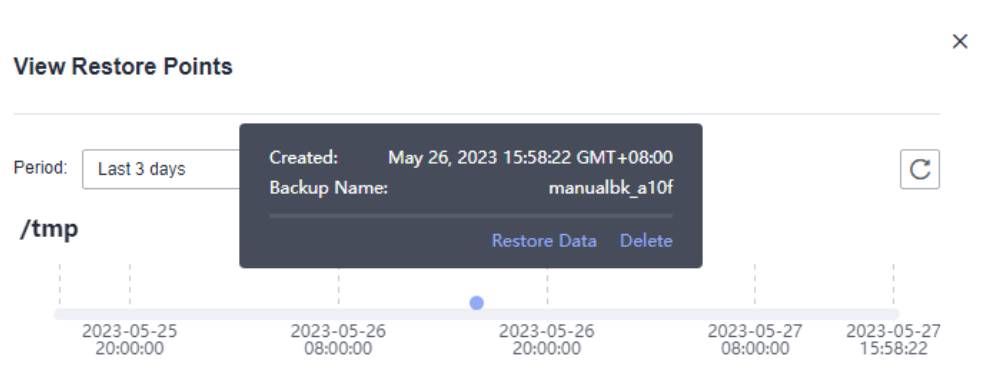
**Step 2** On the **Backup Clients** tab page, locate the name of the target backup client.

**Step 3** Click **Restore Points** in the **Operation** column.

**Step 4** Select a restore point and click **Restore Data**. See [Figure 7-14](#).

Backup data will be restored to the state at the selected time.

**Figure 7-14** Restore Points



**Step 5** Select a restore location.

- **Source location:** Data will be restored to the original file path, and any file with the same name will be overwritten. This option is available only for Linux backup clients.
- **New location:** Data will be restored to a different server you select.  
You can only choose from the backup clients whose Agent status is **Normal**. If your target server is not on the list, install the Agent on the server and try again.

**Step 6** Click **OK**. You can check whether data is successfully restored in the **Backup Details** area of the client details page or on the local host.

When the status of the backup changes to **Available**, the restoration is successful.

----End

## 7.9 Uninstalling the Agent

### Scenarios

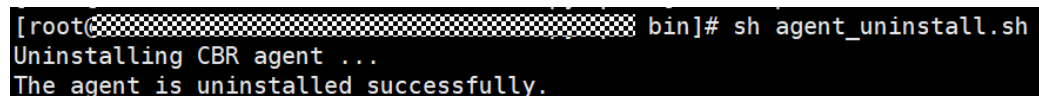
Uninstall the Agent from a backup client if file backup is no longer needed.

### Uninstalling the Agent from Linux

- Step 1** Log in to the server whose Agent needs to be uninstalled and run **su - root** to switch to user **root**.
- Step 2** In the **/opt/huaweicloud/cbragent/bin** directory, run the following command to uninstall the Agent. If information similar to **Figure 7-15** is displayed, the Agent has been uninstalled.

```
sh agent_uninstall.sh
```

Figure 7-15 Agent uninstalled from Linux



```
[root@... bin]# sh agent_uninstall.sh
Uninstalling CBR agent ...
The agent is uninstalled successfully.
```

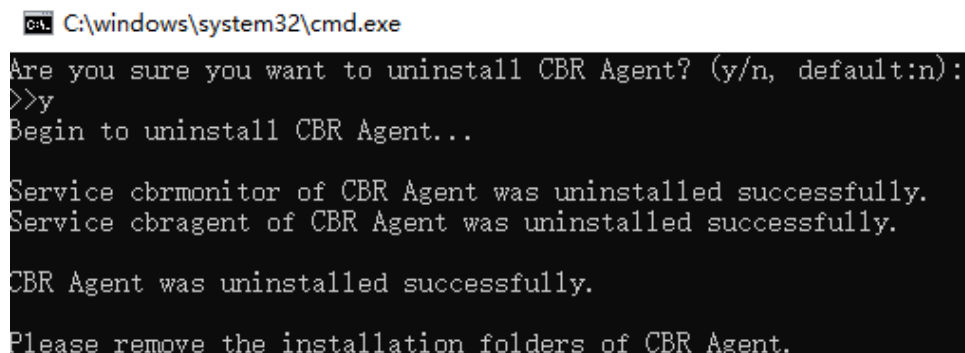
----End

### Uninstalling the Agent from Windows

- Step 1** Log in to the server whose Agent needs to be uninstalled.
- Step 2** Go to the **bin** directory in the installation path and double-click **agent\_uninstall.bat**. Enter **y** to uninstall the Agent.

If information similar to **Figure 7-16** is displayed, the Agent has been uninstalled.

Figure 7-16 Agent uninstalled from Windows



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

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

CBR Agent was uninstalled successfully.

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

----End

## 7.10 Troubleshooting Cases

### Context

You may encounter an Agent installation failure or exception after the Agent is installed. This section describes some common troubleshooting cases to help you quickly locate the problem.

### Abnormal Agent Status

#### Symptom:

After the Agent has been installed, the Agent status was displayed as Abnormal in the client list.

#### Possible cause:

The Agent status is abnormal.

#### Solution:

1. Check whether the Agent process is running properly. If the process has exited, start the process again.  
In Windows, double-click the **agent\_start.bat** file. In Linux, run the **service cbragent start** command.
2. Re-install the Agent.
3. Check the time zone and date on the backup client. If the time difference between the client and server is greater than 15 minutes, adjust your local time based on the UTC time. If the Agent status remains abnormal after the client time is adjusted, wait for about half an hour until the system updates the latest Agent status.

### Agent Installation Failed with Message "BackupService.7403, Invalid Agent" Returned

#### Symptom:

The Agent installation failed, and the message "BackupService.7403, Invalid Client" was returned.

#### Possible cause:

No hybrid cloud backup vault is available before you install the Agent.

#### Solution:

1. Purchase a hybrid cloud backup vault on the CBR console.
2. Re-install the Agent.

### Agent Installation Failed with Message "Could not resolve host" Returned

#### Symptom:



The Agent installation failed, and the message "Could not resolve host" was returned.

**Figure 7-17** "Could not resolve host" message



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

**Possible cause:**

The local DNS server cannot resolve the public domain name of Huawei Cloud.

**Solution:**

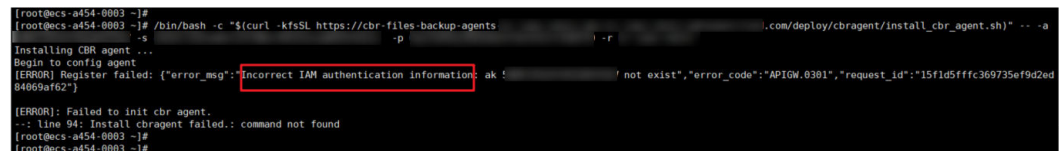
1. Edit the **resolv.conf** file on the local host and check whether the DNS server is configured. If you access Huawei Cloud over the Internet, set the DNS server to **8.8.8.8**.
2. Re-install the Agent.

## Agent Installation Failed with Message "Incorrect IAM authentication information" Returned

**Symptom:**

The Agent installation failed, and the message "Incorrect IAM authentication information" was returned.

**Figure 7-18** "Incorrect IAM authentication information" message



```
[root@ecs-a454-0003 ~]# /bin/bash -c "$(curl -kfsSL https://cbr-files-backup-agents.com/depLoy/cbragent/install_cbr_agent.sh)" -- -a
Installing CBR agent ...
Begin to config agent
[ERROR] Register failed: ("error_msg": "Incorrect IAM authentication information: ak t not exist", "error_code": "APIGW.0301", "request_id": "15f1d5fffc369735ef9d2ed84069af62")
[ERROR] Failed to init cbr agent.
--: line 94: Install cbragent failed.: command not found
[root@ecs-a454-0003 ~]#
```

**Possible cause:**

Wrong AK and SK were entered during installation.

**Solution:**

1. Obtain the correct AK and SK and enter them again.
2. Re-install the Agent.

## Agent Installation in Windows Failed with "OpenSCManager failed" Recorded in the Log

**Symptom:**

The Agent installation in Windows failed, and "OpenSCManager failed" was recorded in the log.

**Possible cause:**

The installation script is not run as administrator.

**Solution:**

Run the installation script as administrator to re-install the Agent.

## **Backup Failed After the Agent of a Windows Client Was Re-installed, and the Agent Status Was Displayed as Abnormal on the Console**

**Symptom:**

After the Agent of a Windows backup client was uninstalled and then re-installed, backups failed and the Agent status was displayed as Abnormal on the console.

**Possible causes:**

- The Agent fails to send heartbeat messages, or the domain name is incorrect.
- Writes to the Agent's configuration file fail or encounter an error.

**Solution:**

Uninstall the Agent and then re-install it.

## **Windows Client Was Offline and Failed to Be Restarted**

**Symptom:**

The Agent installation in Windows failed, and "OpenSCManager failed" was recorded in the log.

**Possible cause:**

There are a large number of .tmp files (generated due to log compression exceptions) in the log directory.

**Solution:**

1. Delete all log files in the log directory and uninstall the Agent.
2. Re-install the Agent.

# 8 Restoring Data

---

## 8.1 Restoring from a Cloud Server Backup

When disks on a server are faulty or their data is lost, you can use a backup to restore the server to its state when the backup was created.

You can also restore the backup to another server. For details, see [How Do I Restore Data on the Original Server to a New Server?](#)

### NOTE

The system shuts down the server before restoring server data, and automatically starts up the server after the restoration is complete. If you deselect **Start the server immediately after restoration**, you need to manually start the server after the restoration is complete.

### Notes and Constraints

- When restoring from a cloud server backup, backup of a data disk cannot be restored to the system disk.
- Data cannot be restored to servers in the **Faulty** state.
- Concurrent data restoration is not supported.
- Scheduled restoration is not supported currently.
- A backup of an ECS created using an ISO image cannot be used to directly restore data. You can use the backup to create an image and then provision an ECS using the image.



### Prerequisites

- Disks are running properly on the server whose data needs to be restored.
- The server has at least one **Available** backup.

### Procedure

**Step 1** Log in to the CBR console.

1. [Log in to the management console.](#)

2. Click  in the upper left corner and select a region.
3. Click  and choose **Storage > Cloud Backup and Recovery**. Select a backup type from the left navigation pane.

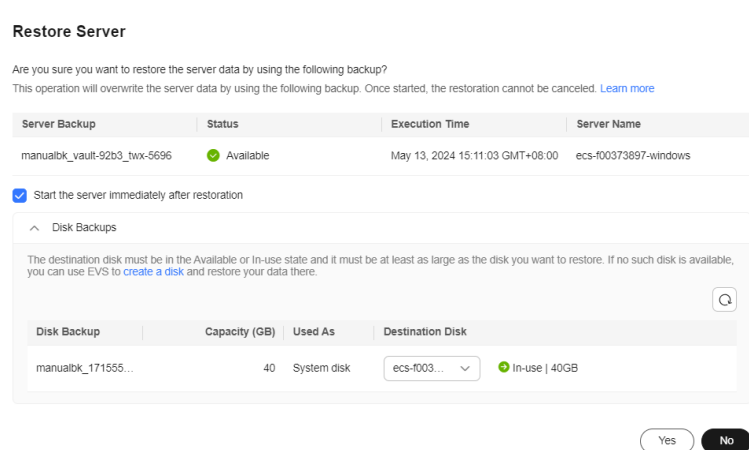
**Step 2** Click the **Backups** tab. Locate the desired backup. For details, see [Viewing a Backup](#).

**Step 3** Click **Restore Server** in the **Operation** column, as shown in [Figure 8-1](#).

### NOTICE

The current server data will be overwritten by the data captured at the time of backup. The restoration cannot be undone.

**Figure 8-1** Restoring a server



**Step 4** (Optional) Deselect **Start the server immediately after restoration**.

If you do so, manually start the server after the restoration is complete.

### NOTICE

Servers will be shut down during restoration, so you are advised to perform a restoration during off-peak hours.

**Step 5** In the **Destination Disk** drop-down list, select the target disk to which the backup will be restored.

 **NOTE**

- If the server has only one disk, the backup is restored to that disk by default.
- If the server has multiple disks, the backup is restored to the original disks by default. You can also restore the backup to a different disk of at least the same size as the original disk.
- When restoring from a cloud server backup, backup of a data disk cannot be restored to the system disk.

---

**NOTICE**

If the number of disks to be restored is greater than the number of disks that were backed up, restoration may cause data inconsistency.

For example, if the Oracle data is scattered across multiple disks and only some of them are restored, data inconsistency may occur and the application may fail to start.

---

**Step 6** Click **Yes** and confirm that the restoration is successful.

You can view the restoration status in the backup list. When the backup enters the **Available** state and no new restoration tasks failed, the restoration is successful. The resource is restored to the state when that backup was created.

For details about how to view failed restoration tasks, see [Managing Tasks](#).

---

**NOTICE**

If you use a cloud server backup to restore a logical volume group, you need to attach the logical volume group again.

Due to Window limitations, data disks may fail to be displayed after a Windows server is restored. If this happens, manually bring these data disks online. For details, see [Data Disks Are Not Displayed After a Windows Server Is Restored](#).

---

----End

## 8.2 Creating an Image from a Cloud Server Backup

CBR allows you to create images using ECS backups. You can use the images to provision ECSs to rapidly restore service running environments.

You can also use server backups to create images and then provision servers to restore data if your servers were accidentally deleted.

### Prerequisites

- The following operations have been performed:
  - You have optimized the Linux ECS (referring to [Optimizing a Linux Private Image](#)) and installed Cloud-Init (referring to [Installing Cloud-Init](#)).

- You have optimized the Windows ECS (referring to [Optimizing a Windows Private Image](#)) and installed Cloudbase-Init (referring to [Installing and Configuring Cloudbase-Init](#)).
- The backup is in the **Available** state, or the backup is in the **Creating** state that is marked with "Image can be created."

 **NOTE**

Once a backup creation starts, the backup enters the **Creating** state. After a period of time, a message stating "Image can be created" is displayed under **Creating**. In this case, the backup can be used for creating an image, even though it is still being created and cannot be used for restoration.



- The backup contains the system disk data.
- Only ECS backups can be used to create images.

## Notes

- Images created using a backup are the same, so CBR allows you to use a backup to create only one full-ECS image that contains the whole data of the system disk and data disks of an ECS, in order to save the image quota. After an image is created, you can use the image to provision multiple ECSs in a batch.
- A backup with an image created cannot be deleted directly. To delete such a backup, delete its image first. If a backup is automatically generated based on a backup policy and the backup has been used to create an image, the backup will not be counted as a retained backup and will not be deleted automatically.
- A backup is compressed when it is used to create an image, so the size of the generated image may be smaller than the backup size.

## Procedure

**Step 1** Log in to the CBR console.

1. [Log in to the management console](#).
2. Click  in the upper left corner and select a region.
3. Click  and choose **Storage > Cloud Backup and Recovery**. Select a backup type from the left navigation pane.

**Step 2** Click the **Backups** tab. Locate the desired backup. For details, see [Viewing a Backup](#).

**Step 3** In the row of the backup, choose **More > Create Image**.

**Step 4** Create an image by referring to [Creating a Full-ECS Image from a CBR Backup](#) in the *Image Management Service User Guide*.

**Step 5** Use the image to provision ECSs when needed. For details, see [Creating an ECS from an Image](#) in the *Image Management Service User Guide*.

----End

## 8.3 Restoring from a Cloud Disk Backup

You can use a disk backup to restore the disk to its state when the backup was created.

Before restoring the disk data, stop the server to which the disk is attached and detach the disk from the server. After the disk data is restored, attach the disk to the server and start the server.

### Prerequisites



- The disk to be restored is **Available**.
- Before restoring the disk data, stop the server to which the disk is attached and detach the disk from the server. After the disk data is restored, attach the disk to the server and start the server.

### Constraints

- If the server OS is changed after the system disk is backed up, the system disk backup cannot be restored to the original system disk due to reasons such as disk UUID change. You can use the system disk backup to create a new disk and copy data to the original system disk.
- Backups can only be restored to original disks. If you want to restore a backup to a different disk, use the backup to create a new disk.
- When restoring from a cloud disk backup, the backup can only be restored to the original disk. To restore backup of a data disk to a system disk, see [How Do I Restore a Data Disk Backup to a System Disk?](#)
- Concurrent data restoration is not supported.

### Procedure

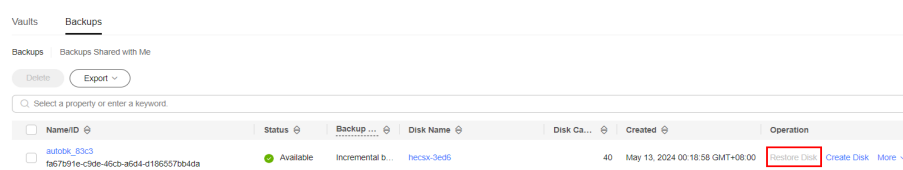
**Step 1** Log in to the CBR console.

1. [Log in to the management console](#).
2. Click  in the upper left corner and select a region.
3. Click  and choose **Storage > Cloud Backup and Recovery**. Select a backup type from the left navigation pane.

**Step 2** Click the **Backups** tab. Locate the desired backup. For details, see [Viewing a Backup](#).

**Step 3** In the row of the backup, click **Restore Disk**. The **Restore Disk** dialog box is displayed. See [Figure 8-3](#).

**Figure 8-2** Locating the target backup

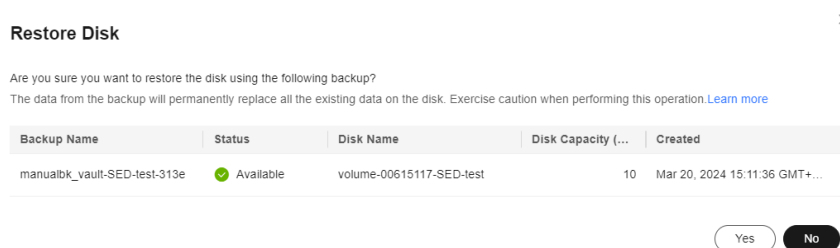


Name/ID	Status	Backup ...	Disk Name	Disk Ca...	Created	Operation
autobk_83c3 fb6791e-c9de-46cb-a6d4-d196557bb4da	Available	Incremental b...	hecsx-3ed5	40	May 13, 2024 00:18:56 GMT+08:00	<b>Restore Disk</b> Create Disk More

**NOTICE**

- The backup data will overwrite the current disk data, and the restoration cannot be undone.
- If the restore button is grayed out, stop the server, detach the disk, and then try again. After the disk data is restored, attach the disk to the server and start the server.

**Figure 8-3** Restore Disk



**Step 4** Click **Yes**. You can check whether data is successfully restored on the **Backups** tab page of **Cloud Disk Backups** or on the EVS console.

When the status of the backup changes to **Available**, the restoration is successful. The resource is restored to the state when that backup was created.

**Step 5** After the restoration is complete, re-attach the disk to the server. For details, see [Attaching a Non-Shared Disk](#).

----End

## 8.4 Creating a Disk from a Cloud Disk Backup


You can use a disk backup to create a disk that contains the same data as the backup.

Disks created using system disk backups can only be used as data disks on servers. They cannot be used as system disks.


Disk backups can only be used to create EVS disks, not servers.

### Procedure

**Step 1** Log in to the CBR console.

1. [Log in to the management console](#).
2. Click  in the upper left corner and select a region.



3. Click  and choose **Storage > Cloud Backup and Recovery**. Select a backup type from the left navigation pane.

**Step 2** Click the **Backups** tab. Locate the desired backup. For details, see [Viewing a Backup](#).

**Step 3** Click **Create Disk** in the **Operation** column of the backup. The button is available only when the backup status is **Available**.

**Step 4** Configure the disk parameters.

 **NOTE**

See the parameter description table in section "Purchase an EVS Disk" of the *Elastic Volume Service User Guide* for more information.

Pay attention to the following:

- You can choose the AZ to which the backup source disk belongs, or a different AZ.
- The new disk must be at least as large as the backup's source disk.

If the capacity of the new disk is greater than that of the backup's source disk, format the additional space by following the steps provided in section "Extending Disk Partitions and File Systems" of the *Elastic Volume Service User Guide*.

- You can create a disk of any type regardless of the backup's source disk type.

**Step 5** Click **Next**.

 **NOTE**

You can choose **Pay-per-use** or **Yearly/Monthly** as your **Billing Mode**. The following steps use the **Yearly/Monthly** billing as an example.

**Step 6** Confirm the disk information and click **Submit**.

**Step 7** Make the payment and click **OK**.

**Step 8** Go back to the disk list. Check whether the disk is successfully created.

You will see the disk status change as follows: **Creating, Available, Restoring, Available**. You may not notice the **Restoring** status because Instant Restore is supported and the restoration speed is very fast. After the disk status has changed from **Creating** to **Available**, the disk is successfully created. After the status has changed from **Restoring** to **Available**, backup data has been successfully restored to the created disk.

----End



## 8.5 Creating a File System from an SFS Turbo Backup

In case of a virus attack, accidental deletion, or software or hardware fault, you can use an SFS Turbo file system backup to create a new file system. Once created, data on the new file system is the same as that in the backup.

### Procedure

**Step 1** Log in to the CBR console.

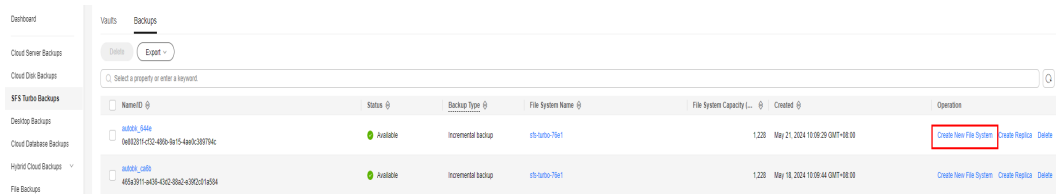
1. [Log in to the management console](#).

2. Click  in the upper left corner and select a region.
3. Click  and choose **Storage > Cloud Backup and Recovery**. Select a backup type from the left navigation pane.

**Step 2** Click the **Backups** tab and locate the desired backup. For details, see [Viewing a Backup](#).

**Step 3** Click **Create File System** in the **Operation** column of the backup. The button is available only when the backup status is **Available**.

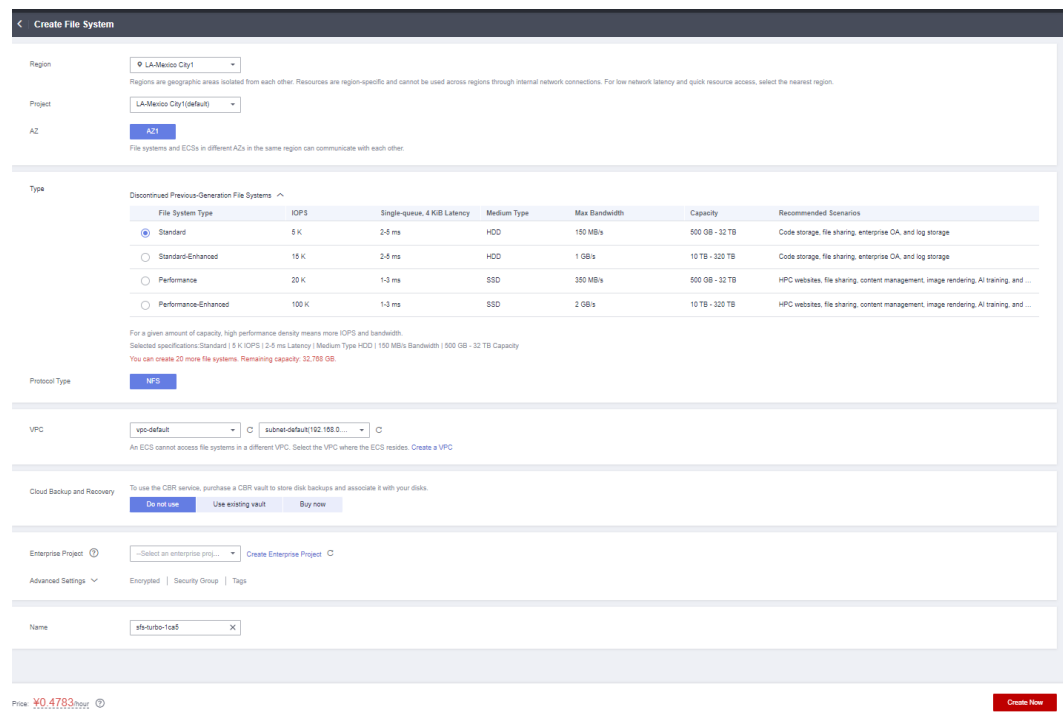
**Figure 8-4** Viewing a backup



 **NOTE**

For how to create backups, see [Creating an SFS Turbo Backup](#).

**Step 4** Configure the file system parameters.



 NOTE

- You can learn about the parameter descriptions in table "Parameter description" under "Creating an SFS Turbo File System" in [Create a File System](#)"Create a File System" of the *Scalable File Service Turbo User Guide*.
- You can change the storage class of the file system within a certain range. For example, you can change a file system from Standard to Performance, but not from Standard to Standard - Enhanced.
- The billing mode of the new file system can only be pay-per-use.

**Step 5** Click **Create Now**.

**Step 6** Confirm the file system information and click **Submit**.

**Step 7** Make the payment and click **OK**.

**Step 8** Go back to the file system list and check whether the file system is successfully created.

You will see the file system status change as follows: **Creating, Available, Restoring, Available**. You may not notice the **Restoring** status because Instant Restore is supported and the restoration speed is very fast. After the file system status has changed from **Creating** to **Available**, the file system is successfully created. After the status has changed from **Restoring** to **Available**, backup data has been successfully restored to the created file system.

----End

## 8.6 Restoring from a Desktop Backup



You can use a desktop backup to restore the desktop to its state when the backup was created.

### Prerequisites

The desktop to be restored is **Available**.

### Procedure

**Step 1** Log in to the CBR console.

1. [Log in to the management console](#).
2. Click  in the upper left corner and select a region.
3. Click  and choose **Storage > Cloud Backup and Recovery**. Select a backup type from the left navigation pane.

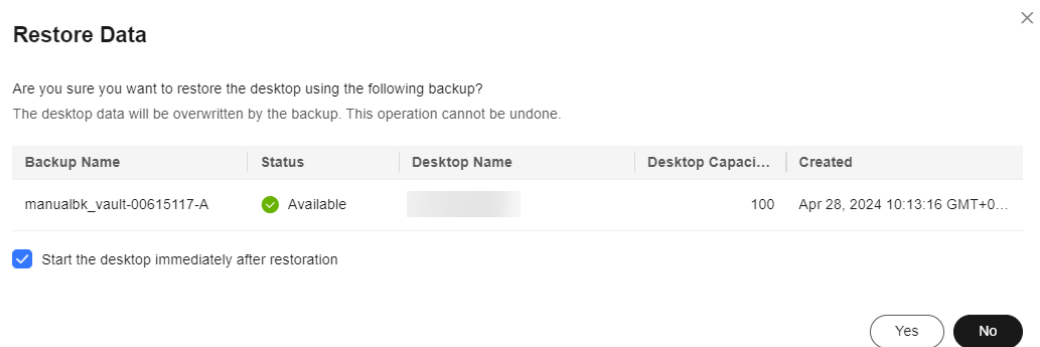
**Step 2** Click the **Backups** tab. Locate the desired backup. For details, see [Viewing a Backup](#).

**Step 3** In the row of the backup, click **Restore Data**. See [Figure 8-5](#).

**NOTICE**

- The current desktop data will be overwritten by the data captured at the time of backup. The restoration cannot be undone.

**Figure 8-5** Restoring a desktop



**Step 4** (Optional) Deselect **Start the desktop immediately after restoration**.

If you do so, manually start the desktop after the restoration is complete.

**NOTICE**

Desktops will be shut down during restoration, so you are advised to perform a restoration during off-peak hours.

**Step 5** Click **Yes**. You can check whether data is successfully restored on the **Backups** tab page of **Desktop Backups** or on the Workspace console.

When the status of the desktop changes to **Available**, the restoration is successful.

----End

## 8.7 Restoring from a File Backup


You can use a file backup to restore individual files of a server to its state when the backup was created.

### Constraints

- The Agent on the server must be **Normal**.
- You are advised not to restore file backups when applications are running. Stop the applications and then restore files.

## Method 1

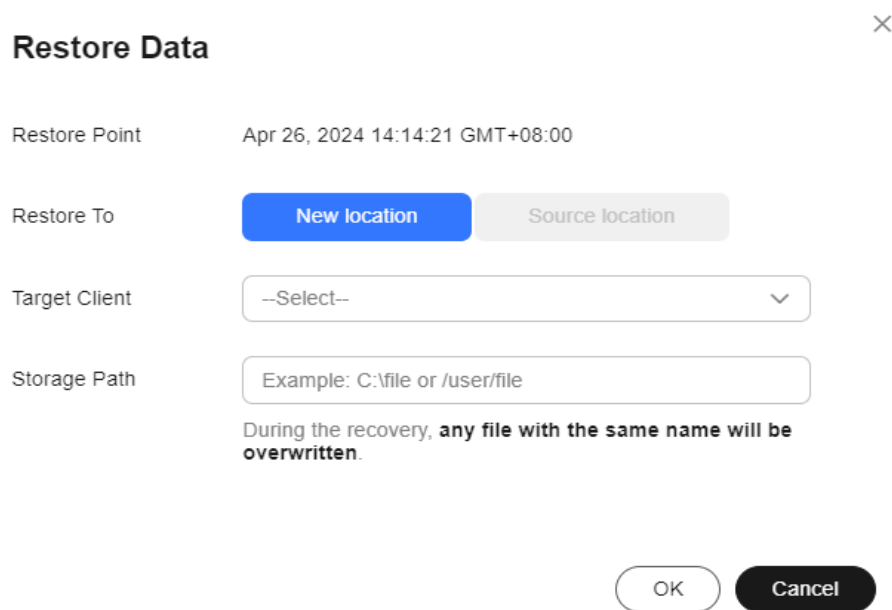
**Step 1** Log in to the CBR console.

1. Log in to the management console.
2. Click  in the upper left corner and select a region.
3. Choose **Storage > Cloud Backup and Recovery > File Backups**.

**Step 2** On the **Backup Clients** tab page, click the name of the target backup client.

**Step 3** Find the desired backup and click **Restore Data**. See [Figure 8-6](#).

**Figure 8-6** Restoring files



**Restore Data** ×

Restore Point Apr 26, 2024 14:14:21 GMT+08:00

Restore To New location Source location

Target Client --Select-- ▼

Storage Path Example: C:\file or /user/file

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

OK Cancel

**Step 4** Select a restore location.

- **Source location:** Data will be restored to the original file path, and any file with the same name will be overwritten. This option is available only for Linux backup clients.
- **New location:** Data will be restored to a different server you select. You can only choose from the backup clients whose Agent status is **Normal**. If your target server is not on the list, install the Agent on the server and try again.

 **NOTE**

The storage path cannot contain spaces.


**Step 5** Click **OK**. You can check whether data is successfully restored in the **Backup Details** area of the client details page or on the local host.

When the status of the backup changes to **Available**, the restoration is successful.

----End

## Method 2

**Step 1** Log in to the CBR console.

1. Log in to the management console.
2. Click  in the upper left corner and select a region.
3. Choose **Storage > Cloud Backup and Recovery > File Backups**.

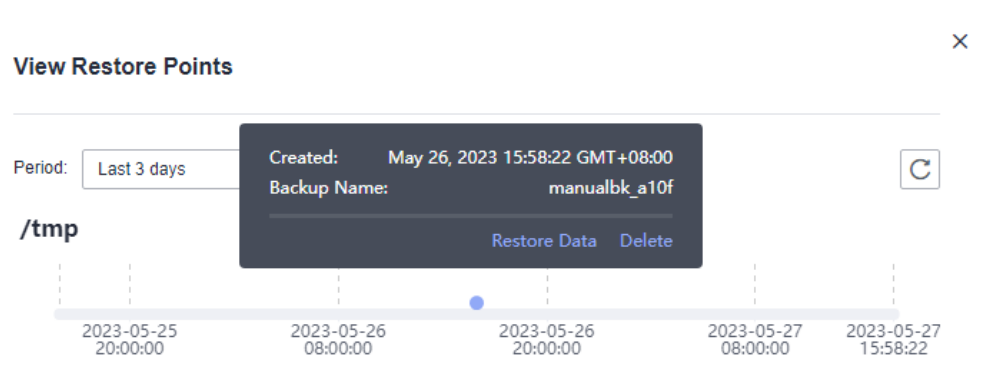
**Step 2** On the **Backup Clients** tab page, locate the name of the target backup client.

**Step 3** Click **Restore Points** in the **Operation** column.

**Step 4** Select a restore point and click **Restore Data**. See [Figure 8-7](#).

Backup data will be restored to the state at the selected time.

**Figure 8-7** Restore Points



**Step 5** Select a restore location.

- **Source location:** Data will be restored to the original file path, and any file with the same name will be overwritten. This option is available only for Linux backup clients.
- **New location:** Data will be restored to a different server you select.  
You can only choose from the backup clients whose Agent status is **Normal**. If your target server is not on the list, install the Agent on the server and try again.

**Step 6** Click **OK**. You can check whether data is successfully restored in the **Backup Details** area of the client details page or on the local host.

When the status of the backup changes to **Available**, the restoration is successful.

----End

## 8.8 Restoring from a Hybrid Cloud Backup

You can synchronize on-premises server backups to hybrid cloud backup vaults and restore the backup data to cloud servers for disaster recovery, service migration, development, or testing.

## Restoring Data Using a VMware Backup

You can synchronize backup data of on-premises VMware VMs and use the backup data to restore data to other servers for cloud DR and quick service deployment.

Before restoring data, configure a security group. Otherwise, the restoration may fail. For details, see [Restoring to Cloud Servers Using VMware Backups](#).

# 9 (Optional) Migrating Resources from CSBS/VBS

## Context

Huawei Cloud has launched the next-generation backup service, CBR. If you have backups in CSBS or VBS but want to switch to CBR to manage these historical backups, you can migrate them to CBR in a few clicks.

If you have never used CSBS or VBS, or do not need the historical backups anymore, skip this section.

## Migration Rules

During migration, CBR will automatically create vaults based on the types of your historical resources.

**Table 9-1** Migration rules

Before Migration	After Migration
Servers or disks are associated with a backup policy.	If backups have been generated, CBR will create a vault with the same name (up to 64 characters) as the policy name (regardless of whether the policy is enabled) and apply the policy to the vault after the vault is created.  If no backup is generated, CBR will create a vault only when the policy is enabled. The policy applying rule and vault naming rule are the same as above.
Servers or disks are associated with a backup or replication policy.	If no backup is generated and the policy is disabled, only the policy will be migrated.
Backup or replication policies are not associated with any resource.	The policies will be migrated.



Before Migration	After Migration
Application-consistent backup is enabled.	CBR will create a database server backup vault and name the vault with the policy name.
Backup replicas are generated.	CBR will create a replication vault named <b>default</b> to store generated backup replicas.
An image is created using a backup and a tag is added to the image.	The backup will fail to be migrated. Go to the IMS console, delete the tag and then migrate the backup again. After the backup is migrated, add the tag if needed.

Other backups, including manual backups, will be stored in a server backup vault named **default**. Different vaults will be created based on different types of resources. For example, CBR will create a disk backup vault to store the migrated disk backups.

If backups are migrated from any of the following regions, all backups in these regions will be migrated: CN East-Shanghai1, CN North-Beijing4, CN South-Guangzhou, CN-Hong Kong, AP-Singapore, and AP-Bangkok. To migrate backups in a region not listed here, switch to that region and proceed with the migration.

After the migration, backups created using CBR will also be displayed on the VBS console, but you will be billed only once.

 **NOTE**

To delete backups from the VBS console, find these backups in CBR and delete them. Then, the backups will also be deleted from the VBS console.

Based on the preceding rules, the capacity of each vault created by the system is predefined as 1.2 times of the total backup size.

For example, a user has a 100 GB ECS and a 50 GB ECS. The used storage capacity of the two ECSs is 20 GB and 10 GB, respectively. The user manually has backed up the two entire ECSs using cloud server backup. During migration, the capacity of the vault automatically created will be 1.2 times of the total backup size. In this example, the total backup size multiplied by 1.2 is 36 GB. So the system will automatically create a 36 GB vault.



## Constraints

- By default, a system-created vault is billed on a pay-per-use basis. If you want to switch to yearly/monthly billing, refer to instructions in [Changing from Pay-per-Use to Yearly/Monthly](#).
- After resources are migrated, VBS and CSBS will be unavailable. CBR uses new billing standards. For more information, see [CBR Pricing Details](#).
- The vaults you have purchased cannot be used for migration. Resources will automatically migrate to system-created vaults.
- Backup resources of one account only need to be migrated once.
- During the migration, do not delete the CBR backup vault that is automatically created. Use it after the migration is complete.

- After resources are migrated, disk backups and server backups will be automatically stored in CBR vaults. No further operations are required.

## Procedure

**Step 1** Log in to the CBR console.

1. [Log in to the management console](#).
2. Click  in the upper left corner and select a region.
3. Click  and choose **Storage > Cloud Backup and Recovery**. Select a backup type from the left navigation pane.

**Step 2** Click **Migrate to CBR** in the upper right corner. Read the content in the displayed dialog box and click **OK**. See [Figure 9-1](#).

**Figure 9-1** Migrating resources to CBR

Notice

### Migration of Backup Services from CSBS & VBS to CBR

The Cloud Backup and Recovery (CBR) service was launched on June 30, 2019. CBR integrates Cloud Server Backup Service (CSBS) and Volume Backup Service (VBS). After CBR goes online, CSBS, VBS, and CBR will be simultaneously available. Please complete your service migration as soon as possible. After migration, CSBS and VBS will no longer be accessible.

Please note the following changes:

1. Function extension: CBR provides a wider service scope than CSBS. Besides cloud server backup, CBR also provides cloud disk backup, application backup, storage backup, and VMware backup.
2. Usage: To use CBR, you need to create vaults first. The backup capacity cannot exceed the vault capacity. If you need to expand the backup capacity, expand the vault capacity first. Backup policies are bound to vaults.
3. Billing mode: CBR is charged based on the capacity of vaults.
4. Limitations and Restrictions: After the migration is complete, CSBS/VBS and existing CSBS/VBS resource packages will no longer be available for CBR. You are advised to unsubscribe from the resource packages promptly. The default vault created by the system for housing migrated backups is billed on pay-per-use basis. If you want to switch to yearly/monthly billing, refer to the instructions in [Changing Billing from Pay-per-Use to Yearly/Monthly](#). [Learn migration rules](#)

Only backups in the current region are shown here. For the backup size and estimated prices for other regions, switch to the regions where the backups are stored.

CSBS Backup Size	VBS Backup Size
269.37 GB	160.10 GB

I have read the migration notice.

OK

Cancel

**Step 3** The system will automatically migrate resources. After the migration, a vault named **default** will be created and a message will be displayed in the upper part of the page indicating that the migration is successful.

----End

## FAQ

1. Why Are CBR Backups Displayed on VBS Console?

If you have migrated data from CSBS and VBS to CBR, and created a backup on the CBR console, the same backup record will be generated on VBS Console. This is due to an underlying mechanism. VBS Console displays all

backups generated by CBR, CSBS, and VBS. These backups will not be billed repeatedly.

2. How Do I Delete Backups from VBS Console?

After you have migrated data from CSBS and VBS to CBR, backups displayed in the VBS console cannot be deleted alone. Find these backups in CBR and delete them. Then, the backups will also be deleted from the VBS console.

3. What Are the Differences Between CBR, CSBS, and VBS?

CBR integrates CSBS and VBS. In addition, CBR supports SFS Turbo backup. The usage and billing of CBR are also different from CSBS and VBS.

4. What Can I Do If a Message Is Displayed Indicating that a Resource Has Been Bound with CSBS or VBS?

Choose **Cloud Server Backup Service** or **Volume Backup Service** from the service list. On the corresponding service console, check whether there are resources bound with policies on the **Policies** tab. If so, unbind the resources from the policy and go to the CBR console to associate the resources with a vault.

# 10 Managing Tasks

---


You can view tasks in the task list, which shows policy-driven tasks that have been executed over the past 30 days.

## Prerequisites


At least one task exists.

## Procedure for Viewing the Task Execution Status

**Step 1** Log in to the CBR console.

1. Log in to the management console.
2. Click  in the upper left corner and select a region.
3. Choose **Storage > Cloud Backup and Recovery > Tasks**.

**Step 2** Filter tasks by enterprise project, task type, task status, task ID, resource ID, resource name, vault ID, vault name, and time.

**Step 3** Click  in front of the task to view the task details.

If a task fails, you can view the failure cause in the task details.

----End

# 11 Cloud Eye Monitoring

## 11.1 Viewing Basic CBR Monitoring Data

### Scenarios

This section describes metrics reported by CBR as well as their namespaces and dimensions. You can use the console or [APIs](#) provided by Cloud Eye to query the metrics generated for CBR.

### Namespace

SYS.CBR

### Metrics

**Table 11-1** CBR metrics

Metric ID	Metric Name	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
used_vault_size	Used Vault Size	Used capacity of the vault Unit: GB	≥ 0	Vault	15 min
vault_util	Vault Usage	Capacity usage of the vault	0~100 %	Vault	15 min

## Dimensions

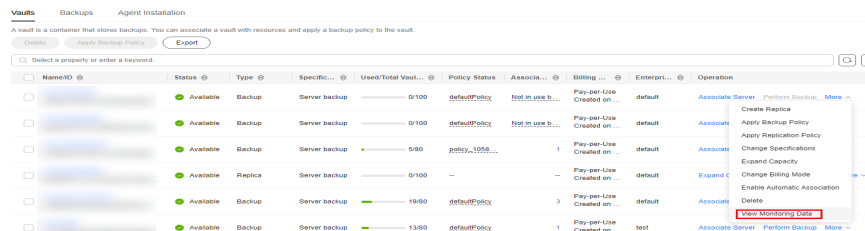
Key	Value
instance_id	Vault name/ID

## Viewing Monitoring Statistics

**Step 1** Log in to the management console.

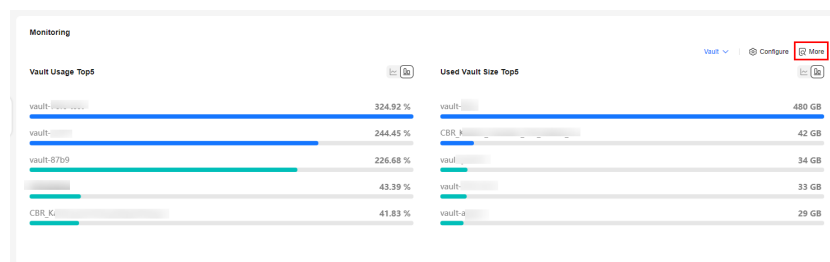
**Step 2** View the monitoring graphs using either of the following methods.

- Method 1: Choose **Storage > Cloud Backup and Recovery**. In the vault list, locate the vault whose monitoring data you want to view and choose **More > View Monitoring Data** in the **Operation** column.



- Method 2: Choose **Management & Governance > Cloud Eye > Cloud Service Monitoring > Cloud Backup and Recovery**. In the vault list, click **View Metric** in the **Operation** column of the vault whose monitoring data you want to view.
- Method 3: Choose **Storage > Cloud Backup and Recovery**. In the vault list on any resource backup page, click the vault name whose monitoring data you want to view to go to the vault details page. Click the **Monitoring** tab to view the monitoring metrics.
- Method 4: Choose **Storage > Cloud Backup and Recovery**. In the left navigation pane, click **Dashboard**. In the **Monitoring** area, view monitoring metrics. Click **More** to view monitoring details.

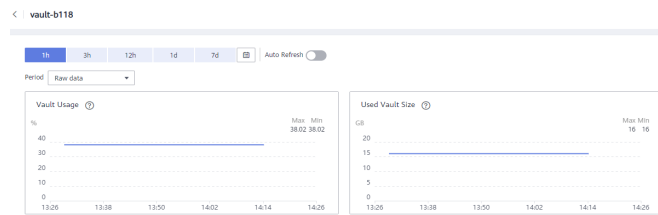
**Figure 11-1** Monitoring area on the CBR console dashboard



**Step 3** View the vault monitoring data by metric or monitored duration.

**Figure 11-2** shows the monitoring graphs. For more information, see the *Cloud Eye User Guide*.

**Figure 11-2** Vault monitoring graphs




----End

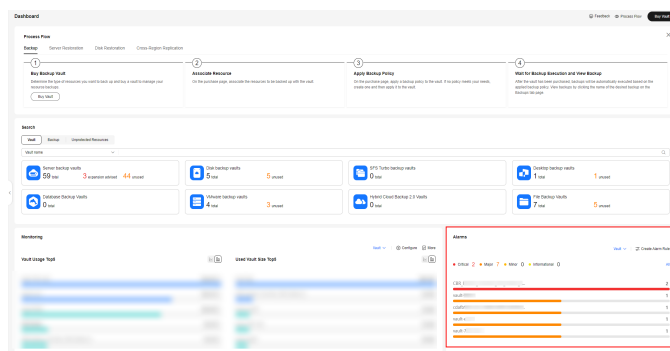
## 11.2 Creating an Alarm Rule

You can create alarm rules for CBR.

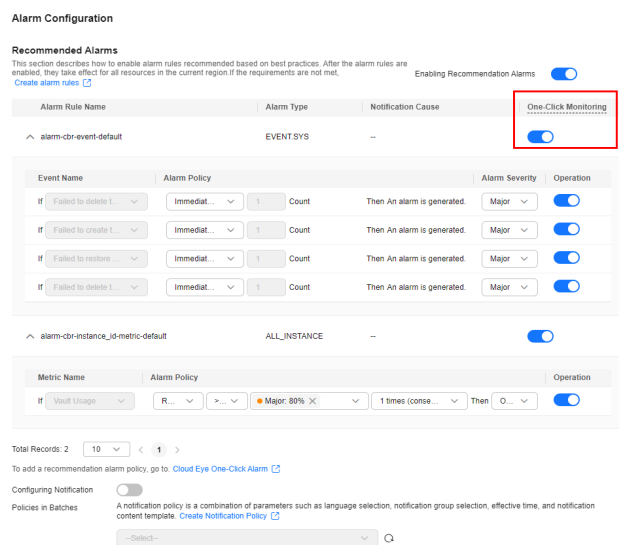
Hybrid cloud backup allows monitoring on vault capacity only. On-premises operations and events cannot be monitored.

### Enabling One-Click Monitoring on the CBR Console Dashboard

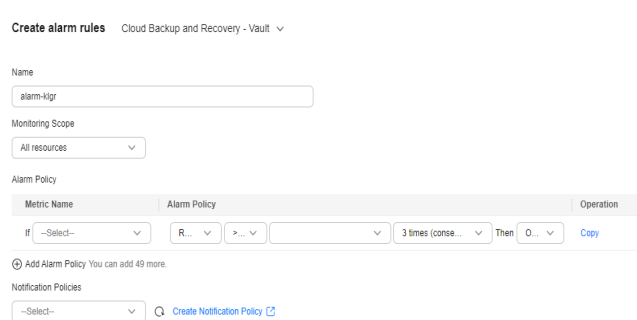
1. Log in to the management console.
2. Click  and choose **Storage > Cloud Backup and Recovery**. In the left navigation pane, click **Dashboard**. In the **Monitoring** area on the dashboard, view monitoring metrics.



3. In the **Alarms** area, click **Create Alarm Rule**. In the dialog box, view recommended alarm rules. Enable **One-Click Monitoring**. The enabled alarm rules will take effect for all resources in the current region.



4. If the current recommended alarm rules cannot meet your requirements, click **Create alarm rules**.



## Creating an Alarm Rule Using Cloud Eye

1. Log in to the management console.
2. Under **Management & Governance**, select **Cloud Eye**. In the navigation pane on the left, choose **Alarm Management > Alarm Rules**.
3. On the displayed page, click **Create Alarm Rule** in the upper right corner.
4. On the displayed **Create alarm rule** page, configure the parameters.
  - a. Set **Name** and **Description**.

**Figure 11-3** Configuring the alarm rule name and description



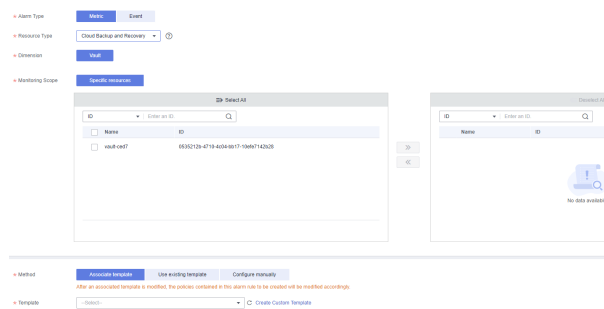
Parameters for configuring the rule name and description



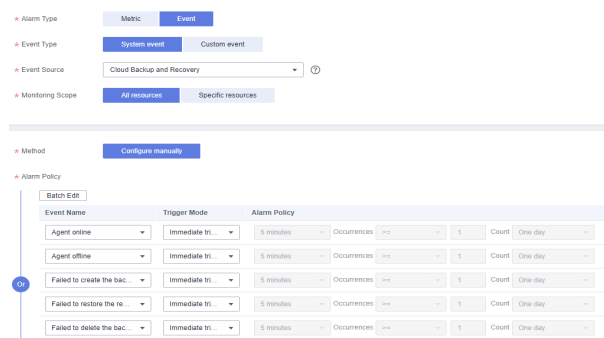
Parameter	Description	Example Value
Name	Name of the alarm rule. The system generates a random name, which you can modify.	alarm-cgnw
Description	Alarm rule description. This parameter is optional.	-

b. Configure alarm content parameters.

**Figure 11-4** CBR vault-based alarm rule configuration

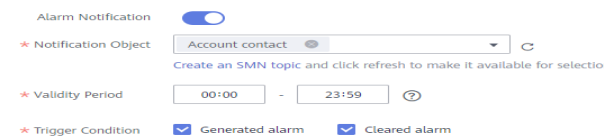


**Figure 11-5** CBR event-based alarm rule configuration



c. Configure alarm notifications.

**Figure 11-6** Configuring alarm notifications



**Table 11-2** Parameters for configuring alarm notifications

Parameter	Description	Example Value
Alarm Notification	Whether to notify users when alarms are triggered. Notifications can be sent by email or text message, or through HTTP/HTTPS request to servers.  You can enable (recommended) or disable <b>Alarm Notification</b> .	-
Notification Window	Cloud Eye sends notifications only within the notification window specified in the alarm rule.  If <b>Notification Window</b> is set to <b>00:00-8:00</b> , Cloud Eye sends alarm notifications only within 00:00-8:00.	-
Notification Object	The name of the topic the alarm notification is to be sent to.  If you enable alarm notification, you need to select a topic. If no desirable topics are available, create one and subscribe to it first. For details about how to create a topic, see the <i>Simple Message Notification User Guide</i> .	-
Trigger Condition	The condition for triggering the alarm notification. You can select <b>Generated alarm</b> , <b>Cleared alarm</b> , or both.	-

- d. Click **Create**.

After the alarm rule is created, if the metric data reaches the specified threshold or a CBR event happens, Cloud Eye immediately informs you that an exception has occurred. For details, see the *Cloud Eye User Guide*.

# 12 Recording CBR Operations Using CTS

You can use Cloud Trace Service (CTS) to trace operations in CBR.

## Prerequisites

CTS has been enabled.

## Key Operations Recorded by CTS

**Table 12-1** CBR operations that can be recorded by CTS

Operation	Resource Type	Trace Name
Creating a policy	policy	createPolicy
Updating a policy	policy	updatePolicy
Deleting a policy	policy	deletePolicy
Setting a vault policy	vault	associatePolicy
Removing a policy from a vault	vault	dissociatePolicy
Creating a vault	vault	createVault
Modifying a vault	vault	updateVault
Deleting a vault	vault	deleteVault
Removing resources	vault	removeResources
Adding resources	vault	addResources
Performing a replication	vault	replicateVaultBackup
Performing a backup	vault	createVaultBackup
Creating a backup	backup	createBackup
Deleting a backup	backup	deleteBackup


Operation	Resource Type	Trace Name
Synchronizing a backup	backup	syncBackup
Restoring a backup	backup	restoreBackup
Replicating a backup	backup	replicateBackup

## Viewing Audit Logs

For how to view audit logs, see section "Querying Real-Time Traces" in the *Cloud Trace Service User Guide*.

## Disabling or Enabling a Tracker

The following procedure illustrates how to disable an existing tracker on the CTS console. After the tracker is disabled, the system will stop recording operations, but you can still view existing operation records.

- Step 1** Log in to the management console.
- Step 2** In the upper left corner of the page, click  and select a region.
- Step 3** Click **Service List** and choose **Management & Governance > Cloud Trace Service**.
- Step 4** Choose **Tracker List** in the left navigation pane.
- Step 5** In the tracker list, click **Disable** in the **Operation** column.
- Step 6** Click **Yes**.
- Step 7** After the tracker is disabled, the available operation changes from **Disable** to **Enable**. To enable the tracker again, click **Enable** and then click **Yes**. The system will start recording operations again.

----End

# 13 Quotas

## What Is Quota?

Quotas can limit the number or amount of resources available to users, such as the maximum number of ECS or EVS disks that can be created.

If the existing resource quota cannot meet your service requirements, you can apply for a higher quota.

## How Do I View My Quotas?


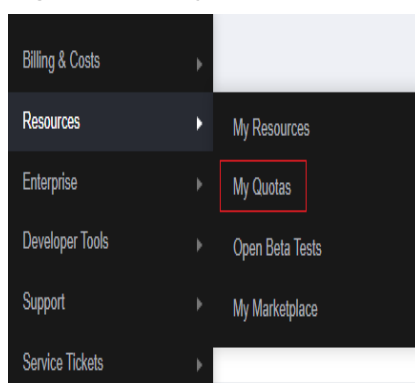
1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. In the upper right corner of the page, choose **Resources > My Quotas**.  
The **Service Quota** page is displayed.

Figure 13-1 My Quotas



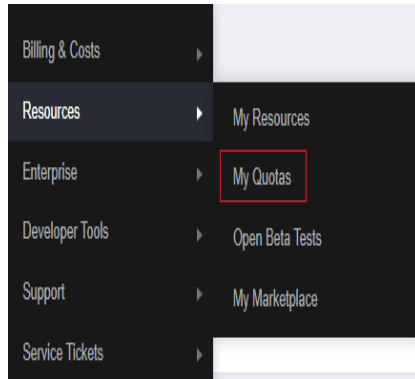
4. View the used and total quota of each type of resources on the displayed page.  
If a quota cannot meet service requirements, apply for a higher quota.

## How Do I Apply for a Higher Quota?

1. Log in to the management console.

- In the upper right corner of the page, choose **Resources > My Quotas**.  
The **Service Quota** page is displayed.

**Figure 13-2** My Quotas



- Click **Increase Quota** in the upper right corner of the page.

**Figure 13-3** Increasing quota

The image shows a screenshot of the 'Service Quota' page. At the top right, there is a red button labeled 'Increase Quota'. Below the header, there is a table with the following columns: 'Service', 'Resource Type', 'Used Quota', and 'Total Quota'. The table lists various services and their corresponding resource types and quota values.

Service	Resource Type	Used Quota	Total Quota
Auto Scaling	AS group	0	
	AS configuration	0	
Image Management Service	Image	0	
Cloud Container Engine	Cluster	0	
FunctionGraph	Function	0	
	Code storage(MB)	0	
Elastic Volume Service	Disk	3	
	Disk capacity(OB)	120	
	Snapshots	4	
Storage Disaster Recovery Service	Protection group	0	
	Replication pair	0	
Cloud Server Backup Service	Backup Capacity(OB)	0	
	Backup	0	
Scalable File Service	File system	0	
	File system capacity(OB)	0	
CDN	Domain name	0	
	File URL refreshing	0	
	Directory URL refreshing	0	
	URL prefetching	0	

- On the **Create Service Ticket** page, configure parameters as required.  
In the **Problem Description** area, fill in the content and reason for adjustment.
- After all necessary parameters are configured, select **I have read and agree to the Ticket Service Protocol and Privacy Statement** and click **Submit**.

# A Appendix

---

## A.1 Agent Security Maintenance

### A.1.1 Changing the Password of User rdadmin

#### Scenarios

- To improve O&M security, you are advised to change the user **rdadmin**'s password of the client OS regularly and disable this user's remote login permission.
- In Linux, user **rdadmin** does not have a password.
- This section describes how to change the password of user **rdadmin** in Windows Server 2012. Change the password according to actual situation in other versions.

#### Prerequisites

- The username and password for logging in to the console have been obtained.
- The username and password for logging in to a Windows ECS have been obtained.

#### Procedure

- Step 1** Go to the ECS console and log in to the Windows ECS.
- Step 2** Choose **Start > Control Panel**. In the **Control Panel** window, click **User Accounts**.
- Step 3** On the displayed **User Account Control** dialog box, select **rdadmin** and click **Reset Password**.
- Step 4** Enter the new password and click **OK**.
- Step 5** In **Task Manager**, click the **Services** tab and then click **Open Service**.

- Step 6** Select RdMonitor and RdNginx respectively. In the displayed dialog box, select **Login**, change the password to the one entered in **Step 4**, and click **OK**.

----End

## A.1.2 Changing the Password of the Account for Reporting Alarms (SNMP v3)

To enhance the system O&M security, you are advised to change the password of the account for reporting alarms.

### Prerequisites

- The username and password for logging in to the console have been obtained.
- The username and password for logging in to a server have been obtained.

### Context

This section introduces the procedures in Windows and Linux.

---

#### NOTICE

There may be security risks if you use the same password for SNMP v3 authentication and data encryption. To ensure system security, you are advised to set different passwords for SNMP v3 authentication and data encryption.

---

Obtain the initial authentication password from technical support.

#### NOTE

The password must meet the following complexity requirements:

- Contains 8 to 16 characters.
- Contains at least one of the following special characters: `~!@#%&^\*()-\_+=+| [{}];:~";<.>/?`
- Contains at least two of the following types of characters:
  - Uppercase letters
  - Lowercase letters
  - Numeric characters
- Cannot be the same as the username or the username in reverse order.
- Cannot be the same as the old passwords.
- Cannot contain spaces.

## Changing the Password of the Account for Reporting Alarms (SNMP v3) in Windows

- Step 1** Log in to the server where the Agent is installed.

- Step 2** Open the CLI and go to the *Installation path*\bin directory.



**Step 3** Run the **agentcli.exe chgsnmp** command, enter the server login password, and press **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:
```

 **NOTE**

**admin** is the username configured during the Agent installation.

**Step 4** Select the SN of the authentication password or data encryption password that you want to change and press **Enter**.

**Step 5** Type the old password and press **Enter**.

**Step 6** Type a new password and press **Enter**.

**Step 7** Type the new password again and press **Enter**.

The password is changed.

----End

## Changing the Password of the Account for Reporting Alarms (SNMP v3) in Linux

**Step 1** Log in to the Linux server using the server password.

**Step 2** Run the **TMOUT=0** command to prevent PuTTY from exiting due to session timeout.

 **NOTE**

After you run the preceding command, the system continues to run even when no operation is performed, which brings security risks. To ensure system security, run the **exit** command to exit the system after you finish the operations.

**Step 3** Run the **su - rdadmin** command to switch to user **rdadmin**.

**Step 4** Run the **/home/rdadmin/Agent/bin/agentcli chgsnmp** command, enter the server login password, and press **Enter**.

 **NOTE**

The installation path of the Agent is **/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:
```

**Step 5** Select the SN of the authentication password or data encryption password that you want to change and press **Enter**.

**Step 6** Type the old password and press **Enter**.

**Step 7** Type a new password and press **Enter**.

**Step 8** Type the new password again and press **Enter**.

The password is changed.

----End

### A.1.3 Replacing the Server Certificate

For security purposes, you may want to use a Secure Socket Layer (SSL) certificate issued by a third-party certification authority. The Agent allows you to replace authentication certificates and private key files as long as you provide the authentication certificates and private-public key pairs. The update to the certificate can take effect only after the Agent is restarted, hence you are advised to update the certificate during off-peak hours.

#### Prerequisites

- The username and password for logging in to the console have been obtained.
- The username and password for logging in to a server have been obtained.
- New certificates in the X.509v3 format have been obtained.

#### Context

- The Agent is pre-deployed with the Agent CA certificate **bcmagentca**, private key file of the CA certificate **server.key** (), and authentication certificate **server.crt**. All these files are saved in **/home/rdadmin/Agent/bin/nginx/conf** (if you use Linux) or **\bin\nginx\conf** (if you use Windows).
- You need to restart the Agent after replacing a certificate to make the certificate effective.

#### Replacing the Server Certificate in Linux

**Step 1** Log in the Linux server with the Agent installed.

**Step 2** Run the **TMOUT=0** command to prevent PuTTY from exiting due to session timeout.

#### NOTE

After you run the preceding command, the system continues to run even when no operation is performed, which brings security risks. To ensure system security, run the **exit** command to exit the system after you finish the operations.

**Step 3** Run the **su - rdadmin** command to switch to user **rdadmin**.

**Step 4** Run the `cd /home/rdadmin/Agent/bin` command to go to the script path.

 **NOTE**

The installation path of the Agent is `/home/rdadmin/Agent`.

**Step 5** Run the `sh agent_stop.sh` command to stop the Agent running.

**Step 6** Place the new certificates and private key files in the specified directory.

 **NOTE**

Place new certificates in the `/home/rdadmin/Agent/bin/nginx/conf` directory.

**Step 7** Run the `/home/rdadmin/Agent/bin/agentcli chgkey` command.

The following information is displayed:

Enter password of admin:

 **NOTE**

`admin` is the username configured during the Agent installation.

**Step 8** Type the login password of the Agent and press **Enter**.

The following information is displayed:

Change certificate file name:

**Step 9** Enter a name for the new certificate and press **Enter**.

 **NOTE**

If the private key and the certificate are the same file, names of the private key and the certificate are identical.

The following information is displayed:

Change certificate key file name:

**Step 10** Enter a name for the new private key file and press **Enter**.

The following information is displayed:

Enter new password:

Enter the new password again:

**Step 11** Enter the protection password of the private key file twice. The certificate is then successfully replaced.

**Step 12** Run the `sh agent_start.sh` command to start the Agent.

----End

## Replacing the Server Certificate in Windows

**Step 1** Log in to the Windows server with the Agent installed.

**Step 2** Open the CLI and go to the `Installation path\bin` directory.

**Step 3** Run the `agent_stop.bat` command to stop the Agent running.

**Step 4** Place the new certificates and private key files in the specified directory.

 NOTE

Place new certificates in the *installation path*\bin\nginx\conf directory.

**Step 5** Run the **agentcli.exe chgkey** command.

The following information is displayed:

```
Enter password of admin:
```

 NOTE

**admin** is the username configured during the Agent installation.

**Step 6** Enter a name for the new certificate and press **Enter**.

 NOTE

If the private key and the certificate are the same file, names of the private key and the certificate are identical.

The following information is displayed:

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

**Step 7** Enter a name for the new private key file and press **Enter**.

The following information is displayed:

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

**Step 8** Enter the protection password of the private key file twice. The certificate is then successfully replaced.

**Step 9** Run the **agent\_start.bat** command to start the Agent.

----End

## A.1.4 Replacing CA Certificates

### Scenarios

A CA certificate is a digital file signed and issued by an authentication authority. It contains the public key, information about the owner of the public key, information about the issuer, validity period, and certain extension information. It is used to set up a secure information transfer channel between the Agent and the server.

If the CA certificate does not comply with the security requirements or has expired, replace it for security purposes.

### Prerequisites

- The username and password for logging in to an ECS have been obtained.
- A new CA certificate is ready.

### Replacing CA Certificates in Linux

**Step 1** Log in the Linux server with the Agent installed.

**Step 2** Run the following command to prevent logout due to system timeout:

```
TMOUT=0
```

**Step 3** Run the following command to switch to user **rdadmin**:

```
su - rdadmin
```

**Step 4** Run the following command to go to the path to the Agent start/stop script:

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

**Step 5** Run the following command to stop the Agent running:

```
sh agent_stop.sh
```

**Step 6** Run the following command to go to the path to the CA certificate:

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

**Step 7** Run the following command to delete the existing CA certificate:

```
rm bcmagentca.crt
```

**Step 8** Copy the new CA certificate file into the **/home/rdadmin/Agent/bin/nginx/conf** directory and rename the file **bcmagentca.crt**.

**Step 9** Run the following command to change the owner of the CA certificate:

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

**Step 10** Run the following command to modify the permissions on the CA certificate:

```
chmod 400 bcmagentca.crt
```

**Step 11** Run the following command to go to the path to the Agent start/stop script:

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

**Step 12** Run the following command to start the Agent:

```
sh agent_start.sh
```

```
----End
```

## Replacing CA Certificates in Windows

**Step 1** Log in to the ECS with the Agent installed.

**Step 2** Go to the *Installation path*\bin directory.

**Step 3** Run the **agent\_stop.bat** script to stop the Agent.

**Step 4** Go to the *Installation path*\nginx\conf directory.

**Step 5** Delete the **bcmagentca.crt** certificate file.

**Step 6** Copy the new CA certificate file into the *Installation path*\nginx\conf directory and rename the file **bcmagentca.crt**.

**Step 7** Go to the *Installation path*\bin directory.

**Step 8** Run the **agent\_start.bat** script to start the Agent.  
----End