

# Cloud Backup and Recovery

## User Guide

**Issue** 05  
**Date** 2023-06-02



**Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2024. 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 Service Overview.....</b>	<b>1</b>
1.1 What Is CBR?.....	1
1.2 Application Scenarios.....	4
1.3 Functions.....	5
1.4 Permissions.....	6
1.5 Constraints.....	9
1.6 CBR and Other Services.....	10
1.7 Basic Concepts.....	10
1.7.1 CBR Concepts.....	10
1.7.2 Region and AZ.....	12
<b>2 Getting Started.....</b>	<b>14</b>
2.1 Step 1: Create a Vault.....	14
2.1.1 Creating a Server Backup Vault.....	14
2.1.2 Creating a Disk Backup Vault.....	15
2.2 Step 2: Associate a Resource with the Vault.....	16
2.3 Step 3: Create a Backup.....	18
2.3.1 Creating a Cloud Server Backup.....	18
2.3.2 Creating a Cloud Disk Backup.....	20
<b>3 Permissions Management.....</b>	<b>22</b>
3.1 Creating a User and Granting CBR Permissions.....	22
3.2 Creating a Custom Policy.....	24
3.3 Configuring Forcible Backup Policies.....	25
<b>4 Vault Management.....</b>	<b>27</b>
4.1 Querying a Vault.....	27
4.2 Deleting a Vault.....	29
4.3 Dissociating a Resource.....	30
4.4 Migrating a Resource.....	30
4.5 Expanding Vault Capacity.....	31
4.6 Changing Vault Specifications.....	32
<b>5 Backup Management.....</b>	<b>33</b>
5.1 Viewing a Backup.....	33
5.2 Sharing a Backup.....	34

5.3 Deleting a Backup.....	36
<b>6 Policy Management.....</b>	<b>38</b>
6.1 Viewing the Policy of a Vault.....	38
6.2 Creating a Backup Policy.....	38
6.3 Modifying a Policy.....	42
6.4 Deleting a Policy.....	42
6.5 Applying a Policy to a Vault.....	43
6.6 Removing a Policy from a Vault.....	44
<b>7 Restoring Data.....</b>	<b>45</b>
7.1 Restoring from a Cloud Server Backup.....	45
7.2 Creating an Image from a Cloud Server Backup.....	47
7.3 Restoring from a Cloud Disk Backup.....	48
7.4 Creating a Disk from a Cloud Disk Backup.....	49
<b>8 Application-Consistent Backup.....</b>	<b>51</b>
8.1 What Is Application-Consistent Backup?.....	51
8.2 Changing a Security Group.....	55
8.3 Installing the Agent.....	56
8.4 Creating an Application-Consistent Backup.....	61
8.5 Uninstalling the Agent.....	62
<b>9 Managing Tasks.....</b>	<b>64</b>
<b>10 Monitoring.....</b>	<b>65</b>
10.1 CBR Metrics.....	65
10.2 Creating an Alarm Rule.....	66
<b>11 Quotas.....</b>	<b>72</b>
<b>12 FAQs.....</b>	<b>73</b>
12.1 Concepts.....	73
12.1.1 What Are Full Backup and Incremental Backup?.....	73
12.1.2 What Are the Differences Between Backup and Disaster Recovery?.....	74
12.1.3 What Are the Differences Between Backups and Snapshots?.....	75
12.1.4 What Are the Differences Between Cloud Server Backup and Cloud Disk Backup?.....	76
12.2 Backup.....	76
12.2.1 Do I Need to Stop the Server Before Performing a Backup?.....	76
12.2.2 Can I Back Up a Server Deployed with Databases?.....	76
12.2.3 How Can I Distinguish Automatic Backups From Manual Backups?.....	77
12.2.4 Can I Choose to Back Up Only Some Partitions of a Disk?.....	77
12.2.5 Does CBR Support Cross-Region Backup?.....	77
12.2.6 Will the Server Performance Be Affected If I Delete Its Backups?.....	77
12.2.7 Can I Use Its Backup for Restoration After a Resource Is Deleted?.....	78
12.2.8 How Many Backups Can I Create for a Resource?.....	78
12.2.9 Can I Stop an Ongoing Backup Task?.....	78

12.3 Capacity.....	78
12.3.1 Why Is My Backup Size Larger Than My Disk Size?.....	78
12.4 Restoration.....	79
12.4.1 Do I Need to Stop the Server Before Restoring Data Using Backups?.....	79
12.4.2 Can I Use a System Disk Backup to Recover an ECS?.....	79
12.4.3 Do I Need to Stop the Server Before Restoring Data Using Disk Backups?.....	79
12.4.4 Can a Server Be Restored Using Its Backups After It Is Changed?.....	79
12.4.5 Can a Disk Be Restored Using Its Backups After Its Capacity Is Expanded?.....	79
12.4.6 What Can I Do if the Password Becomes a Random One After I Use a Backup to Restore a Server or Use an Image to Create a Server?.....	80
12.4.7 What Changes Will Be Made to the Original Backup When I Use the Backup to Restore a Server?.....	80
12.4.8 Can I Stop an Ongoing Restoration Task?.....	80
12.5 Policies.....	80
12.5.1 How Do I Configure Automatic Backup for a Server or Disk?.....	80
12.5.2 Why the New Retention Rule I Changed Is Not Applied?.....	81
12.5.3 How Do I Back Up Multiple Resources at a Time?.....	82
12.6 Others.....	82
12.6.1 Is There a Quota for CBR Vaults?.....	82
12.6.2 Can I Merge My Vaults?.....	82
<b>13 Troubleshooting Cases.....</b>	<b>83</b>
13.1 Failed to Attach Disks.....	83
13.2 Data Disks Are Not Displayed After a Windows Server Is Restored.....	84
13.3 Failed to Cancel Backup Sharing.....	86
13.4 Failed to Download or Install the Agent Required by Application-Consistent .....	86
13.5 A Server Created Using an Image Enters Maintenance Mode After Login.....	89
<b>A Appendix.....</b>	<b>93</b>
A.1 Agent Security Maintenance.....	93
A.1.1 Changing the Password of User rdadmin.....	93
A.1.2 Changing the Password of the Account for Reporting Alarms (SNMP v3).....	94
A.1.3 Replacing the Server Certificate.....	96
A.1.4 Replacing CA Certificates.....	98
A.2 Change History.....	100

# 1 Service Overview

---

## 1.1 What Is CBR?

### Overview

Cloud Backup and Recovery (CBR) enables you to easily back up Elastic Cloud Servers (ECSs) and Elastic Volume Service (EVS) disks. In case of a virus attack, accidental deletion, or software or hardware fault, you can use the backup to restore data to any point when the data was backed up.

### CBR Architecture

CBR involves backups, vaults, and policies.

#### 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. 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. Backups of non-database servers are non-database server backups, and those of database servers are application-consistent backups.

#### Vault

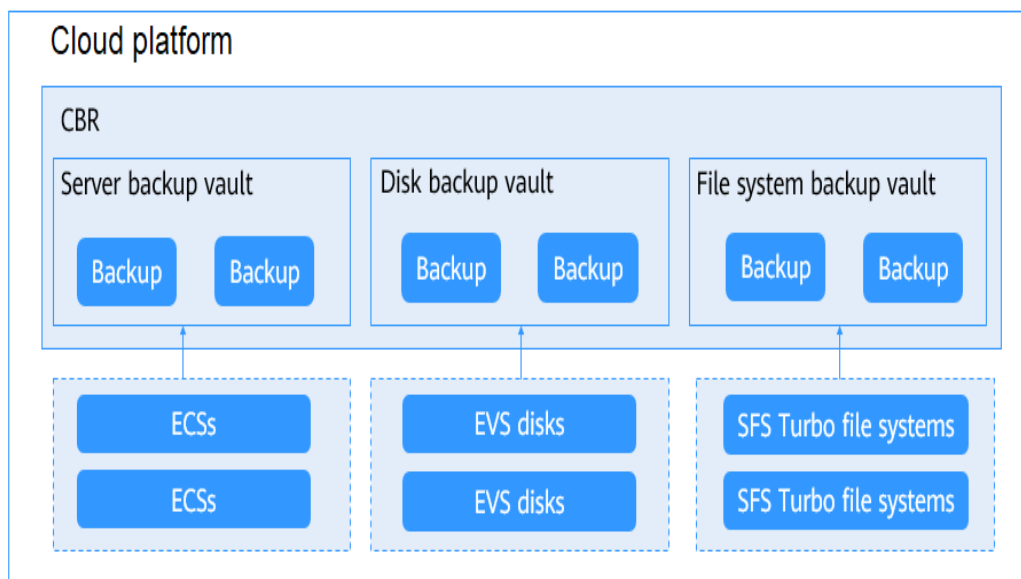
CBR stores backups in vaults. Before creating a backup, you need to create at least one vault and associate the resources you want to back up with the vaults. Then the resources can be backed up to the associated vaults.

Different types of resources must be backed up to different types of vaults. For example, cloud servers must be backed up to server backup vaults, not disk backup vaults or any other types of vaults.

#### Policy

- A backup policy defines when you want to take a backup and for how long you would retain each backup.

**Figure 1-1** CBR architecture



## Differences Among the Backup Types

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

Item	Cloud Server Backup	Cloud Disk Backup
What to back up	All disks (system and data disks) on a server	One or more specific disks (system or data disks)
When to use	You want to back up entire cloud servers.	You want to back up only data disks.
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.

## 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.

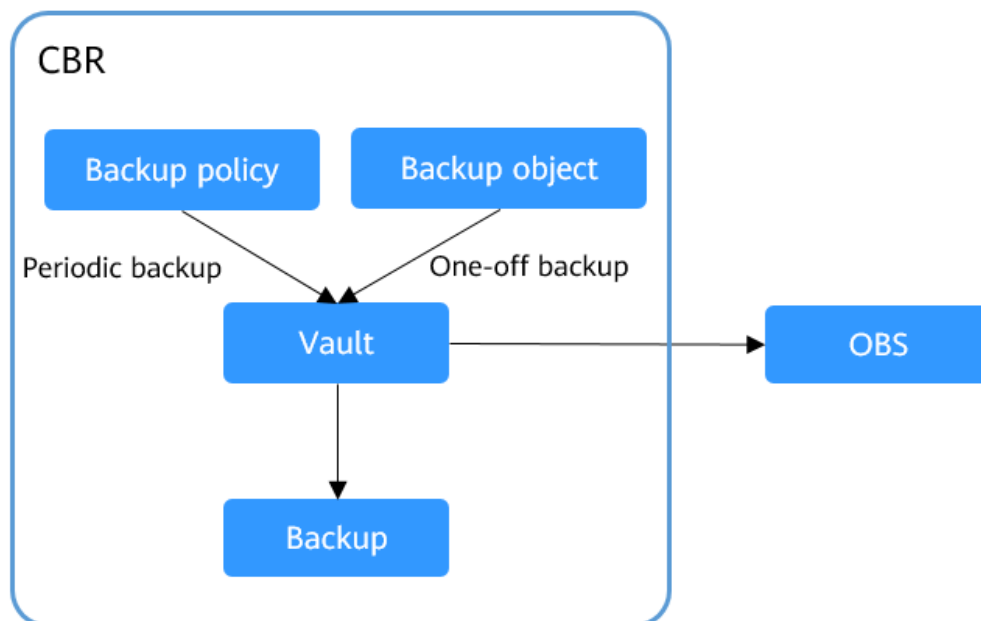
**Table 1-2** compares the two backup options.

**Table 1-2** 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 1-2** shows the use of the two backup options.



**Figure 1-2** Use of the two backup options

## Access to CBR

You can access the CBR service through the console or by calling HTTPS-based APIs.

- Console  
Use the console if you prefer a web-based UI. Log in to the console and choose **Cloud Backup and Recovery**.
- APIs  
Use APIs if you need to integrate CBR into a third-party system for secondary development. For details, see the *Cloud Backup and Recovery API Reference*.

## 1.2 Application Scenarios

CBR is ideal for data backup and restoration. The backups can maximize your data security and consistency.

### Data Backup and Restoration

You can use CBR to quickly restore data to the latest backup point if any of the following incidents occur:

- Hacker or virus attacks
- Accidental deletion
- Application update errors
- System breakdown

## 1.3 Functions

**Table 1-3** lists the functions of CBR.

Before using CBR functions, it is recommended that you learn about **basic CBR concepts**.

**Table 1-3** CBR functions

Category	Function	Description
Cloud disk backup	Manual disk backup	Cloud disk backup provides snapshot-based backup for EVS disks on servers. You can back up specific disks to protect data on them.
Cloud disk backup	Policy-based backup	You can create, modify, or delete a backup policy. A backup policy defines the schedule and retention for automatic backups.
Cloud disk backup	Backup management	You can set search criteria to quickly find the backups you want to manage. Then you can view their details, share, restore, or delete them if needed.
Cloud disk backup	Disk restoration using backups	When a disk is faulty, or their data is lost, you can use a backup to quickly restore the data.
Cloud disk backup	Disk creation using backups	You can use a disk backup to create a disk that contains the same data as the backup.
Cloud disk backup	Sharing a Backup	You can share a disk backup with other accounts to allow them to use the backup to create disks.
Cloud server backup	Manual server backup	Cloud server backup uses the consistency snapshot technology to protect data for ECSs without the need to install the Agent. You can use CBR to back up an entire server to protect their data.
Cloud server backup	Policy-based backup	You can create, modify, or delete a backup policy. A backup policy defines the schedule and retention for automatic backups.

Category	Function	Description
Cloud server backup	Backup management	You can set search criteria to quickly find the backups you want to manage. Then you can view their details, share, restore, replicate, or delete them if needed.
Cloud server backup	Server restoration using backups	When a server is faulty, or their data is lost, you can use a backup to quickly restore the data.
Cloud server backup	Sharing a Backup	You can share a server backup with other accounts to allow them to use the backup to create servers.
Cloud server backup	Image creation using server backups	You can create images from ECS backups and then use the images to quickly provision ECSs to restore service.
Cloud server backup	Database server 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.

## 1.4 Permissions

If you need to assign different permissions to personnel in your enterprise to access your CBR resources, Identity and Access Management (IAM) is a good choice for fine-grained permissions management. IAM provides identity authentication, permissions management, and access control, helping you to securely access your cloud resources.

With IAM, you can create IAM users and assign permissions to control their access to specific resources. For example, if you want some software developers in your enterprise to use CBR resources but do not want them to delete CBR resource or perform any other high-risk operations, you can create IAM users and grant permission to use CBR resources but not permission to delete them.

If your cloud account does not require individual IAM users for permissions management, you can skip this section.

IAM is a free service. You only pay for the resources in your account. For more information about IAM, see the *Identity and Access Management Service Overview*.

## CBR Permissions

New IAM users do not have any permissions assigned by default. You need to first add them to one or more groups and attach policies or roles to these groups. The users then inherit permissions from the groups and can perform specified operations on cloud services based on the permissions they have been assigned.

CBR is a project-level service deployed for specific regions. When you set **Scope** to **Region-specific projects** and select the specified projects in the specified regions, the users only have permissions for CBR resources in the selected projects. If you set **Scope** to **All resources**, the users have permissions for CBR resources in all region-specific projects. When accessing CBR resources, the users need to switch to the authorized region.

You can grant permissions by using roles and policies.

- **Roles:** A coarse-grained authorization strategy provided by IAM to assign permissions based on users' job responsibilities. Only a limited number of service-level roles are available for authorization. Cloud services depend on each other. When you grant permissions using roles, you also need to attach any existing role dependencies. Roles are not ideal for fine-grained authorization and least privilege access.
- **Policies:** A fine-grained authorization strategy that defines permissions required to perform operations on specific cloud resources under certain conditions. This type of authorization is more flexible and is ideal for least privilege access. For example, you can grant users only permission to manage ECSs of a certain type. A majority of fine-grained policies contain permissions for specific APIs, and permissions are defined using API actions. For the API actions supported by CBR, see "Permissions Policies and Supported Actions".

**Table 1-4** lists all the system-defined permissions for CBR.

**Table 1-4** System-defined permissions for CBR

Policy Name	Description	Type
CBR FullAccess	Administrator permissions for CBR. Users with these permissions can operate and use all vaults, backups, and policies.	System-defined policy
CBR BackupsAndVaults-FullAccess	Common user permissions for CBR. Users with these permissions can create, view, and delete vaults and backups, but cannot create, update, or delete policies.	System-defined policy
CBR ReadOnlyAccess	Read-only permissions for CBR. Users with these permissions can only view CBR data.	System-defined policy

**Table 1-5** lists the common operations supported by system-defined permissions of CBR.

**Table 1-5** Common operations supported by system-defined permissions of CBR

Operation	CBR FullAccess	CBR BackupsAndVaultsFullAccess	CBR ReadOnlyAccess
Querying vaults	Supported	Supported	Supported
Creating vaults	Supported	Supported	Not supported
Listing vaults	Supported	Supported	Supported
Updating vaults	Supported	Supported	Not supported
Deleting vaults	Supported	Supported	Not supported
Associating resources	Supported	Supported	Not supported
Dissociating resources	Supported	Supported	Not supported
Creating policies	Supported	Not supported	Not supported
Updating policies	Supported	Not supported	Not supported
Applying policies to vaults	Supported	Supported	Not supported
Removing policies from vaults	Supported	Supported	Not supported
Deleting policies	Supported	Not supported	Not supported
Performing backups	Supported	Supported	Not supported
Updating subscriptions	Supported	Supported	Not supported
Querying the Agent status	Supported	Supported	Not supported
Deleting backups	Supported	Supported	Not supported
Restoring data from backups	Supported	Supported	Not supported
Associating vaults	Supported	Supported	Not supported

## 1.5 Constraints

### General

- A vault can be associated with only one backup policy.
- A vault can be associated with a maximum of 256 resources.
- A maximum of 32 backup policies can be created.
- Only backups in the **Available** or **Locked** vaults can be used to restore data.
- Backups in a **Deleting** vault cannot be deleted.
- When Storage Disaster Recovery Service (SDRS) is used to set up disaster recovery for cloud servers, restorations can be performed at the disaster recovery site only after protection is disabled.
- Backups cannot be downloaded to a local PC or uploaded to OBS.
- A vault and its associated servers or disks must be in the same region.

### Cloud Disk Backup

- Only disks in the **Available** or **In-use** state can be backed up.
- A new disk must be at least as large as the backup's source disk.

### Cloud Server Backup

- A maximum of 10 shared disks can be backed up with a cloud server.
- Only backups in the **Available** or **Locked** vaults can be used to create images.
- Cloud servers support crash-consistent backup, whereas database servers support application-consistent backup in addition to crash-consistent backup.
- Images cannot be created from backups if the amount of resources associated with a server backup vault exceeds the quota.
- You are advised not to back up a server whose disk size exceeds 4 TB.

### Application-Consistent Backup

**Table 1-6** 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 and 12 for x86_64

Database	OS	Version
	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

## 1.6 CBR and Other Services

### CBR-related Services

Table 1-7 CBR-related services

Function	Related Service	Reference
CBR backs up data of an ECS and uses the backup to restore data for the ECS. You can also create images from ECS backups and use the images to quickly provision ECSs to restore services.	ECS	Creating a Cloud Server Backup Creating a Cloud Disk Backup
CBR stores backups securely in OBS.	OBS	<a href="#">What Is CBR?</a>
CBR backs up data of EVS disks and uses the backup to create new disks.	EVS	Creating a Cloud Disk Backup
IAM is a self-service system for enterprise administrators to manage cloud resources. It provides user identity management and access control functions.	IAM	<a href="#">Permissions</a>

## 1.7 Basic Concepts

### 1.7.1 CBR Concepts

#### Vault

CBR stores backups of a variety of resources in vaults, which 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 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.

## 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.

## Backup Policy

A backup policy is a set of rules that define the schedule and retention of backups. After you apply a backup policy to a vault, CBR automatically backs up data and retains backups based on that backup policy.

## Instant Restore

Instant Restore restores data and creates images from backups, much faster than a normal restore.

Instant Restore is an enhanced function of CBR and requires no additional configuration. After Instant Restore is provided, you take less time to restore server data or create images.

## Enhanced Backup

Enhanced backups are backups generated after Instant Restore is provided. Enhanced backups make it faster to restore server data or create images.

Before providing Instant Restore, CBR generates common backups. After providing Instant Restore, CBR first performs a full backup for each associated resource and then generates enhanced backups. CBR only generates enhanced backups currently.

For the same resource, an enhanced backup and a common backup have the same backup content and size. They only differ in the restoration speed.

## Application-Consistent Backup

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.
- **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.

CBR cloud server backup supports both crash-consistent backup and application-consistent backup (also called database server backup). Install the Agent before enabling application-consistent backup to prevent the database server backup from failing.

## 1.7.2 Region and AZ

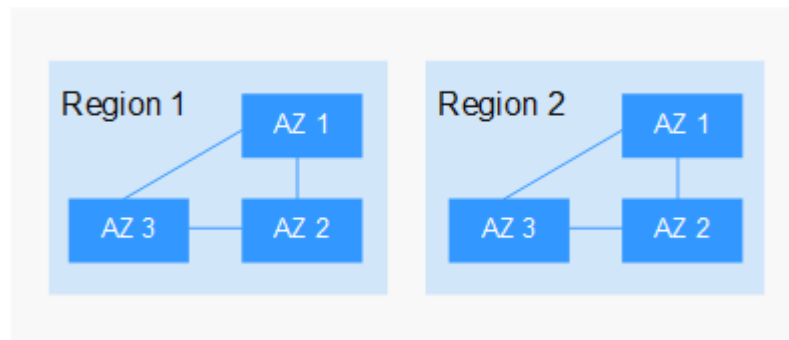
### Concept

A region and availability zone (AZ) identify the location of a data center. You can create resources in a specific region and AZ.

- A region is a physical data center, which is completely isolated to improve fault tolerance and stability. The region that is selected during resource creation cannot be changed after the resource is created.
- An AZ is a physical location where resources use independent power supplies and networks. A region contains one or more AZs that are physically isolated but interconnected through internal networks. Because AZs are isolated from each other, any fault that occurs in one AZ will not affect others.

**Figure 1-3** shows the relationship between regions and AZs.

**Figure 1-3** Regions and AZs



### Selecting a Region

Select a region closest to your target users for lower network latency and quick access.

### Selecting an AZ

When deploying resources, consider your applications' requirements on disaster recovery (DR) and network latency.

- For high DR capability, deploy resources in different AZs within the same region.

- For lower network latency, deploy resources in the same AZ.

## Regions and Endpoints

Before you use an API to call resources, specify its region and endpoint. For more details, see [Regions and Endpoints](#).

# 2 Getting Started

---



## 2.1 Step 1: Create a Vault

### 2.1.1 Creating a Server Backup Vault

This section describes how to create a server 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** In the upper right corner of the page, click **Create Server Backup Vault**.

**Step 3** Select a protection type.

- **Backup:** A server backup vault stores server backups.

**Step 4** (Optional) In the server list, select the servers or disks you want to back up. After the servers or disks are selected, they are added to the list of selected servers. You can also select specific disks on a server and associate them with the vault.

#### NOTE

- The selected servers must have not been associated with any vault and must be in the **Running** or **Stopped** state.
- You can also associate servers with the vault you are creating later if you skip this step.

**Step 5** Specify a vault capacity ranging from 10 GB to 10,485,760 GB. Properly plan the vault capacity, which must be at least the same as the size of the servers you want

to back up. Also, if automatic association is enabled and a backup policy is applied to the vault, more capacity is required.

As the vault's used space grows, you can expand the vault capacity if it becomes insufficient.

**Step 6** 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 servers associated with this vault will be automatically backed up based on this policy.
- If you select **Skip**, servers associated with this vault will not be automatically backed up until you apply a backup policy to the vault.

**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** Complete the creation as prompted.

**Step 9** Go back to the **Cloud Server Backups** page. You can see the created vault in the vault list.

You can associate servers with the vault and perform backup for the servers. For details, see [Querying a Vault](#).



----End

## 2.1.2 Creating a Disk Backup Vault

This section describes how to create a 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** In the upper right corner of the page, click **Create Disk Backup Vault**.

**Step 3** (Optional) In the disk list, select the disks you want to back up. After disks are selected, they are added to the list of selected disks.

 **NOTE**

- The selected disks must have not been associated with any vault and must be in the **Available** or **In-use** state.
- You can also associate disks with the vault you are creating later if you skip this step.

**Step 4** Specify a vault capacity ranging from 10 GB to 10,485,760 GB. Properly plan the vault capacity, which must be at least the same as the size of the disks you want to back up.

**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 disks associated with this vault will be automatically backed up based on this policy.
- If you select **Skip**, disks associated with this vault will not be automatically backed up until you apply a backup policy to the vault.

**Step 6** Specify a name for the vault.

The name must contain 1 to 64 characters including digits, letters, underscores (\_), or hyphens (-), for example, **vault-612c**.

 **NOTE**

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

**Step 7** Complete the creation as prompted.

**Step 8** Go back to the **Cloud Disk Backups** page. You can see the created vault in the vault list.

You can associate disks to the new vault or perform backup for the disks. For details, see [Vault Management](#).

----End

## 2.2 Step 2: Associate a Resource with the Vault

If you have already associated servers or disks when creating a vault, skip this step.

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

### 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 2-1** Resource statuses available for association

Resource Type	Status
Cloud server	Running or Stopped
Cloud disk	Available or In-use

## 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** or **Associate Disk**.

**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.

**Step 4** Click **OK**. Then on the **Associated Servers** tab page, you can view the number of resources that have been associated.

### 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.

- You can enable automatic association only when the vault's remaining capacity (Vault's total capacity – Vault's associated capacity) is greater than both 40 GB and the associated capacity. 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, you can enable automatic association.

- 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.

**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.

----End

## 2.3 Step 3: Create a Backup

### 2.3.1 Creating a Cloud Server Backup

This section describes how to quickly create a cloud server backup.

If you do not need an ECS for the moment, you can back up the ECS and then delete it. When you want an ECS later, you can create an image from the ECS backup and use the image to create ECSs.

Backing up a server does not impact the server performance.



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.

## Prerequisites

- Only servers in the **Running** or **Stopped** state can be backed up.
- At least one server backup vault 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** On the **Cloud Server Backups** page, click the **Vaults** tab and find the vault to which the server is associated.

**Step 3** Perform backup in either of the following ways:

- Choose **More > Perform Backup** in the **Operation** column. In the server list, select the server you want to back up. After a server is selected, it is added to the list of selected servers.
- Click the vault name to go to the vault details page. On the **Associated Servers** tab page, locate the target server and click **Perform Backup** in the **Operation** column.

**Step 4** Set **Name** and **Description** for the backup. [Table 2-2](#) describes the parameters.

**Table 2-2** Parameter description

Parameter	Description	Remarks
Name	Name of the backup you are creating. A name must contain 1 to 64 characters including digits, letters, underscores (_), or hyphens (-). <b>NOTE</b> You can also use the default name <b>manualbk_XXX</b> . If multiple servers are to be backed up, the system automatically adds suffixes to their backup names, for example, <b>backup-0001</b> and <b>backup-0002</b> .	manualbk_d819
Description	Description of the backup. It cannot exceed 255 characters.	--

**Step 5** Choose whether to enable full backup. If full backup is enabled, CBR performs a full backup on every associated server, which requires a larger capacity compared to an incremental backup.



**Step 6** Click **OK**. CBR automatically creates a backup for the server.

On the **Backups** tab page, if the status of the backup is **Available**, the backup task is successful.

 **NOTE**

A server can be restarted if the backup progress exceeds 10%. However, to ensure data integrity, restart it after the backup is complete.

After the backup is complete, you can use the backup to restore server data or create an image. For details, see [Restoring from a Cloud Server Backup](#) and [Creating an Image from a Cloud Server Backup](#).

----End

## 2.3.2 Creating a Cloud Disk Backup

This section describes how to quickly create a cloud disk backup.

Backing up a server does not impact the disk performance.



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.

### Prerequisites

A disk can be backed up only when its status is **Available** or **In-use**. If you have performed operations such as expanding, attaching, detaching, or deleting a disk, refresh the page first to ensure that the operation is complete and then determine whether to back up the disk.

### 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 Disk Backups** page, click the **Vaults** tab and find the vault to which the disk is associated.

**Step 3** Perform backup in either of the following ways:

- Click **Perform Backup** in the **Operation** column. In the disk list, select the disk you want to back up. After a disk is selected, it is added to the list of selected disks.

- Click the vault name to go to the vault details page. On the **Associated Disks** tab page, locate the target disk and click **Perform Backup** in the **Operation** column.

**Step 4** Set **Name** and **Description** for the backup. [Table 2-3](#) describes the parameters.

**Table 2-3** Parameter description

Parameter	Description	Remarks
Name	Name of the backup you are creating. A name must contain 1 to 64 characters including digits, letters, underscores (_), or hyphens (-). <b>NOTE</b> You can also use the default name <b>manualbk_XXXX</b> . If multiple disks are to be backed up, the system automatically adds suffixes to their backup names, for example, <b>backup-0001</b> and <b>backup-0002</b> .	manualbk_d819
Description	Description of the backup. It cannot exceed 255 characters.	--

**Step 5** Choose whether to enable full backup. If full backup is enabled, CBR performs a full backup on every associated disk, which requires a larger capacity compared to an incremental backup.

**Step 6** Click **OK**. CBR automatically creates a backup for the disk.

On the **Backups** tab page, if the status of the backup is **Available**, the backup task is successful.

 **NOTE**

If you delete data from the disk during the backup, the deleted data 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 is complete, you can use the backup to restore disk data. For details, see [Restoring from a Cloud Disk Backup](#).

----End

# 3 Permissions Management

---

## 3.1 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 cloud account or cloud service to perform efficient O&M on your CBR resources.

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

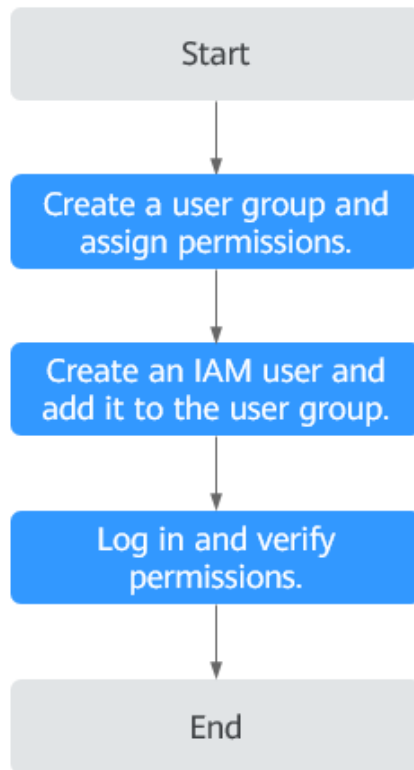
Figure [Figure 3-1](#) illustrates the procedure for granting permissions.

### Prerequisites

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

## Process Flow

Figure 3-1 Process for granting CBR permissions



1. Create a user group and assign permissions.  
Create a user group on the IAM console and click **Authorize** in the **Operation** column to assign the **CBR ReadOnlyAccess** permissions to the group.
2. Create an IAM user and add it to the user group.  
Create a user on the IAM console and add it to the user group created in **1** by choosing **Authorize** in the **Operation** column.
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 **Create 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.

## 3.2 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 section "Permissions Policies and Supported Actions" in *Cloud Backup and Recovery API Reference*.

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"
      ]
    }
  ]
}
```

## 3.3 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"  
          ]  
        }  
      }  
    }  
  ]  
}
```

# 4 Vault Management

## 4.1 Querying 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.

**Table 4-1** Basic information parameters

Parameter	Description
Name/ID	Name and ID of the vault. Click the vault name to view details about the vault.
Type	Vault type
Status	Vault status. <a href="#">Table 4-2</a> describes the vault statuses.



Parameter	Description
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>
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>

**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 4-2](#) describes the vault statuses.

**Table 4-2** 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	<p>An intermediate state displayed when a capacity expansion is in progress.</p> <p>If a vault is in this state, you can perform operations, such as applying a policy and associating servers or disks. However, the following operations are not allowed on such a vault: expanding the vault capacity and changing the vault specifications. Once those operations are complete, the vault status will become <b>Available</b>.</p>

Status	Attribute	Description
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 technical support.
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 technical support.

- Search a vault by its name or ID.

**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.

----End

## 4.2 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.

### Prerequisites

- There is at least one vault.
- The vault 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** Find the target vault and choose **More > Delete** in the **Operation** column. All backups stored in the vault will be deleted once you delete a vault.

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

----End

## 4.3 Dissociating a Resource



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 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.

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

----End

## 4.4 Migrating a Resource

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.

### Constraints



- Resources can be migrated only when the source and destination vaults are in the **Available** or **Locked** state.
- 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.

- 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.

## 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.

**Step 4** Select the destination vault and click **OK**.

**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

## 4.5 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.

- 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

## 4.6 Changing Vault Specifications



Server backup vaults and server replication vaults both 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.
- Step 3** **Application-Consistent Backup** is preset for **Backup Type**. Click **Next**.
- Step 4** Click **Submit** and complete the payment. The system automatically changes the vault specifications.
- End

# 5 Backup Management

## 5.1 Viewing a Backup



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.

- You can search for backups by selecting a status from the **All statuses** drop-down list in the upper right corner of the backup list. [Table 5-1](#) describes the backup statuses.

**Table 5-1** Backup statuses

Status	Status Attribute	Description
All statuses	--	All backups are displayed if this value is selected.

Status	Status Attribute	Description
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 technical support.
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 technical support.
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 technical support.
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 technical support.

- You can search for backups by clicking **Advanced Search** in the upper right corner of the backup list.

You can search by specifying a backup status, backup name, backup ID, vault ID, server name, server ID, server type, or the creation date.

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

----End

## 5.2 Sharing a Backup

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

### Context

**Sharer**



- Backups can only be shared among 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.

### 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.

## Procedure for the Sharer

**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

1. Click the **Share Backup** tab.
2. Enter the account name of the recipient.
3. Click **Add**.

The account and project to be added will be displayed in the list. You can add multiple account names. A backup can be shared to a maximum of 10 projects.

4. Click **OK**.

- Canceling sharing



1. Click the **Cancel Sharing** tab, select the projects you want to cancel sharing, and click **OK**.



----End

## Procedure for the Recipient

**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 [Step 1: Create 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.

**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.

**Step 5** View the shared backup you accepted in the backup list.

----End

## 5.3 Deleting a Backup

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

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](#).



### 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. Alternatively, select the backups you want to delete in a batch and click **Delete** in the upper left corner to delete them.

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



----End

# 6 Policy Management

---

## 6.1 Viewing the Policy of a 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** Find the target vault and click the vault name to view its details.

**Step 3** View the policy applied to the vault.

----End

## 6.2 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.



### Constraints

- Backup policies can be applied to the following types of vaults: server backup vaults, disk 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 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 all 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**.

**Step 3** Set the backup policy parameters. [Table 6-1](#) describes the parameters.

**Table 6-1** 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
Status	Whether to enable the backup policy.	Only after a backup policy is enabled and applied will CBR automatically backs up the vault resources and deletes expired backups.

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>
Backup Cycle	<p>Select a backup cycle.</p> <ul style="list-style-type: none"> <li><b>Week-based cycle</b> Specifies on which days of each week the backup task will be executed. You can select multiple days.</li> <li><b>Custom cycle</b> Specifies the interval (every 1 to 30 days) for executing the backup task.</li> </ul>	<p>Every day</p> <p>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.</p> <p>It is recommended that backups be performed during off-peak hours or when no services are running.</p>

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>Permanent</b></li> </ul> <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>	6 months

 **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.

## 6.3 Modifying a Policy



You can modify a policy to better suit your services.

### 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.

Related parameters are described in [Table 6-1](#).

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

If the retention rule is modified, the new rule does not necessarily apply to existing backups. For details, see [Why the New Retention Rule I Changed Is Not Applied?](#)

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

----End

## 6.4 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 **Yes**.

----End

## 6.5 Applying a Policy to a Vault



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

## Constraints

A vault can only be associated with one backup policy.

## 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**.

**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](#).

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

----End



## 6.6 Removing a Policy from a Vault



If you no longer need automatic backup for a vault, remove the policy from the 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**.

#### NOTE

- If a policy is removed when a backup task is being executed for a resource in the vault, the backup task 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

# 7 Restoring Data

---

## 7.1 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.

### 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.

### 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** In the row of the backup, click **Restore Server**.

---

#### NOTICE

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

---

**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

## 7.2 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 ECS has been optimized before being backed up, and the Cloud-Init (for Linux) or Cloudbase-Init (for Windows) tool has been installed.
- 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.

### 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 section "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 section "Creating an ECS from an Image" in the *Image Management Service User Guide*.
- End

## 7.3 Restoring from a Cloud Disk Backup

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



### 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

- 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.

### 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**.

---

#### 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.
-

**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 section "Attaching an Existing Non-Shared Disk" in the *Elastic Volume Service User Guide*.

----End



## 7.4 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.

### 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 "Create 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**.

**Step 6** 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 Application-Consistent Backup

---

## 8.1 What Is 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. 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.

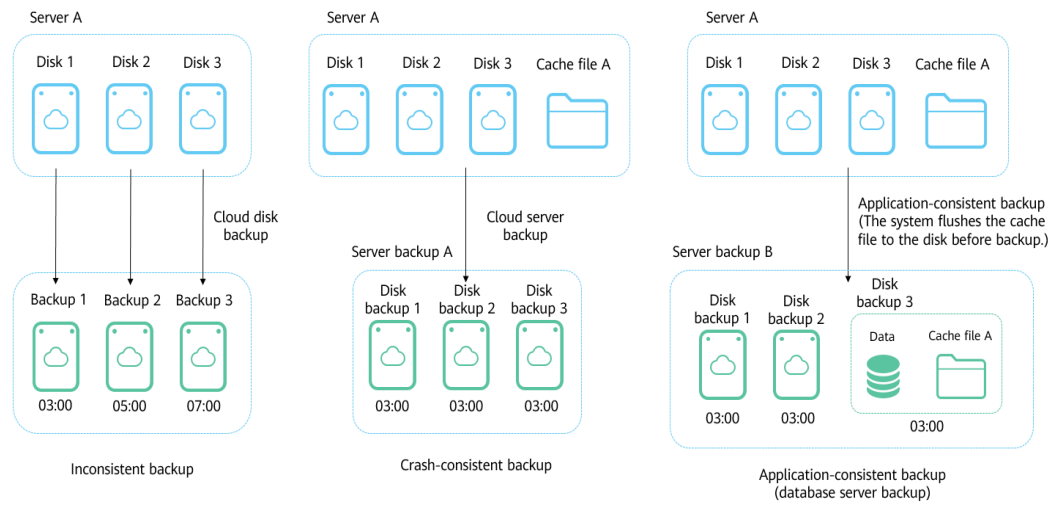
**Figure 8-1** compares these backup types in detail.

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 8-1 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 8-1** lists the OSs that support the installation of Agent.

**Table 8-1** OSs that support installation of the Agent

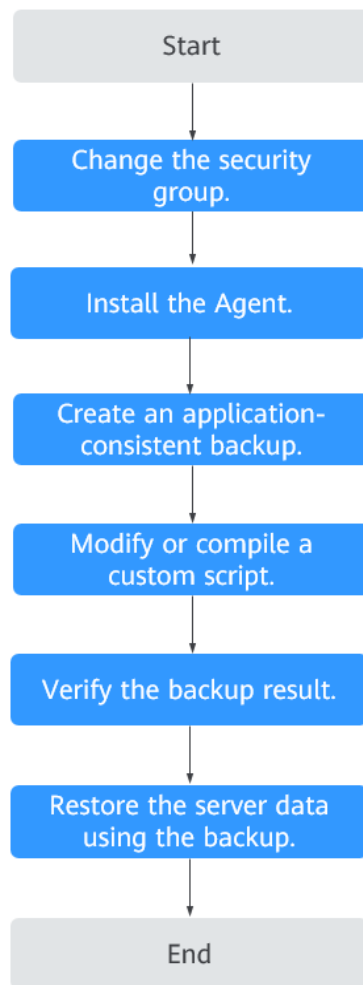
Database	OS	Version
SQL Server 2008/2012/2019	Windows	Windows Server 2008, 2008 R2, 2012, 2012 R2, and 2019 for x86_64
SQL Server 2014/2016/Enterprise Edition	Windows	Windows Server 2014, 2014 R2, and 2016 Datacenter for x86_64
MySQL 5.5/5.6/5.7	Red Hat	Red Hat Enterprise Linux 6 and 7 for x86_64
	SUSE	SUSE Linux Enterprise Server 11 and 12 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

For the databases not included in this list, you can customize a script to perform application-consistent backup by referring to section "Using a Custom Script to Implement Application-Consistent Backup" in the *Cloud Backup and Recovery Best Practices*.

## Process

**Figure 8-2** shows the application-consistent backup process.

**Figure 8-2** 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. For details, see [Changing a Security Group](#).
- 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. For details, see [Installing the Agent](#).
- 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. For details, see [Creating 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 the *Cloud Backup and Recovery Best Practices*.
- Step 5** Verify the backup result: After the backup is performed, verify that the backup succeeds. For details, see the *Cloud Backup and Recovery Best Practices*.
- 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

## 8.2 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**. 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.

**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. 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.

- Step 5** Click the **Outbound Rules** tab, and then click **Add Rule**. The **Add Outbound Rule** dialog box is displayed. 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.

----End

## 8.3 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

- 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 8-2](#) lists OSs that support installation of the Agent.

**Table 8-2** 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 and 12 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

- **Table 8-3** lists the supported SHA256 values.

**Table 8-3** 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.

**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 8-3](#).

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.

**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**.

- 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 8-3](#).
- 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.
- 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

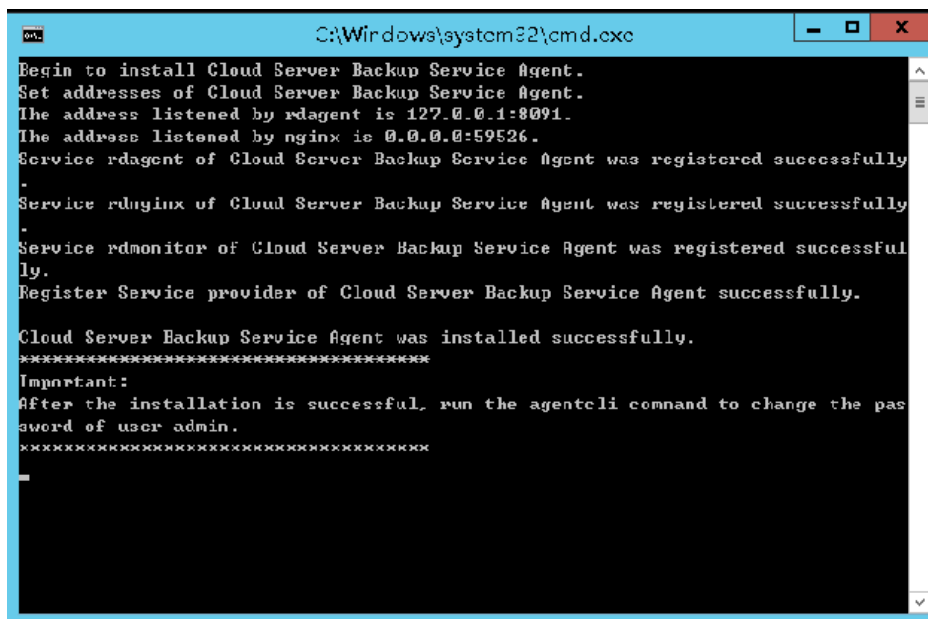
## Installing the Agent for a Windows OS (Method 1)

- 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.
- 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 8-3](#).





- 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 8-3](#).

**Figure 8-3** 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.
- 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 *region1* as the example region. Then press **Enter** to download the installation package.

**https://csbs-agent-region1.obs.region1.myhwclouds.com/Cloud Server Backup Agent-WIN64.zip**

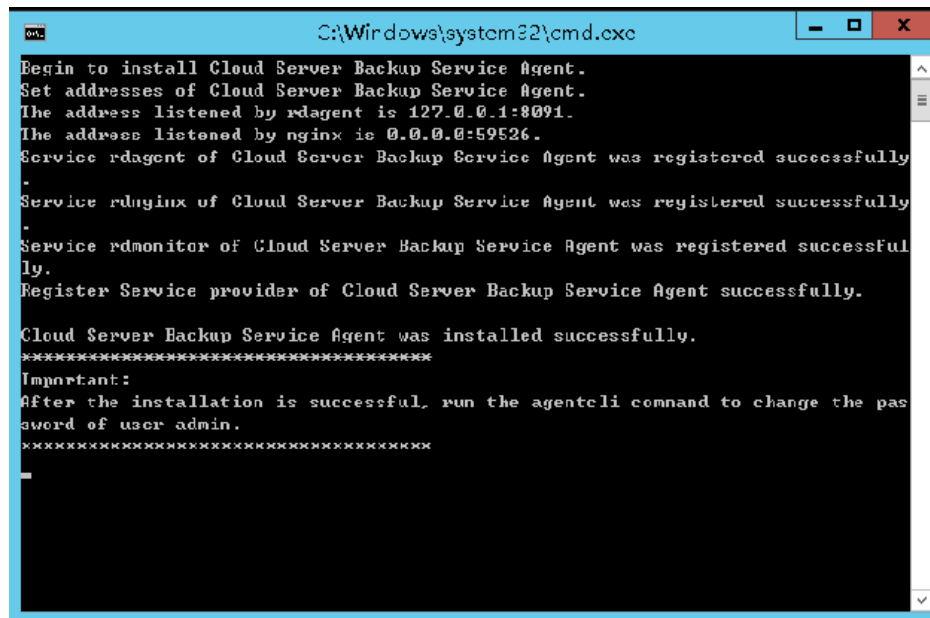
**Step 6** After downloading the Agent to a local directory, check that the package's SHA256 value is the same as that listed in [Table 8-3](#).

**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 8-4](#).

**Figure 8-4** Successful client installation for Windows



```
C:\Windows\system32\cmd.exe
Begin to install Cloud Server Backup Service Agent.
Set addresses of Cloud Server Backup Service Agent.
The address listened by rdagent is 127.0.0.1:8091.
The address listened by nginx is 0.0.0.0:59526.
Service rdagent of Cloud Server Backup Service Agent was registered successfully.
Service rdnginx of Cloud Server Backup Service Agent was registered successfully.
Service rdmonitor of Cloud Server Backup Service Agent was registered successfully.
Register Service provider of Cloud Server Backup Service Agent successfully.
Cloud Server Backup Service Agent was installed successfully.
*****
Important:
After the installation is successful, run the agentcli command to change the password of user admin.
*****
```

----End

## 8.4 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 [Creating a Server Backup Vault](#). Select **Enable** for **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.

**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 from a Cloud Server Backup](#) and [Creating an Image from a Cloud Server Backup](#).

# 8.5 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 8-5** displays an example. If the word **successfully** in green is displayed, the Agent is uninstalled successfully.

```
sh agent_uninstall_ebk.sh
```

**Figure 8-5** Agent uninstalled successfully from Linux

```
user@rdadmin:~/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 8-6**.

**Figure 8-6** 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

# 9 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

**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 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

# 10 Monitoring

## 10.1 CBR Metrics

### 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 10-1** 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<br>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 & Deployment > 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.

**Step 3** View the vault monitoring data by metric or monitored duration.

For more information, see the *Cloud Eye User Guide*.

----End

## 10.2 Creating an Alarm Rule

Cloud Eye allows you to use alarm templates to create alarm rules, making it easy and convenient to add or modify alarm rules for resources or cloud services, especially for a large number of resources and cloud services.

You can use a default alarm template to create an alarm rule for a cloud service resource.

You can create alarm rules for CBR.

### Procedure

1. Log in to the management console.
2. Under **Management & Deployment**, 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**.  
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.
- If you select **Cloud Backup and Recovery** for **Resource Type**, vaults are monitored with two metrics. [Table 10-2](#) describes the parameters.

**Table 10-2** Parameters

| Parameter        | Description                                                                                                                                                                                                                                                                                                                                                                                                                   | Example Value             |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------|
| Resource Type    | <b>Cloud Backup and Recovery</b> is selected in this example.                                                                                                                                                                                                                                                                                                                                                                 | Cloud Backup and Recovery |
| Dimension        | Monitoring dimension. By default, monitoring is performed by vault.                                                                                                                                                                                                                                                                                                                                                           | Vault                     |
| Monitoring Scope | Choose the vaults you want to monitor from the list.                                                                                                                                                                                                                                                                                                                                                                          | vault-56f8                |
| Method           | You can create an alarm rule by using the template or manually creating it.<br><b>NOTE</b><br>If you set <b>Monitoring Scope</b> to <b>Specific resources</b> , you can set <b>Method</b> to <b>Use template</b> .                                                                                                                                                                                                            | Use template              |
| Template         | Template to be used.                                                                                                                                                                                                                                                                                                                                                                                                          | -                         |
| Alarm Policy     | Policy for triggering an alarm.<br>If you set <b>Resource Type</b> to a specific cloud service, the alarm policy takes effect periodically. If you set <b>Resource Type</b> to <b>Event Monitoring</b> , the alarm policy takes effect based on specific events.<br>Currently, the following CBR monitoring metrics are supported: <ul style="list-style-type: none"> <li>• Vault Usage</li> <li>• Used Vault Size</li> </ul> | -                         |



| Parameter      | Description                                                                                            | Example Value |
|----------------|--------------------------------------------------------------------------------------------------------|---------------|
| Alarm Severity | Alarm severity, which can be <b>Critical</b> , <b>Major</b> , <b>Minor</b> , or <b>Informational</b> . | Major         |

- If you set **Resource Type** to **Event Monitoring**, CBR resources are monitored based on specific events. [Table 10-2](#) describes the parameters.

**Table 10-3** Parameters

| Parameter        | Description                                                                                                       | Example Value      |
|------------------|-------------------------------------------------------------------------------------------------------------------|--------------------|
| Resource Type    | <b>Event Monitoring</b> is selected in this example.                                                              | Event Monitoring   |
| Dimension        | Metric dimension of the selected resource type.                                                                   | System event       |
| Monitoring Scope | Monitoring scope for event monitoring.<br>Default value: <b>All resources</b>                                     | -                  |
| Method           | Select Configure manually.                                                                                        | Configure manually |
| Alarm Policy     | Policy for triggering an alarm.<br><a href="#">Table 10-4</a> lists the supported CBR events that trigger alarms. | -                  |

**Table 10-4** CBR events that trigger alarms

| Event Source | Event Name                   | Alarm Severity | Description             | Solution                                               | Impact            |
|--------------|------------------------------|----------------|-------------------------|--------------------------------------------------------|-------------------|
| CBR          | Failed to create the backup. | Critical       | Backup creation failed. | Manually create a backup or contact the administrator. | Data may be lost. |

| Event Source | Event Name                                     | Alarm Severity | Description                                    | Solution                                                                | Impact                    |
|--------------|------------------------------------------------|----------------|------------------------------------------------|-------------------------------------------------------------------------|---------------------------|
|              | Failed to restore the resource using a backup. | Critical       | Resource restoration using a backup failed.    | Restore the resource using another backup or contact the administrator. | Data may be lost.         |
|              | Failed to delete the backup.                   | Critical       | Backup deletion failed.                        | Try again later or contact the administrator.                           | Charging may be abnormal. |
|              | Failed to delete the vault.                    | Critical       | Vault deletion failed.                         | Try again later or contact the administrator.                           | Charging may be abnormal. |
|              | Replication failure                            | Critical       | Backup replication failed.                     | Try again later or contact the administrator.                           | Data may be lost.         |
|              | The backup is created successfully.            | Major          | Backup created.                                | None                                                                    | None                      |
|              | Resource restoration using a backup succeeded. | Major          | Resource restoration using a backup succeeded. | Check that data is successfully restored.                               | None                      |
|              | The backup is deleted successfully.            | Major          | Backup deleted.                                | None                                                                    | None                      |

| Event Source | Event Name                         | Alarm Severity | Description        | Solution | Impact |
|--------------|------------------------------------|----------------|--------------------|----------|--------|
|              | The vault is deleted successfully. | Major          | Vault deleted.     | None     | None   |
|              | Replication success                | Major          | Backup replicated. | None     | None   |

 **NOTE**

You can change the alarm severity as needed.

- c. Configure alarm notifications.

**Table 10-5** 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.<br>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.<br>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.<br>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*.

# 11 Quotas


---

## What Is Quota?

Quotas can limit the number or amount of resources available to users, such as the maximum number of ECSs 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. In the upper right corner of the page, click  .  
The **Service Quota** page is displayed.
3. 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?

The system does not support online quota adjustment. If you need to adjust a quota, contact the operations administrator.

Before contacting the operations administrator, make sure that the following information has been obtained:

- Account name, which can be obtained by performing the following operations:  
Log in to the management console using the cloud account, click the username in the upper right corner, select **My Credentials** from the drop-down list, and obtain the account name on the **My Credentials** page.
- Quota information, which includes service name, quota type, and required quota

# 12 FAQs

---

## 12.1 Concepts

### 12.1.1 What Are Full Backup and Incremental Backup?

#### Description

A full backup backs up all data at a certain time point.

An incremental backup backs up the changed data since the last full or incremental backup.

CBR uses the permanent incremental backup technology. A full backup is performed for a resource in the initial backup and incremental backups in all subsequent backups. If a full backup expires and is deleted, its next incremental backup will be regarded as the resource's full backup.

Suppose that server **X** has backups **A**, **B**, and **C** in time sequence. Backup **A** is a full backup, and backups **B** and **C** are incremental backups. Only changed data blocks are backed up in incremental backups and unchanged data blocks are indexed using pointers, so each incremental backup can be regarded as a virtual full backup.

If backup **A** is deleted, data blocks in backup **A** indexed by subsequent backups will not be deleted. Only data blocks that are exclusive to backup **A** are deleted. So, backups **B** and **C** can still be used to restore data. Or if backups **A** and **B** are deleted, backup **C** can also be used to restore data independently. There is no obvious difference between their restoration speeds.

#### Differences

- Backup duration: A full backup backs up the entire resource data which is usually larger than an incremental backup, so full backup take a longer time.
- Restoration duration: Both full backups and incremental backups can be restored. There is no obvious difference between their restoration speeds.
- Reliability: The latest incremental backup depends on the last full backup and intermediate incremental backups. If any backup data block is damaged,

subsequent backups may be affected, which will reduce the backup reliability. All full backup data is independent and does not depend on previous backups. So full backups are more reliable.

You are advised to configure periodic full backup (for example, once every 30 days) and daily incremental backup to reduce the interval of full backup on which incremental backup depends and improve the reliability of backups.

 **NOTE**

In extreme cases, the size of a backup is the same as the disk size. The used capacity in a full backup and the changed capacity in an incremental backup are calculated based on the data block change in a disk rather than the file change in the operating system. The size of a full backup cannot be evaluated based on the file capacity in the operating system, and the size of an incremental backup cannot be evaluated based on the file size change.

## 12.1.2 What Are the Differences Between Backup and Disaster Recovery?

The following table lists the main differences between backup and disaster recovery (DR).

**Table 12-1** Differences between backup and DR

| Item     | Backup                                                                                                                                                           | DR                                                                                                                                                                                                                                                                                                                                        |
|----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Purpose  | To prevent data loss. It adopts the snapshot or backup techniques to generate data backups that can be used to restore data when data loss or corruption occurs. | To ensure service continuity. It takes the replication techniques (such as application-layer replication, host-based replication at the I/O layer, and storage-layer replication) to construct standby service hosts and data in a remote center, so that the remote center can take over services whenever the primary center is faulty. |
| Scenario | It offers protection against virus attacks, accidental deletions, software and hardware faults.                                                                  | It enables failover upon software and hardware faults, as well as natural disasters, such as tsunami, fires, and earthquakes, to fast recover services. When the source AZ recovers, you can easily fail back to the source AZ.                                                                                                           |
| Cost     | The cost is 1 to 2% of the production system's cost.                                                                                                             | The cost is 20 to 100% of the production system's, varying with the RPO/RTO requirements. For active-active DR, the service system deployed in the standby center is required to be the same as that in the active system. In this case, the cost on infrastructure doubles.                                                              |

 **NOTE**

Recovery Point Objective (RPO) specifies the maximum acceptable period in which data can be lost.

Recovery Time Objective (RTO) specifies the maximum acceptable amount of time for restoring the entire system after a disaster occurs.

### 12.1.3 What Are the Differences Between Backups and Snapshots?

Both backups and snapshots provide data redundancy for disks to improve data reliability. [Table 12-2](#) lists the differences between them.

**Table 12-2** Differences between backups and snapshots

| Item     | Storage Solution                                                                                                                                                                                                                                          | Data Synchronization                                                                                                                                                                                                                                                                                           | Service Recovery                                                                                                  |
|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|
| Backup   | Backup data is stored in OBS, instead of disks. This ensures data restoration upon disk data loss or corruption.                                                                                                                                          | A backup is the data copy of a disk at a given point in time. CBR supports automatic backup by configuring backup policies. Deleting a disk will not clear its backups.                                                                                                                                        | You can restore backups to their original disks or create new disks from the backups.                             |
| Snapshot | <p>Snapshot data is stored with disk data.</p> <p><b>NOTE</b><br/>Creating a backup requires a certain amount of time because data needs to be transferred. Therefore, creating or rolling back a snapshot consumes less time than creating a backup.</p> | A snapshot is the state of a disk at a specific point in time. If a disk is deleted, all the snapshots created for this disk will also be deleted. If you have reinstalled or changed the server OS, snapshots of the system disk are automatically deleted. Snapshots of the data disks can be used as usual. | You can use a snapshot to roll back its original disk or create a disk for data restoration and service recovery. |



## 12.1.4 What Are the Differences Between Cloud Server Backup and Cloud Disk Backup?

**Table 12-3** describes the differences between cloud server backup and cloud disk backup.

**Table 12-3** Differences between cloud server backup and cloud disk backup

| Item                                  | Cloud Server Backup                                                              | Cloud Disk Backup                                                                                       |
|---------------------------------------|----------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------|
| Resources to be backed up or restored | All disks (system and data disks) on a server                                    | One or more specified disks (system or data disks)                                                      |
| Recommended scenario                  | An entire cloud server needs to be protected.                                    | Only data disks need to be backed up, because the system disk does not contain users' application data. |
| Advantages                            | All disks on a server are backed up at the same time, ensuring data consistency. | Backup cost is reduced without compromising data security.                                              |

## 12.2 Backup

### 12.2.1 Do I Need to Stop the Server Before Performing a Backup?

No. You can back up servers that are in use. When a server is running, data is written into disks on the server, and some newly generated data is cached in the server memory. During a backup task, data in the memory will not be automatically written into disks, so the disk data and their backups may be inconsistent.

To ensure data integrity, you are advised to perform the backup during off-peak hours when no data is written to the disks. For applications that require strict consistency, such as databases and email systems, you are advised to enable application-consistent backup.

### 12.2.2 Can I Back Up a Server Deployed with Databases?

Yes. CBR provides application-consistent backup. For details about the function compatibility, see **Table 12-4**. For applications or databases with which the application-consistent function is incompatible, you are advised to suspend all data write operations before performing backup. If write operations cannot be suspended, you can stop the application systems or the server for offline backup. If you do not perform the preceding operations before backup, status of the server after restoration will be similar to restart upon an unexpected power failure. In this case, log rollback will be performed on databases to keep data consistent.

**Table 12-4** 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 and 12 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                       |

### 12.2.3 How Can I Distinguish Automatic Backups From Manual Backups?

They can be distinguished by name prefix:

- Automatic backups: **autobk\_**xxxx
- Manual backups: **manualbk\_**xxxx or custom names

### 12.2.4 Can I Choose to Back Up Only Some Partitions of a Disk?

No. The minimum backup granularity supported by CBR is disks.

### 12.2.5 Does CBR Support Cross-Region Backup?

No. CBR supports only backup and restoration within a region but not across regions.

### 12.2.6 Will the Server Performance Be Affected If I Delete Its Backups?

No. Backups are not stored on a server. Therefore, deleting its backups has no impact on the server performance.

## 12.2.7 Can I Use Its Backup for Restoration After a Resource Is Deleted?

Yes. Resources and backups are not stored together. If a resource is deleted, its backup still stays in your CBR vault. You can use the backup to restore the resource to a backup point in time.

## 12.2.8 How Many Backups Can I Create for a Resource?

You can create as many backups for a resource as needed.

## 12.2.9 Can I Stop an Ongoing Backup Task?

No. An ongoing backup task cannot be stopped.

# 12.3 Capacity

## 12.3.1 Why Is My Backup Size Larger Than My Disk Size?

### Symptoms

- There is no difference or an increase in size between the original backup and a backup generated after a file is deleted.
- The ECS backup size is larger than the used disk space obtained from the file system.

### Possible Causes

Possible causes are as follows:

- The backup mechanism itself causes this problem. The cloud server backups, and cloud disk backups created using CBR are all block-level backups. Different from file-level backups, block-level backups are performed by sector (512 bytes) each time.
- The metadata of the file systems on the disk occupies disk space.
- To reduce performance overhead, the file system adds a delete marker for the deleted file, but does not erase the data that has been written to the sector, and the metadata on the sector still exists. Block-level backups cannot detect whether data on a sector is deleted or not, but only determine whether a backup needs to be performed by checking whether all data blocks are zero blocks.
- CBR determines whether data in each sector changes by comparing two snapshots. Data changes include data addition, modification, and deletion. Backup is not performed if there are no data changes. If there are data changes, CBR further checks whether data blocks in the sector are all zero blocks. If so, backup is also not performed. Backups are performed only when there are non-zero blocks. If the data is deleted but metadata in the sector is not, the data block is also recognized as a non-zero block, and backups will be performed.

## 12.4 Restoration

### 12.4.1 Do I Need to Stop the Server Before Restoring Data Using Backups?

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.

### 12.4.2 Can I Use a System Disk Backup to Recover an ECS?

Yes. However, before the recovery, you need to detach the system disk to be recovered from the ECS.

You can also use a backup of the system disk to create new disks. However, newly created disks cannot be used as system disks.

### 12.4.3 Do I Need to Stop the Server Before Restoring Data Using Disk Backups?

Yes. Before restoring the disk data using a disk backup, you must 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.

### 12.4.4 Can a Server Be Restored Using Its Backups After It Is Changed?

Yes. If a server has been backed up and then changed (adding, deleting, or expanding disks), its backups can still be used to restore data. You are advised to back up data again after the change.

If you have added a disk after a backup and then use the backup to restore data, data on the new disk will not change.

If you have deleted a disk after a backup and then use the backup to restore data, data on the deleted disk cannot be restored.

### 12.4.5 Can a Disk Be Restored Using Its Backups After Its Capacity Is Expanded?

Yes. After restoration, the capacity of the expanded disk goes back to the original capacity before expansion. If you want to use the capacity added to the disk, you need to attach the restored disk to a server, log in to the server, and then manually modify the file system configuration. For detailed operations, see sections about post-expansion operations on disks in the *Elastic Volume Service User Guide*.

## 12.4.6 What Can I Do if the Password Becomes a Random One After I Use a Backup to Restore a Server or Use an Image to Create a Server?

For details about how to reset the password, see section "Passwords" in the *Elastic Cloud Server User Guide*.

## 12.4.7 What Changes Will Be Made to the Original Backup When I Use the Backup to Restore a Server?

- For Linux:
  - Check whether drivers related to the PV driver exist. If yes, delete them.
  - Modify the **grub** and **syslinux** configuration files to add the OS kernel boot parameters and change the disk partition name to **UUID=UUID of the disk partition**.
  - Change the names of the disk partitions in the **/etc/fstab** file to **UUID=UUID of the disk partition**.
  - Delete services of VMware tools.
  - Linux OSs automatically copy the built-in VirtIO driver to **initrd** or **initramfs**.
- For Windows:
  - Inject the VirtIO driver offline to solve the problem that the system cannot start when UVP VMTools is not installed.

## 12.4.8 Can I Stop an Ongoing Restoration Task?

No. An ongoing restoration task cannot be stopped.

## 12.5 Policies

### 12.5.1 How Do I Configure Automatic Backup for a Server or Disk?

1. Go to the Cloud Backup and Recovery console and create a backup vault. You are advised to set the vault capacity to at least twice the total capacity of the resources you want to back up.
2. Associate resources with the vault during or after the creation.
3. Go to the **Policies** page to configure a backup policy. You are advised to set the backup execution time at off-peak hours, for example, early in the morning. Set the backup retention rule as needed. If your vault capacity is small, set a small value for the number of backups to be kept or the days that backups will be retained. Retention rule does not apply to manual backups.
4. Apply the policy you defined to the vault. The system then will back up the resources that are associated with the vault at the specified time and retains the backups based on the retention rule.

## 12.5.2 Why the New Retention Rule I Changed Is Not Applied?

The scenarios of a retention rule change are as follows:

### Rule Type Unchanged, with Only a New Backup Quantity Configured

The new rule will be applied to the backups generated based on the old policy. After a backup is generated, regardless of an automatic or a manual one, the system verifies and uses the latest retention rule.

Example: A user has a vault associated with a disk. At 10:00 a.m. on Monday, the user applies a backup policy to the vault, based on which a backup task will be executed at 02:00 a.m. every day and three most recent backups will be kept. At 10:00 a.m. on Thursday, three backups are kept. Then the user changes the number of backups kept from three to one, and the new policy will be applied immediately. If the user then perform manual backups or wait until the system automatically create a backup at 02:00 a.m. on Friday, the system will verify and use the latest retention rule after the backup task is complete. In this case, only one most recent backup will be kept. Manual backups are not affected by policies, so they will not be deleted.

### Rule Type Changed from Backup Quantity to Time Period/Permanent

The new rule will be applied only to the new backups. Backups generated based on the old policy will not be automatically deleted.

Example: A user has a vault associated with a disk. At 10:00 a.m. on Monday, the user applies a backup policy to the vault, based on which a backup task will be executed at 02:00 a.m. every day and three most recent backups will be kept. At 10:00 a.m. on Thursday, three backups are kept. Then the user changes the retention rule type from backup quantity to time period and sets to retain the backups from the last one month. The new policy will be applied immediately. If the user then perform manual backups or wait until the system automatically create a backup at 02:00 a.m. on Friday, the system will verify and use the latest retention rule after the backup task is complete. The three backups generated based on the old policy will still be kept (the number of backups does not exceed the quantity set in the old retention rule). They will not be automatically deleted and you need manually delete them if needed. Backups generated based on the new policy will be kept based on the new retention rule.

### Rule Type Changed from Time Period to Time Period/Permanent

The new policy will only be applied to the new backups. Backups generated based on the old policy will be kept based on the old policy.

Example: A user has a vault associated with a disk. At 10:00 a.m. on August 5, the user applies a backup policy to the vault, based on which a backup task will be executed at 02:00 a.m. every day and the backups generated from the last one month will be kept. At 10:00 a.m. on August 8, three backups are kept. Then the user changes the backup retention time from the last one month to the last three months. At 02:00 a.m. on September 6, the backup generated on August 6 based on the old policy will be deleted. The backup generated on August 9 will be deleted two months later based on the new policy.

## Rule Type Changed from Time Period to Backup Quantity

Both the old and new policies will be applied to the backups generated based on the old policy. The union set of the old and new rules will be applied.

### New policy applied to old backups

Example: A user has a vault associated with a disk. At 10:00 a.m. on August 5, the user applies a backup policy to the vault, based on which a backup task will be executed at 02:00 a.m. every day and the backups generated from the last one month will be kept. At 10:00 a.m. on August 8, three backups are kept. Then the user changes the retention rule type from time period to backup quantity and sets to retain the most recent seven backups. At 10:00 a.m. on August 15, the backups generated on August 9, 10, 11, 12, 13, 14, and 15 will be kept. The backups generated on August 6, 7, and 8 have been deleted based on the new policy.

### Old policy applied to old backups

Example: A user has a vault associated with a disk. At 10:00 a.m. on August 5, the user applies a backup policy to the vault, based on which a backup task will be executed at 02:00 a.m. every day and the backups generated from the last three days will be kept. At 10:00 a.m. on August 8, three backups are kept. Then the user changes the retention rule type from time period to backup quantity and sets to retain the most recent seven backups. At 10:00 a.m. on August 10, the backups generated on August 8, 9, and 10 will be kept. The backups generated on August 6 and 7 have been deleted based on the old policy.

## 12.5.3 How Do I Back Up Multiple Resources at a Time?

1. Log in to the CBR console and click **Cloud Server Backups** or **Cloud Disk Backups** on the left navigation pane. On the displayed page, create a backup vault. It is recommended that the capacity of the vault be at least twice the total size of resources to be backed up.
2. Associate resources with the vault during or after the creation.
3. After the resources are associated, choose **More > Perform Backup** in the **Operation** column of the target vault. You can manually back up two or more resources at a time.

Alternatively, you can set a backup policy for the vault. In this way, the system will automatically back up the associated resources at the scheduled time.

## 12.6 Others

### 12.6.1 Is There a Quota for CBR Vaults?

There are no quotas on CBR vaults. You can create as many vaults as needed.

### 12.6.2 Can I Merge My Vaults?

No. Vaults cannot be merged.

# 13 Troubleshooting Cases

---

## 13.1 Failed to Attach Disks

### Symptom

Failed to attach disks despite following the procedure: Create EVS disks using the same disk backup (XFS file system backup) and attach them to the same server (to which multiple EVS disks with XFS file system backup have been attached). Running the **mount** command to attach disks fails.

### Possible Cause

The superblock of an EVS disk (with XFS file systems) stores a universally unique identifier (UUID) about the file system. If a server has multiple disks (with XFS file systems), multiple UUIDs will exist on the server. Multiple disks may have the same UUID, which can cause the file system mounting to fail.

### Troubleshooting Methods

When attaching an EVS disk, use parameters without UUID control or reallocate a new UUID to ensure that each UUID is unique.

### Solution

**Step 1** Log in to the server to which EVS disks failed to be attached.

**Step 2** Resolve the problem in either of the following ways:

- Use a parameter without UUID when attaching an EVS disk: Run **mount -o nouuid /dev/*Device name* /*Mount path***, for example:  
**mount -o nouuid /dev/sda6 /mnt/aa**
- Reallocate a new UUID: Run **xfs\_admin -U generate /dev/*Device name***.



 **NOTE**

Because setting a parameter without UUID requires you to execute the command every time, you are advised to reallocate a new UUID.

----End

## 13.2 Data Disks Are Not Displayed After a Windows Server Is Restored

### Symptom

When a Windows server is restored, the data disks are not displayed.

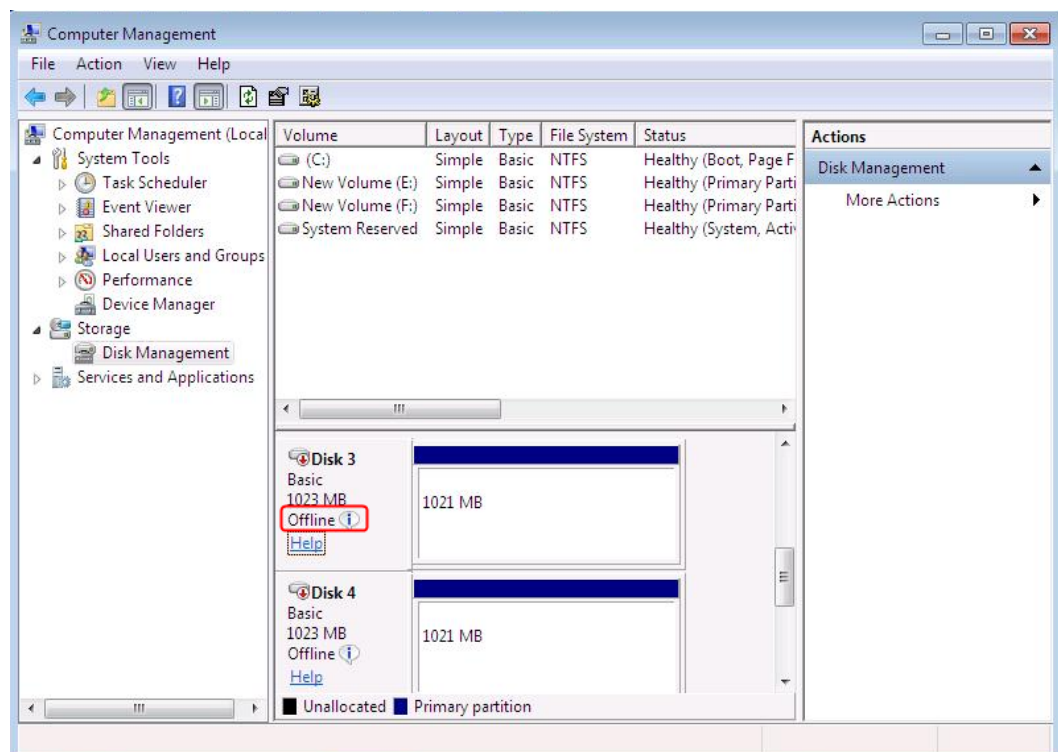
### Possible Cause

Due to the limitations of Windows operating systems, data disks are in offline mode after a server is restored.

### Solution

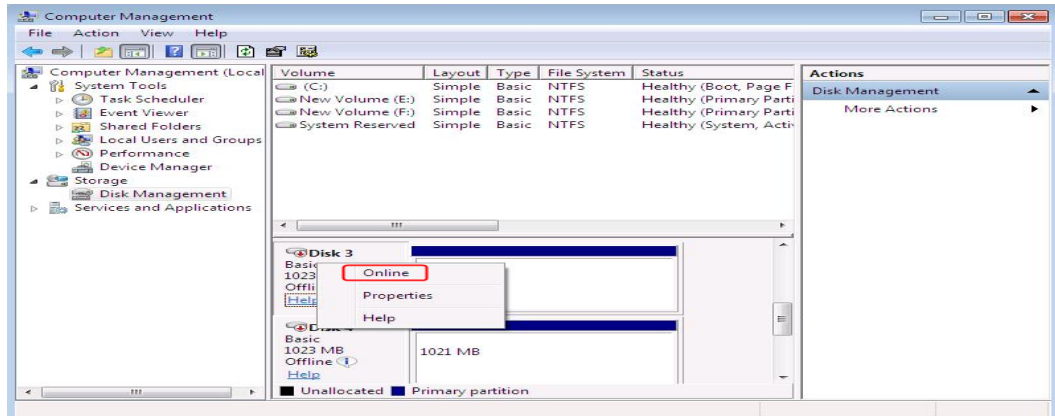
- Step 1** On the Windows desktop, right-click the **My Computer** icon.
- Step 2** Choose **Manage** from the shortcut menu. The **Computer Management** page is displayed.
- Step 3** In the navigation tree, choose **Storage > Disk Management**.  
Data disks are in the offline state, as shown in [Figure 13-1](#).

**Figure 13-1** Data disks in the offline state



**Step 4** Right-click a data disk in the offline state and choose **Online**, as shown in **Figure 13-2**.

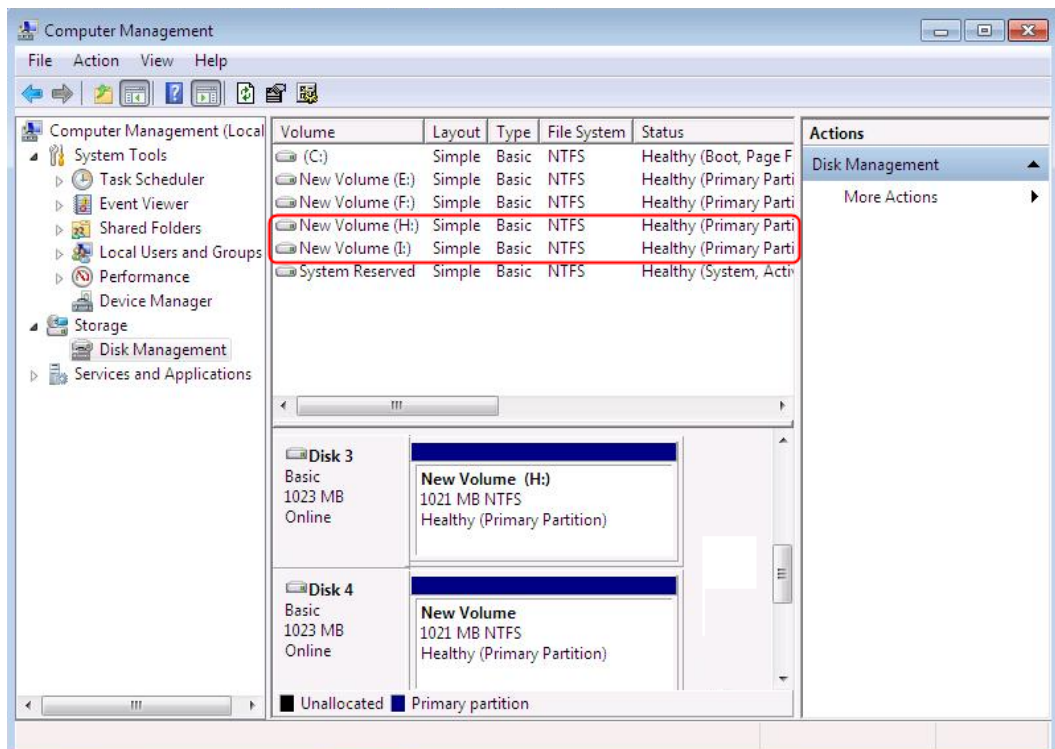
**Figure 13-2** Setting a data disk to be online



After the data disk status changes to **Online**, the data disk will be displayed in the disk list, as shown in **Figure 13-3**.

In addition, the data disk will be properly displayed on the server.

**Figure 13-3** Viewing online data disks



----End

## 13.3 Failed to Cancel Backup Sharing

### Symptom

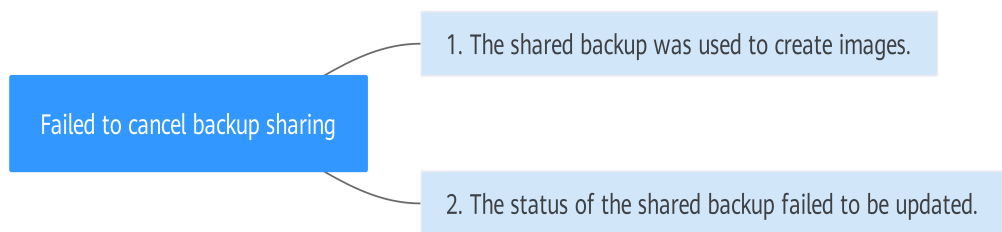
When you cancel the backup sharing, the system prompts a message indicating that the canceling failed.

### Troubleshooting

Possible causes are listed here in order of their probability.

If the fault persists after you have ruled out one cause, move on to the next one.

**Figure 13-4** Troubleshooting



**Table 13-1** Troubleshooting

| Possible Cause                                        | Solution                                                                                                                                            |
|-------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| The shared backup was used to create images.          | Delete the images and then delete the shared backup. For details, see section "Deleting Images" in the <i>Image Management Service User Guide</i> . |
| The status of the shared backup failed to be updated. | Try again or contact technical support.                                                                                                             |

## 13.4 Failed to Download or Install the Agent Required by Application-Consistent

### Symptom

The system displays a message indicating that the script cannot be downloaded or the Agent fails to be installed in Linux mode 2.

### Possible Causes

- Cause 1: The DNS cannot resolve the OBS domain name.

- Cause 2: The OpenSSL version of the target server is too early.

## Solution for Cause 1

Cause 1: The DNS cannot resolve the domain name.

You need to manually change the DNS server address. Obtain the IP address from technical support. If the problem persists, try later or use the Linux mode 1 to install it.

### Procedure (Linux)

- Step 1** Log in to the server as the **root** user.
- Step 2** Run the **vi /etc/resolv.conf** command to edit the **/etc/resolv.conf** file. Add the DNS server IP address above the existing name server information, as shown in [Figure 13-5](#).

Figure 13-5 Configuring DNS

```

; generated by /sbin/dhclient-script
search openstacklocal
nameserver 114.204.114.114
nameserver 114.204.115.115

```

The format is as follows:

```
nameserver DNS server IP address
```

- Step 3** Press **Esc**, input **:wq**, and press **Enter** to save the changes and exit the vi editor.
- Step 4** Run the following command to check whether the IP address is added. If yes, the operation is complete.

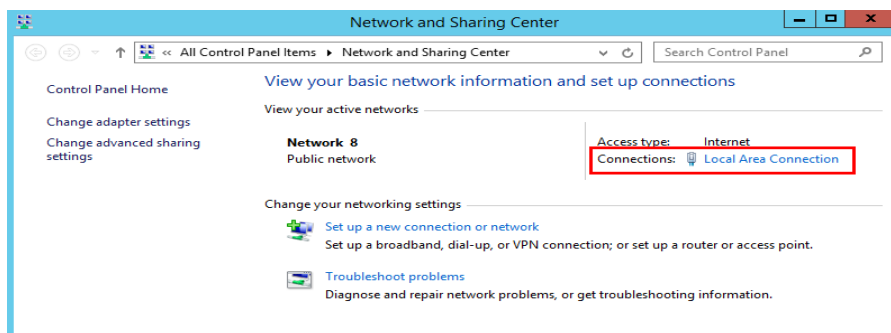
```
cat /etc/resolv.conf
```

----End

### Procedure (Windows)

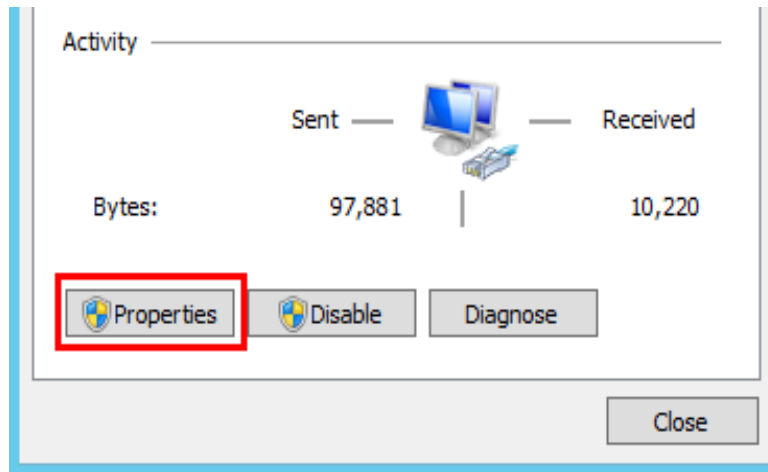
- Step 1** Go to the ECS console and log in to the ECS running Windows Server 2012.
- Step 2** Click **This PC** in the lower left corner.
- Step 3** On the page that is displayed, right-click **Network** and choose **Properties** from the drop-down list. The **Network and Sharing Center** page is displayed, as shown in [Figure 13-6](#). Click **Local Area Connection**.

Figure 13-6 Page for network and sharing center



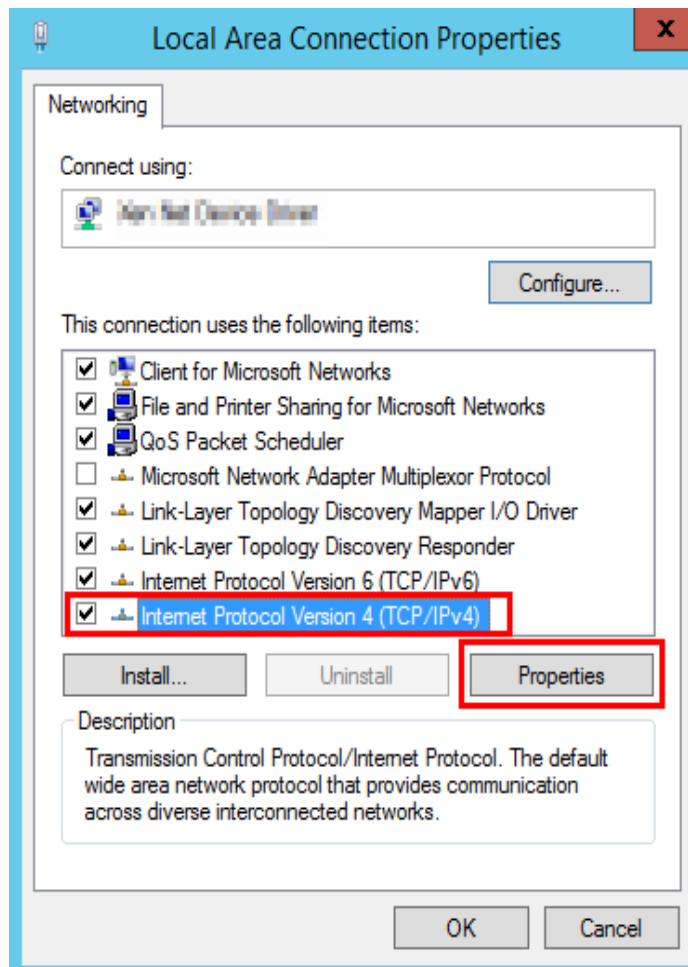
**Step 4** In the **Activity** area, select **Properties**. See **Figure 13-7**.

**Figure 13-7** Local area connection



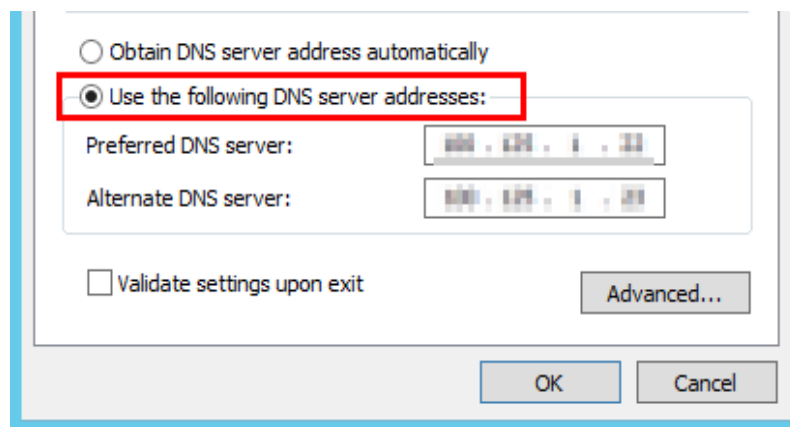
**Step 5** In the **Local Area Connection Properties** dialog box that is displayed, select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**. See **Figure 13-8**.

**Figure 13-8** Local area connection properties



- Step 6** In the dialog box that is displayed, select **Use the following DNS server addresses:** and configure DNS, as shown in **Figure 13-9**. You need to manually change the DNS server address. Obtain the IP address from technical support. Then click **OK**.

**Figure 13-9** Configuring DNS



----End

## Solution for Cause 2

Cause 2: The OpenSSL version of the target server is too early.

- Step 1** Use a remote management tool (such as PuTTY or Xshell) to connect to your ECS through the elastic IP address.
- Step 2** Select the Agent version based on your needs, copy the command of installation mode 2 to the server, and change **https** to **http** in wget. Run the command as the root user.

----End

## 13.5 A Server Created Using an Image Enters Maintenance Mode After Login

### Symptom

A server is created using the image of a cloud server backup. However, upon login to the server, the server enters maintenance mode and cannot be used.

### Possible Cause

After the server creation, the configuration parameters contained in the **/etc/fstab** file in the system disk of the new server are that of the backup source server, causing the UUID information to be inconsistent with the new data disks. As a result, the ECS encounters an error when uploading **/etc/fstab** during the bootup and enters maintenance mode.

## Solution

The following uses CentOS as an example.

- Step 1** After creating an ECS using an image, log in to the ECS console, click **Remote Login** in the row of the ECS.
- Step 2** On the maintenance mode page that is displayed, access the system as prompted.

**Figure 13-10** Maintenance mode of the system

```
CentOS Linux 7 (Core)
Kernel 3.10.0-1062.12.1.el7.x86_64 on an x86_64

Hint: Num Lock on

cli-demo login: root
Password:
Last login: Tue Feb 7 16:48:33 on tty1

      Welcome to Huawei Cloud Service

[root@cli-demo ~]#
```

- Step 3** Run the `cat /etc/fstab` command to check the disk attachment information.

**Figure 13-11** Data disk UUIDs

```
WARNING! The remote SSH server rejected X11 forwarding request.
Last login: Tue Feb 7 16:35:37 2023

      Welcome to ██████ Cloud Service

[root@cli-demo ~]#
[root@cli-demo ~]# cat /etc/fstab

#
# /etc/fstab
# Created by anaconda on Mon Apr 27 13:51:12 2020
#
# Accessible filesystems, by reference, are maintained under '/dev/disk'
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info
#
UUID=207b19eb-8170-4983-acb5-9098af381e72 /          ext4    defaults    1 1
UUID=08e5c568-86ca-40ce-8145-66b3ea53076a /tmp/test  ext4    defaults    1 0
[root@cli-demo ~]#
```

- Step 4** Run the `vi /etc/fstab` command to open the file, press `i` to enter the editing mode, and delete the attachment information of all data disks. Then, press `Esc` to exit the editing mode and run `:wq!` to save the change and exit.

**Figure 13-12** `/etc/fstab` after being updated

```
[root@cli-demo ~]# vi /etc/fstab
[root@cli-demo ~]# cat /etc/fstab

#
# /etc/fstab
# Created by anaconda on Mon Apr 27 13:51:12 2020
#
# Accessible filesystems, by reference, are maintained under '/dev/disk'
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info
#
UUID=207b19eb-8170-4983-acb5-9098af381e72 /          ext4    defaults    1 1

[root@cli-demo ~]#
```

**Step 5** Run the **reboot** command to restart the system.

**Figure 13-13** Normal bootup page

```
CentOS Linux 7 (Core)
Kernel 3.10.0-1062.12.1.el7.x86_64 on an x86_64

cli-demo login:
```

**Step 6** After entering the system, attach the data disks manually.

**Figure 13-14** Attaching the data disks manually

```
[root@cli-demo ~]#
[root@cli-demo ~]# cat /etc/fstab

#
# /etc/fstab
# Created by anaconda on Mon Apr 27 13:51:12 2020
#
# Accessible filesystems, by reference, are maintained under '/dev/disk'
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info
#
UUID=207b19eb-8170-4983-acb5-9098af381e72 / ext4 defaults 1 1

[root@cli-demo ~]#
[root@cli-demo ~]# mount /dev/vdb /tmp/test
[root@cli-demo ~]#
[root@cli-demo ~]#
```

**Step 7** Run the **blkid** command to obtain the UUID information of the data disks.

**Figure 13-15** Obtaining UUIDs of data disks

```
[root@cli-demo ~]# blkid
/dev/vda1: UUID="207b19eb-8170-4983-acb5-9098af381e72" TYPE="ext4"
/dev/vdb: UUID="08e5c568-86ca-40ce-8145-66b3ea53076a" TYPE="ext4"
[root@cli-demo ~]#
```

**Step 8** Run the **vi /etc/fstab** command to open the file, press **i** to enter the editing mode, and add the attachment information of all data disks. Then, press **Esc** to exit the editing mode and run **:wq!** to save the change and exit.

**Figure 13-16** Adding attachment information of data disks

```
[root@cli-demo ~]# blkid
/dev/vda1: UUID="207b19eb-8170-4983-acb5-9098af381e72" TYPE="ext4"
/dev/vdb: UUID="08e5c568-86ca-40ce-8145-66b3ea53076a" TYPE="ext4"
[root@cli-demo ~]#
[root@cli-demo ~]#
[root@cli-demo ~]# vi /etc/fstab
[root@cli-demo ~]# vi /etc/fstab
[root@cli-demo ~]# cat /etc/fstab

#
# /etc/fstab
# Created by anaconda on Mon Apr 27 13:51:12 2020
#
# Accessible filesystems, by reference, are maintained under '/dev/disk'
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info
#
UUID=207b19eb-8170-4983-acb5-9098af381e72 / ext4 defaults 1 1
UUID=08e5c568-86ca-40ce-8145-66b3ea53076a /tmp/test ext4 defaults 1 0
[root@cli-demo ~]#
```



After the information is added, the system will automatically attach the data disks on restart.

**----End**

# 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**.



```
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

## Procedure (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.

### Procedure (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

## Procedure (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.

### Procedure (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
```

## Procedure (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\nnginx\conf` directory.

**Step 5** Delete the `bcmagentca.crt` certificate file.

**Step 6** Copy the new CA certificate file into the `Installation path\nnginx\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
```



## A.2 Change History

| Released On | Description                               |
|-------------|-------------------------------------------|
| 2024-04-15  | This issue is the first official release. |