

Cloud Backup and Recovery

User Guide

Date **2023-05-08**

Contents

1 Service Overview.....	1
1.1 What Is CBR?.....	1
1.2 Advantages.....	5
1.3 Application Scenarios.....	5
1.4 Functions.....	6
1.5 Permissions.....	8
1.6 Constraints.....	11
1.7 CBR and Other Services.....	12
1.8 Basic Concepts.....	12
1.8.1 CBR Concepts.....	12
1.8.2 Project and Enterprise Project.....	14
1.8.3 Region and AZ.....	14
2 Getting Started.....	16
2.1 Step 1: Create a Vault.....	16
2.1.1 Creating a Server Backup Vault.....	16
2.1.2 Creating a Disk Backup Vault.....	18
2.1.3 Creating an SFS Turbo Backup Vault.....	19
2.2 Step 2: Associate a Resource with the Vault.....	21
2.3 Step 3: Create a Backup.....	22
2.3.1 Creating a Cloud Server Backup.....	22
2.3.2 Creating a Cloud Disk Backup.....	24
2.3.3 Creating an SFS Turbo Backup.....	27
3 Permissions Management.....	30
3.1 Creating a User and Granting CBR Permissions.....	30
3.2 Creating a Custom Policy.....	31
4 Vault Management.....	34
4.1 Querying a Vault.....	34
4.2 Deleting a Vault.....	36
4.3 Dissociating a Resource.....	37
4.4 Migrating a Resource.....	38
4.5 Expanding Vault Capacity.....	39
5 Backup Management.....	41

5.1 Viewing a Backup.....	41
5.2 Sharing a Backup.....	43
5.3 Deleting a Backup.....	46
5.4 Using a Backup to Create an Image.....	47
5.5 Using a Backup to Create a Disk.....	49
5.6 Using a Backup to Create a File System.....	50
6 Policy Management.....	52
6.1 Creating a Backup Policy.....	52
6.2 Modifying a Policy.....	57
6.3 Deleting a Policy.....	60
6.4 Applying a Policy to a Vault.....	60
6.5 Removing a Policy from a Vault.....	61
7 Restoring Data.....	63
7.1 Restoring from a Cloud Server Backup.....	63
7.2 Restoring from a Cloud Disk Backup.....	65
7.3 Restoring from an SFS Turbo Backup.....	67
8 Managing Tasks.....	69
9 Monitoring.....	70
9.1 CBR Metrics.....	70
10 Auditing.....	72
11 Quotas.....	74
12 FAQs.....	76
12.1 Concepts.....	76
12.1.1 What Are Full Backup and Incremental Backup?.....	76
12.1.2 What Are the Differences Between Backup and Disaster Recovery?.....	77
12.1.3 What Are the Differences Between Backups and Snapshots?.....	78
12.1.4 Why Is My Backup Size Larger Than My Disk Size?.....	78
12.1.5 What Are the Differences Between Backups and Images?.....	79
12.1.6 What Are the Differences Between Cloud Server Backup and Cloud Disk Backup?.....	81
12.1.7 Why Does the Used Capacity of a Vault Change Only Slightly After I Deleted Unwanted Backups?	81
12.2 Backup.....	82
12.2.1 Do I Need to Stop the Server Before Performing a Backup?.....	82
12.2.2 Can I Back Up a Server Deployed with Databases?.....	82
12.2.3 How Can I Distinguish Automatic Backups From Manual Backups?.....	83
12.2.4 Can I Choose to Back Up Only Some Partitions of a Disk?.....	83
12.2.5 Does CBR Support Cross-Region Backup?.....	83
12.2.6 Can I Back Up Two Disks to One Target Disk?.....	83
12.2.7 How Do I Replicate a Disk to the Same AZ in a Region as the Source Disk?.....	83
12.2.8 Will the Server Performance Be Affected If I Delete Its Backups?.....	83

12.2.9 Can I Use Its Backup for Restoration After a Resource Is Deleted?.....	83
12.2.10 How Many Backups Can I Create for a Resource?.....	83
12.2.11 Can I Stop an Ongoing Backup Task?.....	83
12.2.12 How Do I Reduce the Vault Space Occupied by Backups?.....	84
12.2.13 How Do I View the Size of Each Backup?.....	84
12.2.14 How Do I View My Backup Data?.....	84
12.2.15 How Long Will My Backups Be Kept?.....	85
12.3 Restoration.....	85
12.3.1 Do I Need to Stop the Server Before Restoring Data Using Backups?.....	85
12.3.2 Can I Use a System Disk Backup to Recover an ECS?.....	85
12.3.3 Do I Need to Stop the Server Before Restoring Data Using Disk Backups?.....	85
12.3.4 Can a Server Be Restored Using Its Backups After It Is Changed?.....	86
12.3.5 Can a Disk Be Restored Using Its Backups After Its Capacity Is Expanded?.....	86
12.3.6 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?.....	86
12.3.7 What Changes Will Be Made to the Original Backup When I Use the Backup to Restore a Server?	86
12.3.8 How Do I Restore Data on the Original Server to a New Server?.....	87
12.3.9 How Do I Restore a Data Disk Backup to a System Disk?.....	87
12.3.10 Can I Use CBR to Restore Data to Any Point When the Data Was Backed Up?.....	87
12.3.11 Can I Stop an Ongoing Restoration Task?.....	88
12.4 Policies.....	88
12.4.1 How Do I Configure Automatic Backup for a Server or Disk?.....	89
12.4.2 Why the New Retention Rule I Changed Is Not Applied?.....	89
12.4.3 How Do I Back Up Multiple Resources at a Time?.....	90
12.4.4 How Do I Retain My Backups Permanently?.....	91
12.4.5 How Can I Cancel Auto Backup?.....	91
12.4.6 How Can I Have the System Automatically Delete Backups That I No Longer Need?.....	91
12.4.7 Why Aren't My Backups Deleted Based on the Retention Rule?.....	91
12.5 Optimization.....	91
12.5.1 What Are Common Problems During Cloud-Init Installation?.....	92
12.5.2 What Can I Do If Injecting the Key or Password Using Cloud-Init Fails After NetworkManager Is Installed?.....	96
12.5.3 What Can Cloud-Init Do?.....	96
12.6 Others.....	96
12.6.1 Is There a Quota for CBR Vaults?.....	96
12.6.2 Can I Merge My Vaults?.....	97
12.6.3 How Do I Delete a Backup That Has Been Used to Create an Image While Retaining the Image?	97
12.6.4 What Can I Do If the Vault Capacity Is Not Enough?.....	97
12.6.5 Will Backup Continue If the Usage of a Vault Reaches the Upper Limit?.....	97
12.6.6 Can I Export Disk Backup Data to Another Server?.....	97
12.6.7 Why Do I Need a Vault to Accept the Image Shared to Me?.....	97

12.6.8 Can I Download Backup Data to a Local PC?..... 98

12.6.9 How Do I Copy Disk Data to Another Account?..... 98

13 Troubleshooting Cases..... 99

13.1 Failed to Attach Disks..... 99

13.2 Data Disks Are Not Displayed After a Windows Server Is Restored..... 100

13.3 A Server Created Using an Image Enters Maintenance Mode After Login..... 102

A Appendix..... 106

A.1 Agent Security Maintenance..... 106

A.1.1 Changing the Password of User rdadmin..... 106

A.1.2 Changing the Password of the Account for Reporting Alarms (SNMP v3)..... 107

A.1.3 Replacing the Server Certificate..... 109

A.1.4 Replacing CA Certificates..... 111

A.2 Change History..... 113

1 Service Overview

- [1.1 What Is CBR?](#)
- [1.2 Advantages](#)
- [1.3 Application Scenarios](#)
- [1.4 Functions](#)
- [1.5 Permissions](#)
- [1.6 Constraints](#)
- [1.7 CBR and Other Services](#)
- [1.8 Basic Concepts](#)

1.1 What Is CBR?

Overview

Cloud Backup and Recovery (CBR) enables you to easily back up Elastic Cloud Servers (ECSs), Bare Metal Servers (BMSs), Elastic Volume Service (EVS) disks, and SFS Turbo file systems. 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 and BMSs. Backups of non-database servers are non-database

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

- SFS Turbo backup: backs up data of SFS Turbo file systems.

Vault

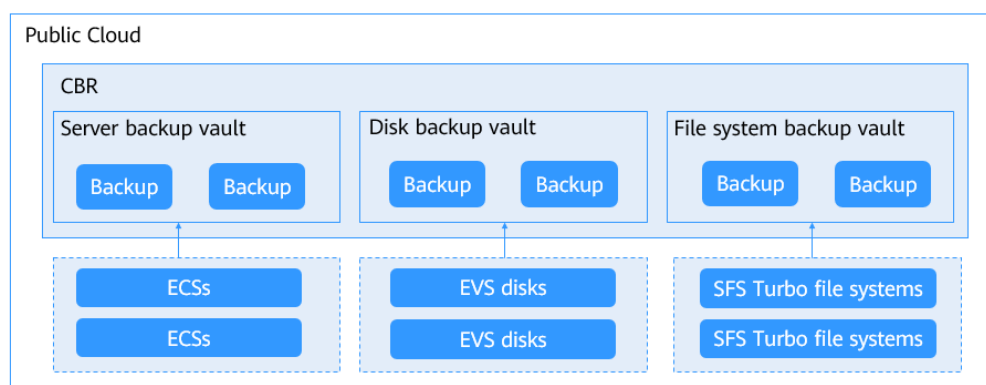
CBR stores backups in vaults. Before creating a backup, you need to create at least one vault and associate the resources you want to back up with the vaults. Then the resources can be backed up to the associated vaults.

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	SFS Turbo Backup
What to back up	All disks (system and data disks) on a server	One or more specific disks (system or data disks)	SFS Turbo file systems
When to use	You want to back up entire cloud servers.	You want to back up only data disks.	You want to back up entire SFS Turbo file systems.

Item	Cloud Server Backup	Cloud Disk Backup	SFS Turbo Backup
Advantages	All disks on a server are backed up at a time.	Only data of specific disks is backed up, which costs less than backing up an entire server.	File system data and their backups are stored separately, and the backups can be used to create new file systems.

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.

A backup will not be deleted if it is 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.

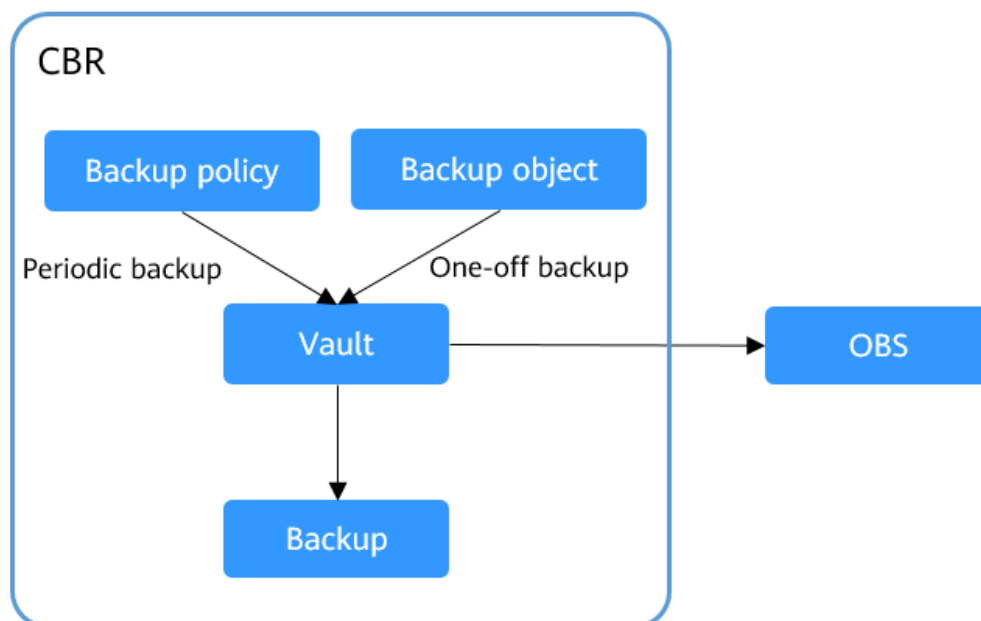
Table 1-2 One-off backup and periodic backup

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 manualbk_ xxxx by default	System-assigned backup name, which is autobk_ xxxx 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.

Item	One-Off Backup	Periodic Backup
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 [Cloud Backup and Recovery API Reference](#).

1.2 Advantages

Reliable

CBR offers crash-consistent backup for multiple disks on a server. The backups protect against human errors, virus attacks, and natural disasters, and ensure your data security and reliability.

Efficient

Incremental forever backups shorten the time required for backup by 95%. With Instant Restore, CBR offers an RPO of as low as 1 hour and an RTO of only several minutes.

NOTE

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

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

Easy to Use

CBR is easier to use than conventional backup systems. You can complete backup in just three steps, and no professional backup skills are required.

Secure

If the disks are encrypted, their backups are also encrypted to ensure data security.

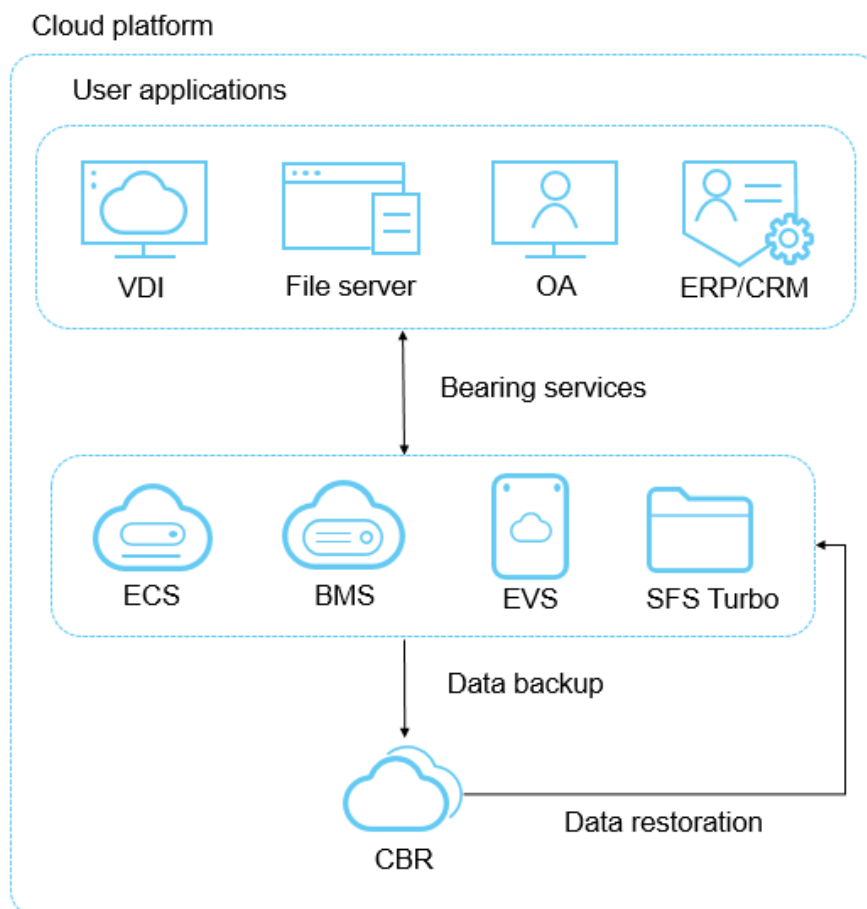
1.3 Application Scenarios

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

Figure 1-3 Data backup and restoration

1.4 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.
	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
	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.
	Disk restoration using backups	When a disk is faulty, or their data is lost, you can use a backup to quickly restore the data.
	Disk creation using backups	You can use a disk backup to create a disk that contains the same data as the backup.
	5.2 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. You can use CBR to back up an entire server to protect their data.
	Backup of specific disks on a server	You can create a single backup for multiple disks on a server to save the vault space.
	Policy-based backup	You can create, modify, or delete a backup policy. A backup policy defines the schedule and retention for automatic backups.
	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.
	Server restoration using backups	When a server is faulty, or their data is lost, you can use a backup to quickly restore the data.
	5.2 Sharing a Backup	You can share a server backup with other accounts to allow them to use the backup to create servers.
	Image creation using server backups	You can create images from ECS backups and then use the images to quickly provision ECSs to restore service.

Category	Function	Description
SFS Turbo backup	Manual SFS Turbo backup	You can back up SFS Turbo file systems and use the backups to create new SFS Turbo file systems.
	Policy-based backup	You can create, modify, or delete a backup policy. A backup policy defines the schedule and retention for automatic backups.
	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.
	File system restoration using backups	When a file system is faulty, or their data is lost, you can use a backup to quickly restore the data.
	File system creation using backups	You can use an SFS Turbo file system backup to create a file system that contains the same data as the backup.

1.5 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 [IAM 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

Operation	CBR FullAccess	CBR BackupsAndVaultsFullAccess	CBR ReadOnlyAccess
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 a vault	Supported	Supported	Not supported
Removing policies from a vault	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 using backups	Supported	Supported	Not supported
Associating vaults	Supported	Supported	Not supported
Batch adding or deleting vault tags	Supported	Supported	Not supported
Adding vault tags	Supported	Supported	Not supported
Editing tags	Supported	Supported	Not supported

1.6 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.
- 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.
- Concurrent data restoration is not supported.
- Auto capacity expansion does not take effect if it is enabled after the vault is full.

Cloud Disk Backup

- Only disks in the **Available** or **In-use** state can be backed up.
- Frozen disks in the retention period cannot 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.
- Frozen servers in the retention period cannot be backed up.
- You can back up specific disks on a server, but such a backup must be restored as a whole. File- or directory-level restoration is not supported.
- Images cannot be created from backups if the amount of resources associated with a server backup vault exceeds the quota.
- Only ECS backups can be used to create images.
- You are advised not to back up a server whose disk size exceeds 4 TB.

SFS Turbo Backup

- Only file systems in the **Available** state can be backed up.
- An SFS Turbo file system backup cannot be used to restore data to the original file system.

1.7 CBR and Other Services

CBR-related Services

Table 1-6 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	2.3.1 Creating a Cloud Server Backup 2.3.2 Creating a Cloud Disk Backup
CBR backs up data of a BMS and uses the backup to restore data for the BMS. The backup and management processes for BMSs and ECSs are the same.	BMS	What Is CBR? Creating a Cloud Server Backup
CBR backs up data of SFS Turbo file systems and uses the backup to create new file systems to restore lost or corrupted data.	SFS	2.3.3 Creating an SFS Turbo Backup
CBR stores backups securely in OBS.	OBS	What Is CBR?
CBR backs up data of EVS disks and uses the backup to create new disks.	EVS	2.3.2 Creating a Cloud Disk Backup
Cloud Trace Service (CTS) records operations on CBR resources, facilitating future queries, audits, and backtracking.	CTS	10 Auditing
IAM is a self-service system for enterprise administrators to manage cloud resources. It provides user identity management and access control functions.	IAM	1.5 Permissions

1.8 Basic Concepts

1.8.1 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.
- **Disk backup vaults:** store only disk backups. You can associate disks with a disk backup vault and apply a backup policy to schedule automatic backups.
- **SFS Turbo backup vaults:** store only backups of SFS Turbo file systems. You can associate file systems with an SFS Turbo backup vault and apply a backup policy to schedule automatic backups.

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.

1.8.2 Project and Enterprise Project

Project

A project is used to group and isolate OpenStack resources, such as the compute, storage, and network resources. A project can be a department or a project team. Multiple projects can be created for one account.

Enterprise Project

An enterprise project manages multiple resource instances by category. Resources and projects in different cloud service regions can be classified into one enterprise project. An enterprise can classify resources based on department or project group and put relevant resources into one enterprise project for management. Resources can be migrated between enterprise projects.

1.8.3 Region and AZ

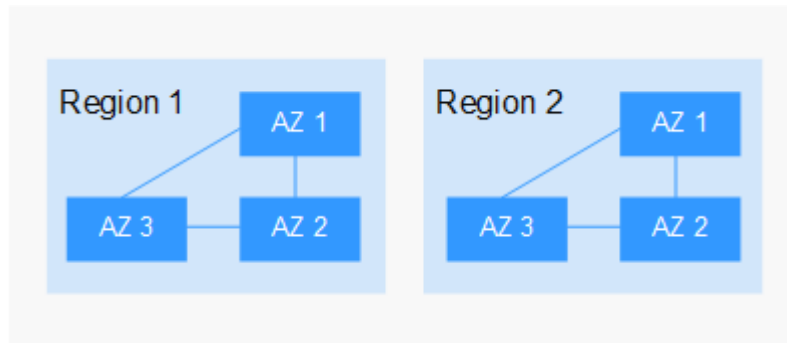
Concept

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 1-4 shows the relationship between regions and AZs.

Figure 1-4 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](#)

[2.2 Step 2: Associate a Resource with the Vault](#)

[2.3 Step 3: Create a Backup](#)



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 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 Select a backup data redundancy policy.

- **Single-AZ:** Backup data is stored in a single AZ, with lower costs.
- **Multi-AZ:** Backup data is stored in multiple AZs to achieve higher reliability.

The backup data redundancy policy cannot be changed after a vault is purchased. Plan and select a policy that best suits your service needs.

Step 5 (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. See

Figure 2-1. You can also select specific disks on a server and associate them with the vault.

Figure 2-1 Selecting servers

Server List

All projects

All statuses

Name

Q

↺

<div><div></div></div> Name/ID	Status	Type	AZ	Associated	↗
<div><div>▼</div><div><div><div><div>✓</div></div><div>as-config-a379-GT9GF9GR</div><div>57112560-0084-42e9-8c35-9e...</div></div></div></div>	<div><div>●</div>Running</div>	ECS	AZ1	No	

Selected Servers (1)

Name

Q

Name/ID	Selected D...	Opera...
<div><div>▼</div><div><div><div><div>as-config-a379-GT9GF9GR</div><div>57112560-0084-42e9-8c...</div></div></div></div></div>	1/1	<div><div>🗑</div></div>

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 6 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 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 7 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 8 If you have subscribed to the Enterprise Project Management Service (EPS), add the vault to an existing enterprise project.

EPS provides a unified method to manage cloud resources by project, allowing you to manage resources, users, and user groups in your projects. The default enterprise project is **default**.

NOTE

If the **CBR FullAccess** permissions have been assigned to IAM users, enterprise projects will not be displayed for you to choose from when you create a vault. Go to the Enterprise Project Management console and assign the **CBR FullAccess** permissions to the target user group.

Step 9 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 10 Complete the creation as prompted.

Step 11 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 [4.1 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 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. See [Figure 2-2](#).

Figure 2-2 Selecting disks

Disk List

All projects

All statuses

Name

	Name	Status	ECS/BMS	Capacity (GB)	Associated
<input checked="" type="checkbox"/>	as-config-a379-GT9GF9GR 1a384961-4a83-4f98-8b5e-068fb...	<div><div>In-use</div></div>	as-config-a3...	40	No

Selected Disks (1)

Name

Name	ECS/BMS	Operation
as-config-a379-GT9GF9GR 1a384961-4a83-4f98-8b5...	as-config-a379-	<div><div></div></div>

 **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 If you have subscribed to the EPS service, add the vault to an existing enterprise project.

EPS provides a unified method to manage cloud resources by project, allowing you to manage resources, users, and user groups in your projects. The default enterprise project is **default**.

 **NOTE**

If the **CBR FullAccess** permissions have been assigned to IAM users, enterprise projects will not be displayed for you to choose from when you create a vault. Go to the Enterprise Project Management console to add the permissions.

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-612c**.

 **NOTE**

You can also use the default name **vault_XXXX**.

Step 8 Complete the creation as prompted.

Step 9 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

2.1.3 Creating an SFS Turbo Backup Vault

This section describes how to create an SFS Turbo backup vault.

Procedure

Step 1 Log in to 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 > SFS Turbo Backups**.

Step 2 In the upper right corner of the page, click **Create SFS Turbo Backup Vault**.

Step 3 Select a protection type.

- **Backup:** An SFS Turbo backup vault stores SFS Turbo backups.

Step 4 Select a backup data redundancy policy.

- **Single-AZ:** Backup data is stored in a single AZ, with lower costs.
- **Multi-AZ:** Backup data is stored in multiple AZs to achieve higher reliability.

The backup data redundancy policy cannot be changed after a vault is purchased. Plan and select a policy that best suits your service needs.

Step 5 (Optional) In the file system list, select the file systems to be backed up. After file systems are selected, they are added to the list of selected file systems. See [Figure 2-3](#).

Figure 2-3 Selecting file systems

Name	Status	Backup Space (GB)	Associated
sfs-test 9707c20a-cb4-4443-80a2-d989a133d38d	Available	500	No
sfs-turbo-6026 b62027b-4aca-4963-9048-e7583d42ab	Available	500	Yes (vault-test)

Name	Operation
sfs-test 9707c20a-cb4-4443-80a2-d989a133d38d	

NOTE

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

Step 6 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 file systems you want to back up.

Step 7 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 file systems associated with this vault will be automatically backed up based on this policy.
- If you select **Skip**, file systems associated with this vault will not be automatically backed up until you apply a backup policy to the vault.

Step 8 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 9 Complete the creation as prompted.

Step 10 Go back to the **SFS Turbo Backups** page. You can see the created vault in the vault list.

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

----End

2.2 Step 2: Associate a Resource with the Vault

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

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

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
SFS Turbo file system	Available

Procedure

Step 1 Log in to 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 a backup page, locate the target vault and click **Associate Server**, **Associate File System**, 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. See [Figure 2-4](#).

Figure 2-4 Associate Server

Name/ID	Status	Type	AZ	Associated
as-config-a379-GT9GF9GR 57112560-0084-42e9-8c35-9e4...	Running	ECS	AZ1	No

Name/ID	Selected D...	Operat...
as-config-a379-GT9GF9GR 57112560-0084-42e9-8c3...	1/1	

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

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.

The backup process for BMSs is the same as that for ECSs.

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 00:00 to 06:00, during which backup schedules may be delayed. So you are advised to evaluate your service types and schedule backups outside of the backup peak hours.

Prerequisites

- Only servers in the **Running** or **Stopped** state can be backed up.
- At least one server backup vault is available.

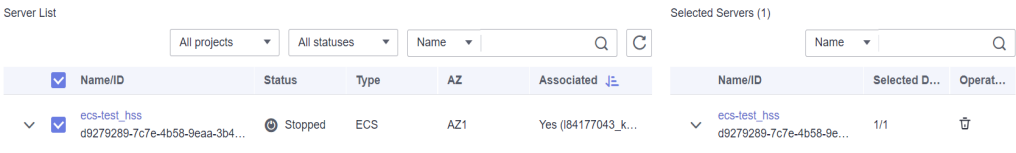
Procedure

Step 1 Log in to 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.

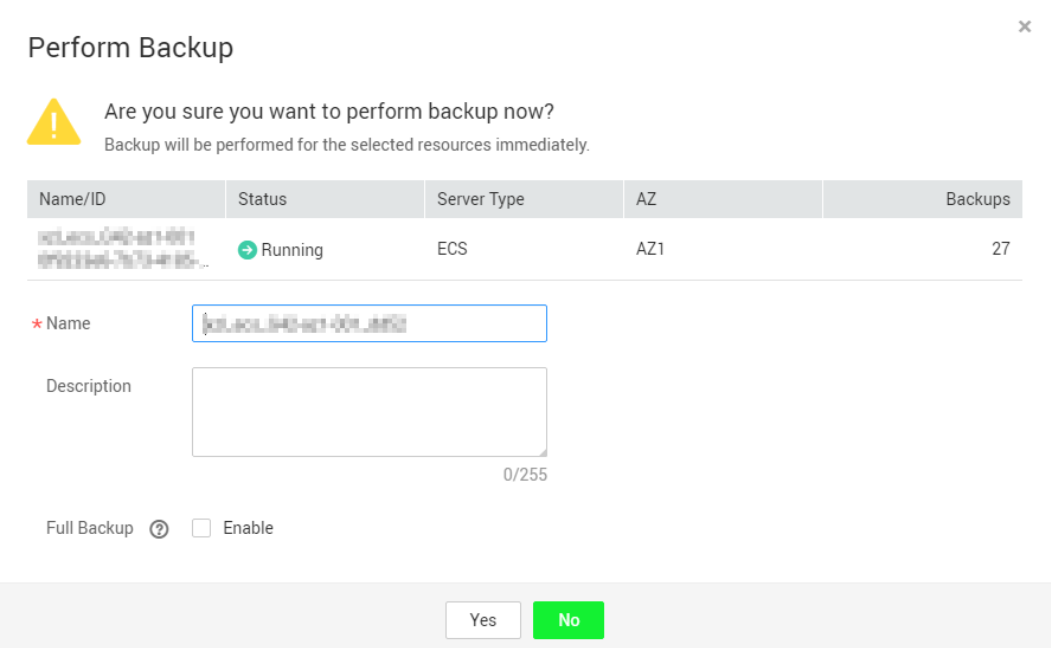
- Step 2** On the **Cloud Server Backups** page, click the **Vaults** tab and find the vault to which the server is associated.
- Step 3** Perform backup in either of the following ways:
- Choose **More > Perform Backup** in the **Operation** column. In the server list, select the server you want to back up. After a server is selected, it is added to the list of selected servers. See [Figure 2-5](#).

Figure 2-5 Selecting the server to be backed up



- 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. See [Figure 2-6](#).

Figure 2-6 Perform Backup



- 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 (-). NOTE You can also use the default name manualbk_xxxx . If multiple servers are to be backed up, the system automatically adds suffixes to their backup names, for example, backup-0001 and backup-0002 .	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. See [Figure 2-7](#).

Figure 2-7 Full Backup

Full Backup  ☐ Enable

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 [7.1 Restoring from a Cloud Server Backup](#) and [5.4 Using a Backup to Create an Image](#).

----End

2.3.2 Creating a Cloud Disk Backup

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

If the disk to be backed up is encrypted, the backup will also be automatically encrypted. The encryption attribute of backups cannot be changed.

Backing up a server does not impact the disk performance.



Peak hours of the backup service are from 00:00 to 06:00, during which backup schedules may be delayed. So you are advised to evaluate your service types and schedule backups outside of the backup peak hours.

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 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. See [Figure 2-8](#).

Figure 2-8 Selecting the disk to be backed up



The screenshot shows the 'Disk List' and 'Selected Disks (1)' panels. The 'Disk List' panel has filters for 'All projects', 'All statuses', and a search bar. It contains a table with columns: Name, Status, ECS/BMS, Capacity (GB), and Associated. One disk is listed with status 'In-use'. The 'Selected Disks (1)' panel shows the same disk selected, with columns for Name, ECS/BMS, and Operation.


Name	Status	ECS/BMS	Capacity (GB)	Associated
as-config-a379-GT9GF9GR 1a384961-4a83-4f98-8b5e-068fb...	In-use	as-config-a37...	40	Yes (vault-edfd)

Name	ECS/BMS	Operation
as-config-a379-GT9GF9GR 1a384961-4a83-4f98-8b5...	as-config-a379-	


- 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. See [Figure 2-9](#).

Figure 2-9 Perform Backup

Perform Backup



Are you sure you want to perform backup now?
Backup will be performed for the selected resources immediately.

Name/ID	Status	ECS/BMS	Capacity (GB)	Backups
volume-az3-0001 3d5ac8c6-0d0c-4f8c-...	 Available	--	10	3


* Name

volume-az3-0001_71d2

Description

0/255


Full Backup



☐ Enable

Yes

No

 **NOTE**

CBR will identify whether the selected disk is encrypted. If it is encrypted, the backups will be automatically encrypted.

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 (-). NOTE You can also use the default name manualbk_XXXX . If multiple disks are to be backed up, the system automatically adds suffixes to their backup names, for example, backup-0001 and backup-0002 .	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. See [Figure 2-10](#).

Figure 2-10 Full Backup

Full Backup  ☐ Enable

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 [7.2 Restoring from a Cloud Disk Backup](#).

----End

2.3.3 Creating an SFS Turbo Backup

This section describes how to quickly create an SFS Turbo file system backup.

To ensure data integrity, you are advised to back up the file system during off-peak hours when no data is written to the file system.



Peak hours of the backup service are from 00:00 to 06:00, during which backup schedules may be delayed. So you are advised to evaluate your service types and schedule backups outside of the backup peak hours.

Prerequisites

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

Procedure

Step 1 Log in to CBR Console.

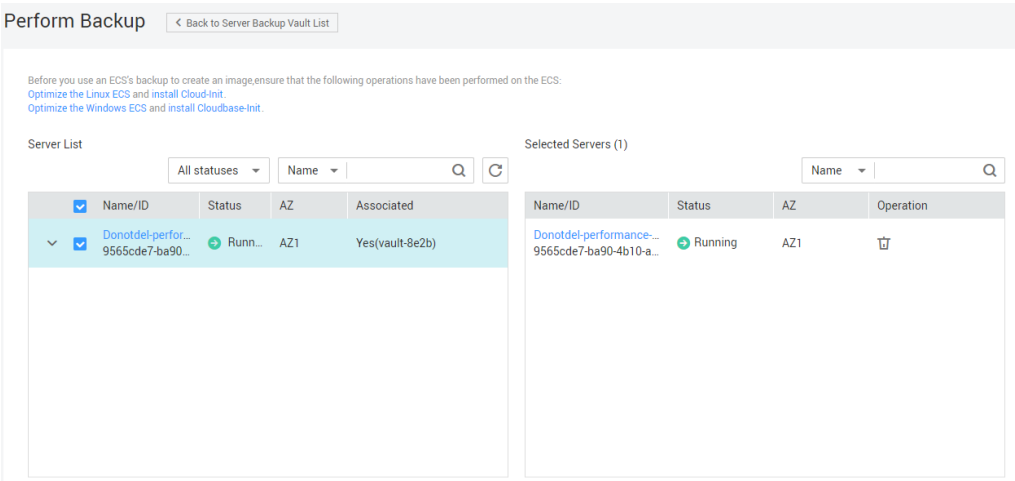
1. Log in to the management console.
2. Click  in the upper left corner and select a region.
3. Click  and choose **Storage > Cloud Backup and Recovery > SFS Turbo Backups**.

Step 2 On the **SFS Turbo Backups** page, click the **Vaults** tab and find the vault to which the file system is associated.

Step 3 Perform backup in either of the following ways:

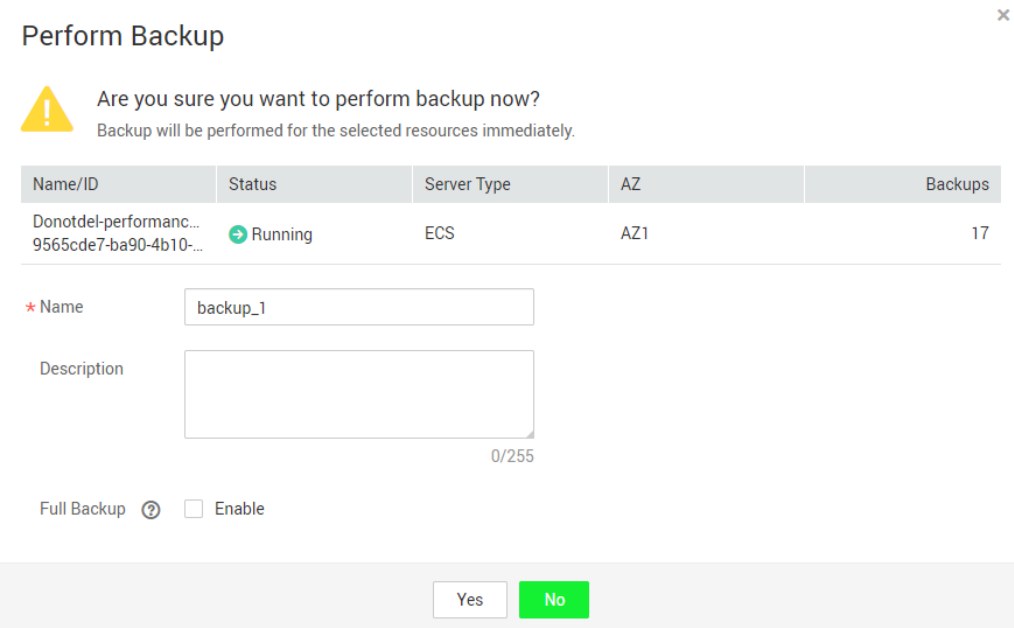
- Choose **More > Perform Backup** in the **Operation** column. In the file system list, select the file system to be backed up. After a file system is selected, it is added to the list of selected file systems. See [Figure 2-11](#).

Figure 2-11 Selecting the file system to be backed up



- Click the vault name to go to the vault details page. On the **Associated File Systems** tab page, locate the target file system and click **Perform Backup** in the **Operation** column. See [Figure 2-12](#).

Figure 2-12 Perform Backup



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

Table 2-4 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 (-). NOTE You can also use the default name manualbk_XXXX . If multiple file systems are to be backed up, the system automatically adds suffixes to their backup names, for example, backup-0001 and backup-0002 .	manualbk_d819
Description	Description of the backup. It cannot exceed 255 characters.	--

Step 5 Click **OK**. CBR automatically creates a backup for the file system.

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 file system 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 create a new SFS Turbo file system using the backup. For details, see [5.6 Using a Backup to Create a File System](#).

----End

3 Permissions Management

[3.1 Creating a User and Granting CBR Permissions](#)

[3.2 Creating a Custom Policy](#)

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 employees based on your enterprise's organizational structure. Each IAM user will have their own security credentials for accessing CBR resources.
- Grant only the permissions required for users to perform a specific task.
- 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.

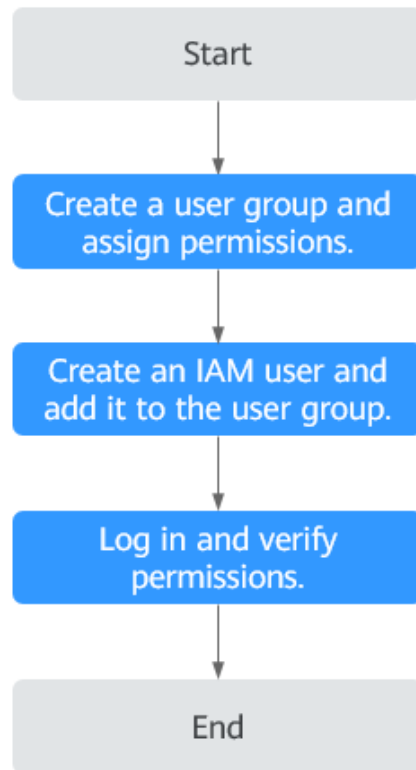
Figure [Figure 3-1](#) illustrates the procedure for granting permissions.

Prerequisites

Learn about the permissions (see [1.5 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 assign the **CBR ReadOnlyAccess** policy to the group.
2. Create an IAM user and add it to the user group.
Create a user on the IAM console and add the user to the group created in [1](#).
3. Log in and verify permissions.
Log in to 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 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"
    ]
  }
]
```

4 Vault Management

[4.1 Querying a Vault](#)

[4.2 Deleting a Vault](#)

[4.3 Dissociating a Resource](#)

[4.4 Migrating a Resource](#)

[4.5 Expanding Vault Capacity](#)

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 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.

Parameter	Description
Type	Vault type
Status	Vault status. Table 4-2 describes the vault statuses.
Specifications	Vault specifications, which can be server backup or application-consistent backup <ul style="list-style-type: none">• A server backup vault stores backups of non-database servers.• An application-consistent backup vault stores backups of database servers.
Vault Capacity (GB)	Capacity used by the backups in the vault. It shows the space used by backups and the total vault capacity. For example: If 20/100 is displayed, 20 GB has been used out of the 100 GB vault capacity.
Policy Status	Policy status or no policy applied <ul style="list-style-type: none">• No policy applied: The vault has not been applied with any backup policy yet.• Enabled: The vault has been applied with a backup policy, and the policy is enabled.• Disabled: The vault has been applied with a backup policy, but the policy is disabled.
Associated Servers/ File Systems/Disks	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.

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.

Status	Attribute	Description
Locked	An intermediate state	An intermediate state displayed when a capacity expansion is in progress. 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 Available .
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 Error state when an exception occurs during task execution. You can click Tasks 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.

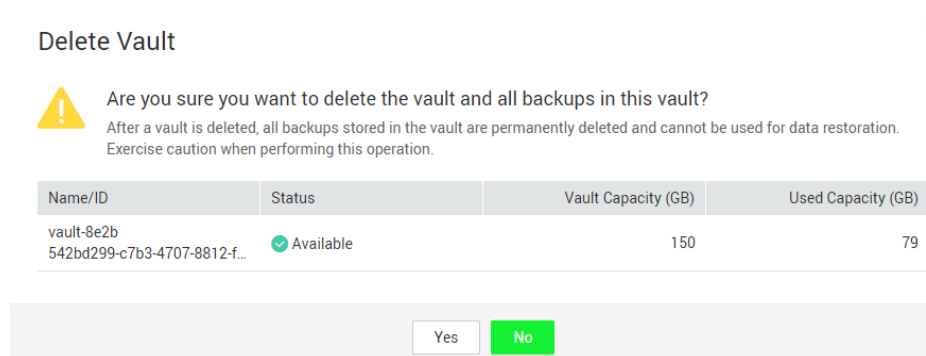
Procedure

Step 1 Log in to CBR Console.

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

Step 2 Find the target vault and choose **More > Delete** in the **Operation** column. See [Figure 4-1](#). All backups stored in the vault will be deleted once you delete a vault.

Figure 4-1 Deleting 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 CBR Console.

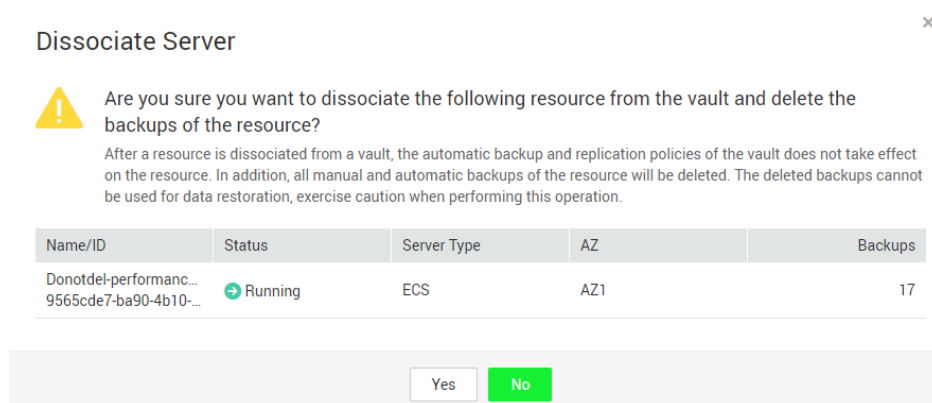
1. Log in to the management console.
2. Click  in the upper left corner and select a region.

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

Step 2 Find the target vault and click its name.

Step 3 In this example, we will be using the **Cloud Server Backups** page to illustrate the process. Click the **Associated Servers** tab. Find the target server and click **Dissociate** in the **Operation** column. See [Figure 4-2](#).

Figure 4-2 Dissociating a server



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 specifications.
- 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 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 **Yes**.

Step 5 View the migration progress on the **Tasks** page. If **Status** changes to **Successful**, the resource has been migrated.

Step 6 Go to the destination vault to confirm that the resource has been associated and all its backups have been migrated.



----End

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 CBR Console.

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

Step 2 Find the target vault and choose **More > Expand Capacity** in the **Operation** column. See [Figure 4-3](#).

Figure 4-3 Expanding vault capacity

Expand Server Backup Vault

[← Back to Server Backup Vault List](#)

Current Configuration

Vault Name	vault-7d25	Region	ru-moscow
Vault ID	bb97392b-c4ef-48d4-a874-1c8cdf5dd668	Backup Type	Server backup
Current Capacity (GB)	100		
Used Capacity (GB)	0		

Add Capacity (GB)

−

10

+

New Capacity (GB): 110

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

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

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

----End

Auto Capacity Expansion



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

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

NOTE

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

Step 1 Log in to CBR Console.

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

Step 2 Find the target vault and click its name.

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

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

----End

5 Backup Management

[5.1 Viewing a Backup](#)

[5.2 Sharing a Backup](#)

[5.3 Deleting a Backup](#)

[5.4 Using a Backup to Create an Image](#)

[5.5 Using a Backup to Create a Disk](#)

[5.6 Using a Backup to Create a File System](#)

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.

Viewing Backup Details

Step 1 Log in to 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.
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 Tasks 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 Tasks 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 Tasks 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 Error 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.
- You can search for backups by selecting a project from the **All projects** drop-down list in the upper right corner of the backup list.
- You can export the backup list by clicking  in the list's upper right corner.

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.
- Encrypted backups cannot be shared.
- 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 CBR Console.

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

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

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

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

- Sharing a backup

Figure 5-1 Share Backup

×

Share Backup

Backup Details

Backup Nameautobk_6ad7

Server NameDonotdel-performance-jumpserver

Backup ID47a03e17-ec70-449a-9724-0474192b1647

Backup TypeECS

Share Backup

Cancel Sharing

You can share the backup with 10 more projects.

★ Enter the domain name of the recipient.

Add

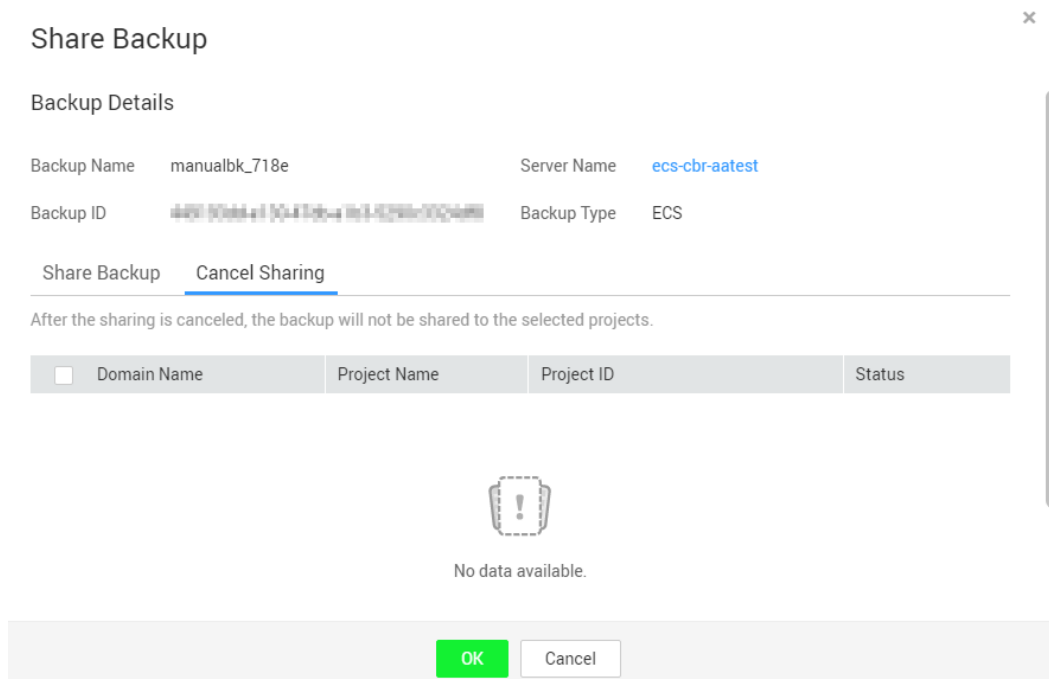
Domain Name	Project Name	Project ID	Operation
-------------	--------------	------------	-----------

OK

Cancel

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 ten projects.
 4. Click **OK**.
- Canceling sharing
 1. Click the **Cancel Sharing** tab, select the projects you want to cancel sharing, and click **OK**. See [Figure 5-2](#).



Figure 5-2 Cancel Sharing



----End

Procedure for the Recipient

Step 1 Log in to 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 [2.1 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. See [Figure 5-3](#).

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

Figure 5-3 Accepting a shared backup

Accept Shared Backup

To accept a shared backup, you need to create a vault or select an existing vault.

★ Select Vault

The remaining backup capacity of the vault must be greater than that of the shared backup.

Name

Q

Create Vault

Name	Type	Status	Vault Capacity (GB)
<div></div> vault-demo	Backup	<div></div> Available	Used <div></div> 0/100

OK

Cancel

Step 5 View the shared backup you accepted in the backup list. See [Figure 5-4](#).

Figure 5-4 Shared backup accepted

Vaults

Backups

Backups

Received Shared Backups

Delete

All statuses

Advanced Search

Backup Name	Status	Created	Operation
<div></div> autobk_d425	<div></div> Available	2023/05/05 12:00:48 GMT+08:00	Delete Create Disk
<div></div> autobk_bda0	<div></div> Available	2023/05/04 12:00:59 GMT+08:00	Delete Create Disk

----End

5.3 Deleting a Backup

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

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


CBR supports manual deletion of backups and automatic deletion of expired backups. The latter is executed based on the backup retention rule in the backup policy. For details, see [6.1 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 CBR Console.

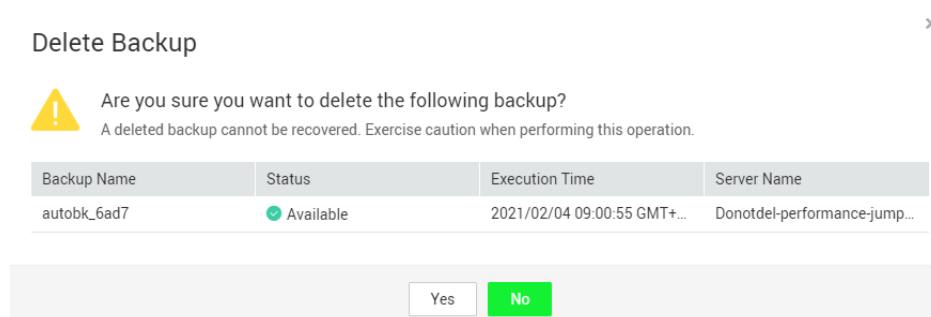
1. Log in to the management console.
2. Click  in the upper left corner and select a region.

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 [5.1 Viewing a Backup](#).

Step 3 Choose **More > Delete** from the **Operation** column. See [Figure 5-5](#). Alternatively, select the backups you want to delete in a batch and click **Delete** in the upper left corner to delete them.

Figure 5-5 Deleting a backup



Step 4 Click **Yes**.

----End

Follow-up Procedure

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

5.4 Using a Backup to Create an Image

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

Prerequisites

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

- The backup is in the **Available** state or in the **Creating** state which is marked with "Image can be created."

 **NOTE**

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



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

Notes

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

Procedure

Step 1 Log in to 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 [5.1 Viewing a Backup](#).

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

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

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

----End



5.5 Using a Backup to Create a Disk

You can create new disks from backups. Once created, the new disks will contain the backup data.

The new 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 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 [5.1 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

5.6 Using a Backup to Create a File System

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

Procedure

Step 1 Log in to CBR Console.

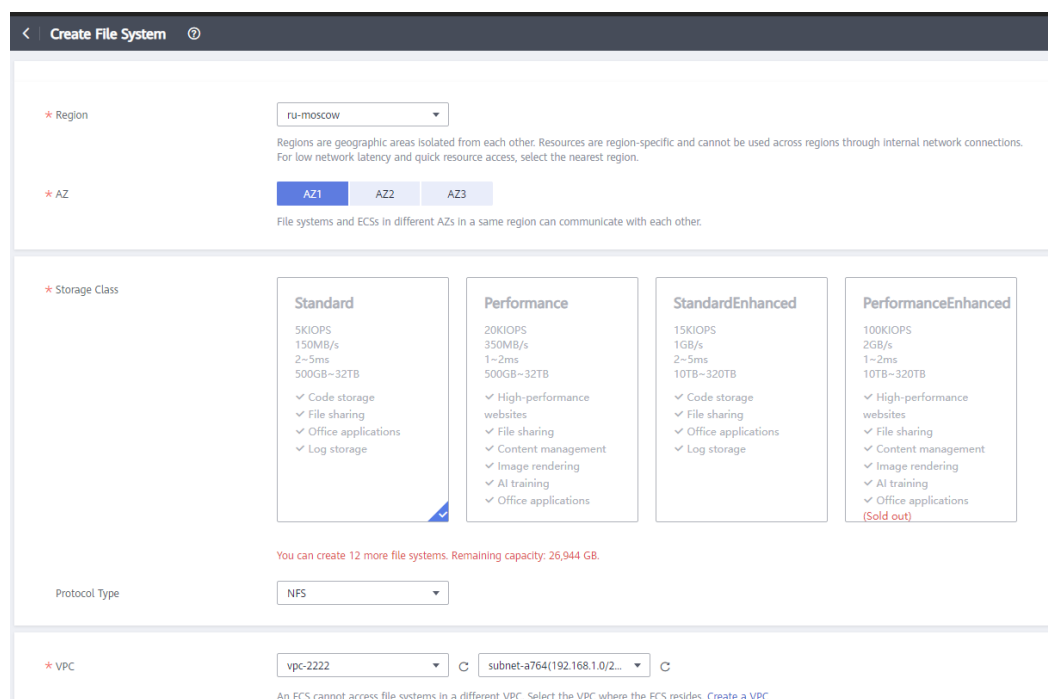
1. Log in to the management console.
2. Click  in the upper left corner and select a region.
3. Click  and choose **Storage > Cloud Backup and Recovery**. Select a backup type from the left navigation pane.

Step 2 Click the **Backups** tab and locate the desired backup. For details, see [5.1 Viewing a Backup](#).

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

Step 4 Configure the file system parameters. See [Figure 5-6](#).

Figure 5-6 Creating a file system



The screenshot shows the 'Create File System' configuration page. It includes the following sections:

- Region:** A dropdown menu set to 'ru-moscow'. A note states: 'Regions are geographic areas isolated from each other. Resources are region-specific and cannot be used across regions through internal network connections. For low network latency and quick resource access, select the nearest region.'
- AZ:** Three buttons labeled 'AZ1', 'AZ2', and 'AZ3'. A note states: 'File systems and ECSs in different AZs in a same region can communicate with each other.'
- Storage Class:** Four cards representing different storage classes:
 - Standard:** 5KIOPS, 150MB/s, 2~5ms, 500GB~32TB. Features: Code storage, File sharing, Office applications, Log storage.
 - Performance:** 20KIOPS, 350MB/s, 1~2ms, 500GB~32TB. Features: High-performance websites, File sharing, Content management, Image rendering, AI training, Office applications.
 - StandardEnhanced:** 15KIOPS, 1GB/s, 2~5ms, 10TB~320TB. Features: Code storage, File sharing, Office applications, Log storage.
 - PerformanceEnhanced:** 100KIOPS, 2GB/s, 1~2ms, 10TB~320TB. Features: High-performance websites, File sharing, Content management, Image rendering, AI training, Office applications. Status: (Sold out).
- Protocol Type:** A dropdown menu set to 'NFS'. A note states: 'You can create 12 more file systems. Remaining capacity: 26,944 GB.'
- VPC:** Two dropdown menus. The first is set to 'vpc-2222' and the second to 'subnet-a764(192.168.1.0/2...'. A note states: 'An ECS cannot access file systems in a different VPC. Select the VPC where the ECS resides. Create a VPC.'

 **NOTE**

- You can learn about the parameter descriptions in table "Parameter description" under "Creating an SFS Turbo File System" in "Create a File System" of the *Scalable File Service User Guide*.

Step 5 Click **Create Now**.

Step 6 Go back to the file system list and check whether the file system is successfully created.

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

----**End**

6 Policy Management

[6.1 Creating a Backup Policy](#)

[6.2 Modifying a Policy](#)

[6.3 Deleting a Policy](#)

[6.4 Applying a Policy to a Vault](#)

[6.5 Removing a Policy from a Vault](#)

6.1 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, SFS Turbo backup vaults
- A backup policy must be enabled before it can be used for periodic backups.
- A maximum of 32 backup policies can be created in each account.
- When 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.

Procedure

Step 1 Log in to CBR Console.

1. Log in to the management console.
2. Click  in the upper left corner and select a region.

3. Click  and choose **Storage > Cloud Backup and Recovery**.

Step 2 Choose **Policies** in the left navigation pane and click the **Backup Policies** tab. In the upper right corner, click **Create Policy**. See [Figure 6-1](#).

Figure 6-1 Creating a backup policy

Create Policy

Basic Information

Type

Backup policy

Name

policy_163713

Status

Enable

Disable

Backup Rule

Current rule:
Automatically perform weekly backups at 22:00 on the following selected days: Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday

Backup Frequency

Weekly

Day based

Automatically perform backups every

Mon

Tues

Wed

Thur

Fri

Sat

Sun

Execution Time

Select All

Invert Selection

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

Retention Rule

Current rule: Keep backups from the last 1 month.

Type

Backup quantity

Time period

Permanent

Rule

Keep backups from the last

1 month

Older backups are automatically deleted.

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

2023-05-08

53

Parameter	Description	Example Value
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.
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>NOTICE</p> <ul style="list-style-type: none">• There may be a time difference between the scheduled backup time and the actual backup time.• If a large amount of data needs to be backed up, you are advised to make backup less frequent to prevent the system from skipping any execution time. For example, a disk is scheduled to be backed up at 00:00, 01:00, and 02:00. A backup task starts at 00:00. Because a large amount of incremental data needs to be backed up or a heap of backup tasks are executed at the same time, this backup task takes 90 minutes and completes at 01:30. The system 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.• The execution times refer to the local times of clients, not the time zone and times of the region.	<p>00:00, 02:00</p> <ul style="list-style-type: none">• It is recommended that backups be performed during service off-peak hours or when no services are running.• Peak hours of the backup service are from 00:00 to 06:00, during which backup schedules may be delayed. So you are advised to evaluate your service types and schedule backups outside of the backup peak hours.

Parameter	Description	Example Value
Backup Cycle	<p>Select a backup frequency.</p> <ul style="list-style-type: none"> • Week-based cycle Specifies on which days of each week the backup task will be executed. You can select multiple days. • Custom cycle Specifies the interval (every 1 to 30 days) for executing the backup task. 	<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">• Time period 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.• Backup quantity You can set the maximum number of backups to retain for each resource. The value ranges from 2 to 99999.• Advanced Options You can also set long-term retention rules with advanced options. Long-term retention rules and quantity-based retention rules will be both applied.<ul style="list-style-type: none">– Day-based: 0–100– Weekly: 0–100– Monthly: 0–100– Yearly: 0–100A resource may be backed up multiple times in a day. If day-based backup is configured, only the most recent backup of that day is retained. If you set Day-based to 5, the most recent backup of each of the last five days that have backups generated will be retained and the earliest backups will be deleted automatically. If day-based, weekly, monthly, and yearly retention rules are all configured, all the rules will apply and the union set of backups will be retained. For example, if Day-based is set to 5 and Weekly to 1, five backups will be retained. The long-term retention rule and the quantity-based retention rule both apply.• Permanent	6 months

Parameter	Description	Example Value
	<p>NOTE</p> <ul style="list-style-type: none">- 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.- Expired backups are not deleted right after they are expired. They will be deleted from 12:00 to 00:00 in batches.- The retention rules apply only to auto-generated backups, but not manual backups. Manual backups need to be deleted manually.- A maximum of 10 backups are retained for failed periodic backup tasks. They are retained for one month and can be deleted manually.	

 **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.

6.2 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 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.

Edit Policy

Basic Information

Name

Status Enabled Disabled

Backup Rule

Current rule:

Automatically perform backups at 00:00,01:00,02:00,03:00,04:00,05:00,06:00,07:00,08:00,09:00,10:00,11:00,12:00,13:00,14:00,15:00,16:00,17:00,18:00,19:00,20:00,21:00,22:00,23:00 every day.

Backup Frequency Weekly Day based

Automatically perform backups every — 1 + days.

Execution Time Select All Invert Selection

<input checked="" type="checkbox"/> 00:00	<input checked="" type="checkbox"/> 01:00	<input checked="" type="checkbox"/> 02:00	<input checked="" type="checkbox"/> 03:00	<input checked="" type="checkbox"/> 04:00
<input checked="" type="checkbox"/> 05:00	<input checked="" type="checkbox"/> 06:00	<input checked="" type="checkbox"/> 07:00	<input checked="" type="checkbox"/> 08:00	<input checked="" type="checkbox"/> 09:00
<input checked="" type="checkbox"/> 10:00	<input checked="" type="checkbox"/> 11:00	<input checked="" type="checkbox"/> 12:00	<input checked="" type="checkbox"/> 13:00	<input checked="" type="checkbox"/> 14:00
<input checked="" type="checkbox"/> 15:00	<input checked="" type="checkbox"/> 16:00	<input checked="" type="checkbox"/> 17:00	<input checked="" type="checkbox"/> 18:00	<input checked="" type="checkbox"/> 19:00
<input checked="" type="checkbox"/> 20:00	<input checked="" type="checkbox"/> 21:00	<input checked="" type="checkbox"/> 22:00	<input checked="" type="checkbox"/> 23:00	

Retention Rule

Current rule: Permanent

Type Backup quantity Time period Permanent

After the policy's retention rule type is changed from Time period to Permanent, the new retention rule will be applied only to new backups, and backups generated before this change will be kept and deleted based on the old rule. [Learn more](#)

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 [12.4.2 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

6.3 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 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

6.4 Applying a Policy to a Vault

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

Procedure

Step 1 Log in to 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**. See [Figure 6-2](#).

Figure 6-2 Setting a backup policy

Apply Backup Policy

Status 

★ Backup Policy defaultPolicy | Enabled | Automatically perform weekly... ▼  Create Policy

OK Cancel

Step 3 Select an existing backup policy from the drop-down list or create a new one. For how to create a policy, see [6.1 Creating a Backup Policy](#).

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

----End

6.5 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

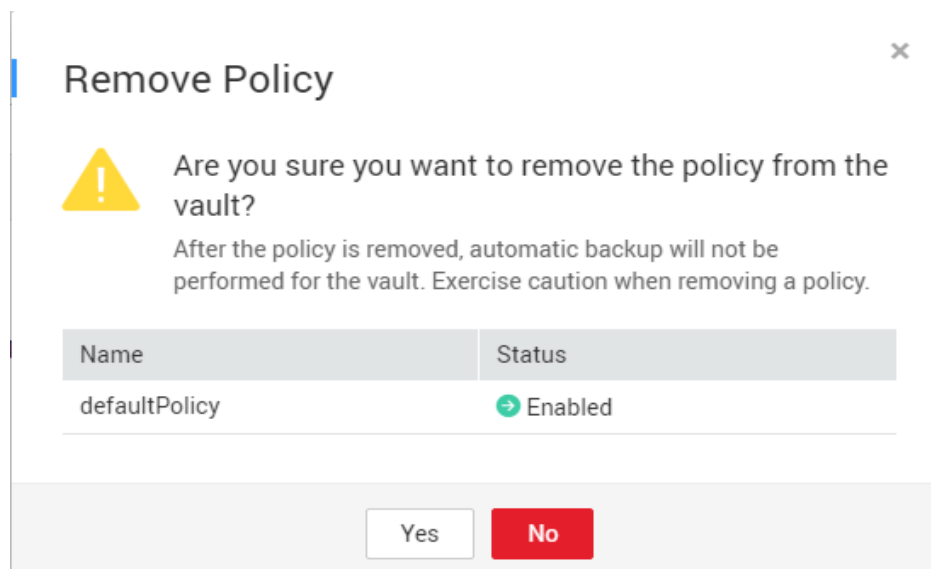
Step 1 Log in to CBR Console.

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

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

Step 3 In the **Policies** area, click **Remove Policy**. See [Figure 6-3](#).

Figure 6-3 Removing a 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](#)

[7.2 Restoring from a Cloud Disk Backup](#)

[7.3 Restoring from an SFS Turbo Backup](#)

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.

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

Constraints



- When restoring from a cloud server backup, backup of a data disk cannot be restored to the system disk.
- Data cannot be restored to servers in the **Faulty** state.
- Concurrent data restoration is not supported.

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 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 [5.1 Viewing a Backup](#).
- Step 3** In the row of the backup, click **Restore Server**. See [Figure 7-1](#).

NOTICE

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

Figure 7-1 Restoring a server

Restore Server

Are you sure you want to restore the server data by using the following backup?
This operation will overwrite the server data by using the following backup. Once started, the restoration cannot be canceled.

Backup Name	Status	Execution Time	Server Name
autobk_6ad7	Available	2021/02/04 09:00:55 GMT+...	Donotdel-performance-jump...

☒ Start the server immediately after restoration

^ Disk Backups

The specified disk must be in the Available or In-use state and its capacity cannot be smaller than the disk you want to back up.

You can create a disk and specify that backups are restored to this disk. [Create a disk](#).

After the disk is created, manually attach the disk to the server you want to restore.

Backup Name	Capacity (GB)	Used As	Specified Disk
-------------	---------------	---------	----------------

Yes No

- 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 [8 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 [13.2 Data Disks Are Not Displayed After a Windows Server Is Restored](#).

----End

7.2 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

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

Procedure

Step 1 Log in to 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.

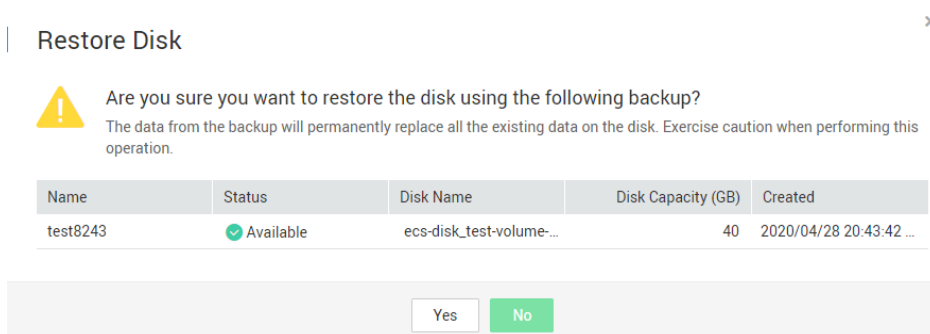
Step 2 Click the **Backups** tab. Locate the desired backup. For details, see [5.1 Viewing a Backup](#).

Step 3 In the row of the backup, click **Restore Disk**. The **Restore Disk** dialog box is displayed. See [Figure 7-2](#).

NOTICE

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

Figure 7-2 Restore Disk



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

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

Step 5 After the restoration is complete, re-attach the disk to the server. For details, see section "Attaching an Existing Non-Shared Disk" in the *Elastic Volume Service User Guide*.

----End

7.3 Restoring from an SFS Turbo Backup



You can use an SFS Turbo backup to restore the file system to its state when the backup was created.

Prerequisites

The file system to be restored is **Available**.

Procedure

Step 1 Log in to 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 [5.1 Viewing a Backup](#).

Step 3 In the row of the backup, click **Restore Data**. See #cbr_03_0106/fig122481021113018.

NOTICE


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

Restore Data



Are you sure you want to restore the file system using the following backup?

The file system data will be overwritten by the backup. This operation cannot be undone.

Backup Name	Status	File System Name	File System Capacity (...)	Created
autobk_f6fd	 Available	sfs-turbo-a423	500	2021/02/04 08:59:28 ...

Yes

No

Step 4 Click **Yes**. You can confirm whether data has been restored on the **Backups** tab page of **SFS Turbo Backups** or on the SFS console.

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

----**End**

8 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 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

9Monitoring

9.1 CBR Metrics

9.1 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 9-1 CBR metrics

Metric ID	Metric Name	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
used_vault_size	Used Vault Size	Used capacity of the vault Unit: GB	≥ 0	Vault	15 min
vault_util	Vault Usage	Capacity usage of the vault	0~100 %	Vault	15 min

Dimensions

Key	Value
instance_id	Vault name/ID

Viewing Monitoring Statistics

Step 1 Log in to the management console.

Step 2 View the monitoring graphs using either of the following methods.

- Method 1: Choose **Storage > Cloud Backup and Recovery**. In the vault list, locate the vault whose monitoring data you want to view and choose **More > View Monitoring Data** in the **Operation** column.
- Method 2: Choose **Management & 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 Auditing

You can use Cloud Trace Service (CTS) to trace operations in CBR.

Prerequisites

CTS has been enabled.

Key Operations Recorded by CTS

Table 10-1 CBR operations that can be recorded by CTS

Operation	Resource Type	Trace Name
Creating a policy	policy	createPolicy
Updating a policy	policy	updatePolicy
Deleting a policy	policy	deletePolicy
Setting a vault policy	vault	associatePolicy
Removing a policy from a vault	vault	dissociatePolicy
Creating a vault	vault	createVault
Modifying a vault	vault	updateVault
Deleting a vault	vault	deleteVault
Removing resources	vault	removeResources
Adding resources	vault	addResources
Performing a backup	vault	createVaultBackup
Creating a backup	backup	createBackup
Deleting a backup	backup	deleteBackup
Restoring a backup	backup	restoreBackup

Viewing Audit Logs

For how to view audit logs, see section "Querying Real-Time Traces" in the *Cloud Trace Service User Guide*.

Disabling or Enabling a Tracker

The following procedure illustrates how to disable an existing tracker on the CTS console. After the tracker is disabled, the system will stop recording operations, but you can still view existing operation records.

- Step 1** Log in to the management console.
- Step 2** Click **Service List** and choose **Management & Deployment > Cloud Trace Service**.
- Step 3** Choose **Tracker List** in the left navigation pane.
- Step 4** In the tracker list, click **Disable** in the **Operation** column.
- Step 5** Click **Yes**.
- Step 6** After the tracker is disabled, the available operation changes from **Disable** to **Enable**. To enable the tracker again, click **Enable** and then click **Yes**. The system will start recording operations again.

----End



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. Click  in the upper left corner and select the desired region and project.
3. In the upper right corner of the page, click  .
The **Service Quota** page is displayed.
4. View the used and total quota of each type of resources on the displayed page.

If a quota cannot meet service requirements, apply for a higher quota.

How Do I Apply for a Higher Quota?

The system does not support online quota adjustment. If you need to adjust a quota, call the hotline or send an email to the customer service mailbox. Customer service personnel will timely process your request for quota adjustment and inform you of the real-time progress by making a call or sending an email.

Before dialing the hotline number or sending an email, make sure that the following information has been obtained:

- Account name, project name, and project ID, 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, project name, and project ID on the **My Credentials** page.
- Quota information, which includes:

- Service name
- Quota type
- Required quota

[Learn how to obtain the service hotline and email address.](#)

12 FAQs

[12.1 Concepts](#)

[12.2 Backup](#)

[12.3 Restoration](#)

[12.4 Policies](#)

[12.5 Optimization](#)

[12.6 Others](#)

12.1 Concepts

12.1.1 What Are Full Backup and Incremental Backup?

CBR by default performs a full backup for a resource in the initial backup and incremental backups in all subsequent backups. If a resource has been backed up for many times, and then all of its generated backups are deleted, and the resource is backed up again, the system will also perform a full backup for the resource.

- The initial full backup covers only the used capacity of a disk. If a 100 GB disk contains 40 GB data, the initial backup consumes 40 GB backup space.
- Subsequent incremental backup backs up data changed since the last backup. If 5 GB data changed since the last backup, only the 5 GB changed data will be backed up.

CBR allows you to use any backup, no matter it is a full or incremental one, to restore the full data of a resource. By virtue of this, manual or automatic deletion of a backup will not affect the restoration function.

Suppose server **X** has backups **A**, **B**, and **C** (in time sequence) and every backup involves data changes. If backup **B** is deleted, you can use backup **A** or **C** to restore data. If backup **A** and backup **B** are both deleted, you can still use backup **C** to restore data.

 **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, not by calculating 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	Snapshot data is stored with disk data. NOTE 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.	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 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, cloud disk backups, and SFS Turbo 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.

12.1.5 What Are the Differences Between Backups and Images?

CBR and Image Management Service (IMS) have some complementary functions and can be used together in certain scenarios. Like CBR, IMS can also be used to back up ECSs.

Differences Between Backups and Images

[Table 12-3](#) lists the differences between them.

Table 12-3 Differences between backups and images

Item	CBR	IMS
Concept	A backup contains the status, configuration, and data of a cloud server or disk stored at a specific time point for recovery in case of a fault. It is used to ensure data security and improve availability.	An image provides all information required for starting a cloud server. It is used to create a cloud server and deploy software environments in batches. A system disk image contains an OS and pre-installed application software for running services. A data disk image contains service data. A full-ECS image contains data of the system disk and data disks.

Item	CBR	IMS
Usage method	<ul style="list-style-type: none">• Data storage location: Unlike server or disk data, backups are stored in OBS. Deleting a disk will not clear its backups.• Operation object: A server or disk can be backed up at a given point in time. CBR supports automatic backup and automatic deletion by configuring backup policies.• Usage: Backups can be used to restore data to the original server or disk, or to create a new disk or full-ECS image.• Support exporting to a local PC: No	<ul style="list-style-type: none">• Data storage location: Unlike server or disk data, backups are stored in OBS. If a server or disk that is created using an image is deleted, the image will not be cleared.• Operation object: The system disk and data disks of a server can be used to create private images. You can also create private images using external image files.• Usage: System disk images or full-ECS images can be used to create new servers, and data disk images can be used to create new disks for service migration.• Support exporting to a local PC: Yes However, full-ECS images cannot be exported to a local PC.
Application scenarios	CBR applies to the following scenarios: <ul style="list-style-type: none">• Data backup and restoration• Rapid service deployment and migration	IMS applies to the following scenarios: <ul style="list-style-type: none">• Server migration to the cloud or between clouds• Deploying a specific software environment• Deploying software environments in batches• Backing up server operating environments
Advantages	Supports automatic backup. Data on a server or disk at a certain time point can be retained periodically or quantitatively. You can back up on-premises VMware VMs, synchronize the backups to the cloud, and then use the backups to restore data to new ECSs.	Supports system disk backup. You can import the data disk image of a local server or a server provided by another cloud platform to IMS and then use the image to create an EVS disk.

 **NOTE**

Although backups and images are stored in OBS, you cannot view backup and image data in OBS, because they do not occupy your resources.

Relationship Between Backups and Images

1. You can use an ECS backup to create a full-ECS image.
2. Before creating a full-ECS image for an ECS, you need to back up the target ECS.
3. 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.

12.1.6 What Are the Differences Between Cloud Server Backup and Cloud Disk Backup?

Table 12-4 describes the differences between cloud server backup and cloud disk backup.

Table 12-4 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.

12.1.7 Why Does the Used Capacity of a Vault Change Only Slightly After I Deleted Unwanted Backups?

Symptoms

After unwanted backups are deleted from the vault, the used capacity of the vault decreases by only 1 GB to 2 GB.

Possible Causes

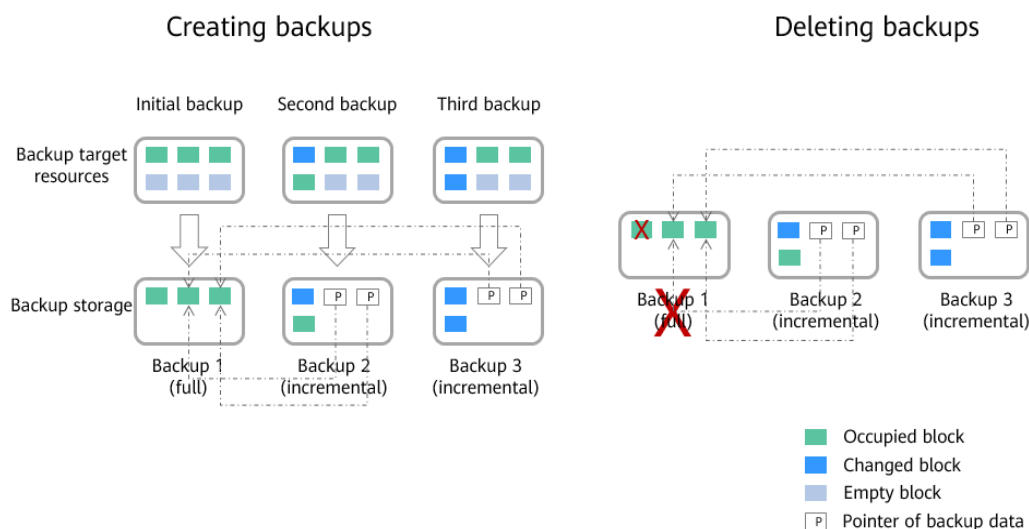
The backup mechanism of CBR:

- By default, CBR performs a full backup for a resource for the first time and backs up all used data blocks. All subsequent backups are incremental. An

incremental backup backs up only the data blocks changed since the last backup.

- Each incremental backup is a virtual full backup. Correlated data blocks are indexed by using pointers.
- When you delete a backup, no matter manually or automatically, only data blocks that are not referenced by other backups will be deleted.

Figure 12-1 Backup mechanism



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.

12.2.2 Can I Back Up a Server Deployed with Databases?

Yes. To back up applications requiring strict consistency, such as databases and email systems, you are advised to suspend all write operations and then perform backup. If write operations cannot be suspended, you can stop the application systems or the server for offline backup. Without doing these, status of the server after restoration is similar to restart upon an unexpected power failure and log rollback will be performed on databases to keep data consistent.

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 Can I Back Up Two Disks to One Target Disk?

No. One target disk corresponds to one source disk. The data of two disks cannot be backed up to one target disk.

12.2.7 How Do I Replicate a Disk to the Same AZ in a Region as the Source Disk?

Back up the desired disk. Then use the disk backup to create a new disk, and select the same AZ as that of the source disk for the new one.

12.2.8 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.

12.2.9 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.

12.2.10 How Many Backups Can I Create for a Resource?

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

12.2.11 Can I Stop an Ongoing Backup Task?

No. An ongoing backup task cannot be stopped.

12.2.12 How Do I Reduce the Vault Space Occupied by Backups?

Symptom

The size of a disk backup is much greater than the used space of the disk displayed on a server. Even if you delete large files from the disk and back up the disks again, the backup size does not reduce significantly.

Possible Cause

After files are deleted from a disk, the data remains though it is no longer available. When you use CBR to back up a disk, all disk data including the invisible data will be backed up. For the backup principles, see [12.1.4 Why Is My Backup Size Larger Than My Disk Size?](#).

Solution

Currently, CBR cannot help reduce the backup size. You can use a third-party tool to do this but need to evaluate the security of the tool by yourself.

12.2.13 How Do I View the Size of Each Backup?

You cannot view the size of each backup.

However, you can view the size of all backups for each resource. On the **Backups** tab page, click the name of the target backup to view its details.

12.2.14 How Do I View My Backup Data?

You can check your backup data in the following ways:

NOTE

Backup data cannot be viewed on the CBR console.

Server Backups

1. Create an image from a server backup. For details, see [5.4 Using a Backup to Create an Image](#).
2. Use the image to create a server. For details, see [Creating an ECS from an Image](#).
3. Log in to the server to view the data.

Disk Backups

1. Create a new disk from a disk backup. For details, see [5.5 Using a Backup to Create a Disk](#).
2. Attach the created disk to a server. For details, see [Attaching a Non-Shared Disk](#) or [Attaching a Shared Disk](#).
3. Log in to the server to view the data.

SFS Turbo Backups

1. Create a new SFS Turbo file system from an SFS turbo backup. For details, see [5.6 Using a Backup to Create a File System](#).
2. Mount the file system to a server.
 - To mount the file system to a Linux server, see [Mounting an NFS File System to ECSs \(Linux\)](#).
 - To mount the file system to a Windows server, see [Mounting an NFS File System to ECSs \(Windows\)](#).
3. Log in to the server to view the data.

12.2.15 How Long Will My Backups Be Kept?

Manual backup: The name of a manual backup is usually in the format of **manualbk_**xxxx or is customized. If you do not delete manual backups, manual backups will always be kept.

Automatic backup: The name of an automatic backup is in the format of **autobk_**xxxx. If a retention rule has been set in the policy, automatic backups will be kept and deleted based on the retention rule. If the policy's retention rule has been changed during the backup execution, some automatic backups may not be deleted. For details, see [12.4.2 Why the New Retention Rule I Changed Is Not Applied?](#)

12.3 Restoration

12.3.1 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.

12.3.2 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.

12.3.3 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.

12.3.4 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.

12.3.5 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*.

12.3.6 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 [Passwords](#) in the *Elastic Cloud Server User Guide*.

12.3.7 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.

12.3.8 How Do I Restore Data on the Original Server to a New Server?

You can restore data on your original server to a new server in either of the following ways:

- Method 1:
Create an image using the backup of the original server and then use the image to create a new server. For details, see [5.4 Using a Backup to Create an Image](#).

- Method 2:
If a new server has already been created, perform the following steps:

NOTE

Data consistency is not guaranteed using method 2.

- a. Back up the disks on the original server.
Ensure that all disks on the server are backed up. For how to back up server disks, see [2.3.2 Creating a Cloud Disk Backup](#).
- b. Create new disks from the backups.
Create new disks using their backups one by one. For details, see [5.5 Using a Backup to Create a Disk](#).
- c. Attach the new disks to the new server. For details, see [Attaching a Non-Shared Disk](#) or [Attaching a Shared Disk](#).

12.3.9 How Do I Restore a Data Disk Backup to a System Disk?

You can [use a disk backup to create a new disk](#) and [attach the new disk to a server](#). Then copy data in the data disk to the system disk.

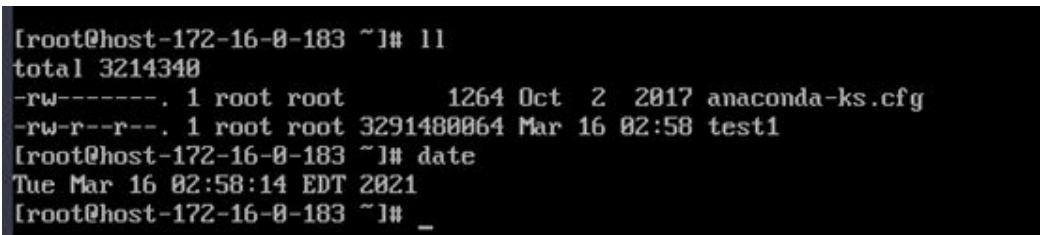
12.3.10 Can I Use CBR to Restore Data to Any Point When the Data Was Backed Up?

Yes. You can do as follows to verify this.

Procedure

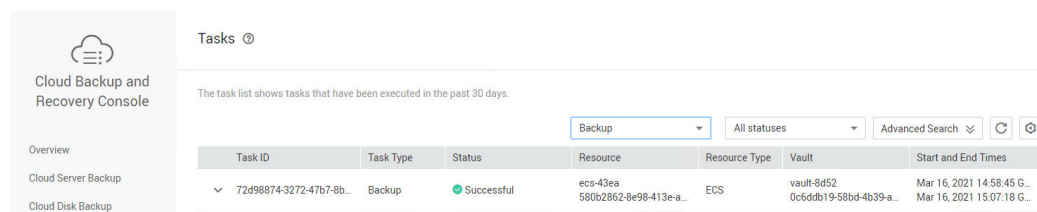
- Step 1** Log in to a server and create a file named **test1**.

Figure 12-2 Viewing the file

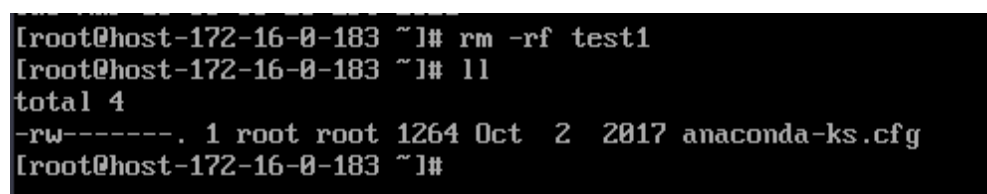


```
[root@host-172-16-0-183 ~]# ll
total 3214348
-rw-----. 1 root root      1264 Oct  2  2017 anaconda-ks.cfg
-rw-r--r--. 1 root root 3291480064 Mar 16 02:58 test1
[root@host-172-16-0-183 ~]# date
Tue Mar 16 02:58:14 EDT 2021
[root@host-172-16-0-183 ~]# _
```

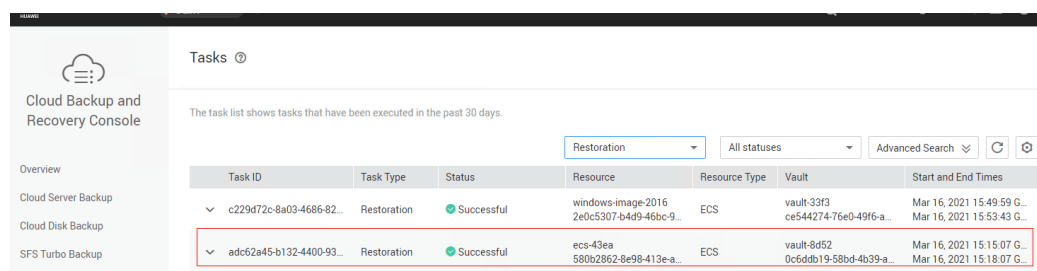
- Step 2** Log in to CBR Console and create a backup for the server.

Figure 12-3 Creating a backup for the server

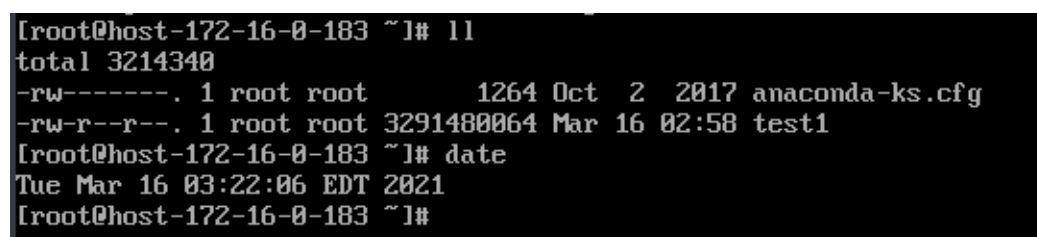
Step 3 Log in to the server again and delete the **test1** file.

Figure 12-4 Deleting the file

Step 4 On CBR Console, use the server backup you created to restore data.

Figure 12-5 Restoring data

Step 5 Log in to the server and confirm that the data has been restored to the state when the backup was created.

Figure 12-6 Confirming the restoration result

----End

12.3.11 Can I Stop an Ongoing Restoration Task?

No. An ongoing restoration task cannot be stopped.

12.4 Policies

12.4.1 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.

12.4.2 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.

12.4.3 How Do I Back Up Multiple Resources at a Time?

1. Log in to 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.

12.4.4 How Do I Retain My Backups Permanently?

Manual Backups

You can permanently keep backups that you manually created as long as you do not delete them and your account balance is sufficient.

Automatic Backups

To keep automatically generated backups permanently, set **Retention Rule** to **Permanent** or set the retention period to **99999** days.

12.4.5 How Can I Cancel Auto Backup?

To cancel auto backup, remove the policy from the vault or disable the policy.

12.4.6 How Can I Have the System Automatically Delete Backups That I No Longer Need?

1. Log in to CBR Console and create a backup vault.
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. Ensure that the vault has enough space to keep all backups automatically generated based on the policies before the retention rule takes effect. Or, auto backup will fail, and the quantity-based retention rule may not take effect. Retention rules are not applied to manual backups.
4. Apply the backup policy to your vault. The system will back up the resources associated with the vault at the specified time and keep backups based on the retention rule.

12.4.7 Why Aren't My Backups Deleted Based on the Retention Rule?

1. The policy applied to the vault is not enabled. Go to the **Policies** page to enable the policy.
2. The policy's retention rule was changed during the backup execution. For details, see [12.4.2 Why the New Retention Rule I Changed Is Not Applied?](#)
3. The backups are created manually. The policy's retention rule does not apply to manual backups. They can only be deleted manually.

12.5 Optimization

12.5.1 What Are Common Problems During Cloud-Init Installation?

You are advised to install Cloud-Init after the restoration to ensure the new server restored by using backups support custom configurations.

To install Cloud-Init, see [Installing Cloud-Init](#).

To configure Cloud-Init, see [Configuring Cloud-Init](#).

This section illustrates the FAQs encountered when installing Cloud-Init and their solutions.

Ubuntu 16.04/CentOS 7: Failed to Set Cloud-Init Automatic Start

- Symptom

After Cloud-Init is installed, run the following command to set Cloud-Init automatic start:

```
systemctl enable cloud-init-local.service cloud-init.service cloud-config.service cloud-final.service
```

Information similar to the following is displayed:

Figure 12-7 Failed to set Cloud-Init automatic start

```
root@ecs-wjq-ubuntu14:~# systemctl enable cloud-init-local.service cloud-init.service cloud-config.service cloud-final.service
Failed to execute operation: Unit file is masked
root@ecs-wjq-ubuntu14:~#
```

- Solution

a. Run the following command:

```
systemctl unmask cloud-init-local.service cloud-init.service cloud-config.service cloud-final.service
```

b. Run the following commands to set automatic start again:

```
systemctl enable cloud-init-local.service cloud-init.service cloud-config.service cloud-final.service
```

c. Run the following commands to check the Cloud-Init status:

```
systemctl status cloud-init-local.service cloud-init.service cloud-config.service cloud-final.service
```

As shown in the following figures, **failed** is displayed and all services are in the **inactive** state.

This is because the address that the system uses to access Cloud-Init is redirected to **/usr/bin/**, but the actual installation path is **/usr/local/bin**.

Figure 12-8 Checking Cloud-Init status

```
root@ecs-wjq-ubuntu14:~# systemctl status cloud-init-local.service
• cloud-init-local.service - Initial cloud-init job (pre-networking)
   Loaded: loaded (/lib/systemd/system/cloud-init-local.service; enabled; vendor
   Active: failed (Result: exit-code) since Fri 2018-08-17 07:12:20 UTC; 1min 25
   Process: 4418 ExecStart=/usr/bin/cloud-init init --local (code=exited, status=
   Main PID: 4418 (code=exited, status=203/EXEC)

Aug 17 07:12:20 ecs-wjq-ubuntu14 systemd[1]: Starting Initial cloud-init job (pr
Aug 17 07:12:20 ecs-wjq-ubuntu14 systemd[1]: cloud-init-local.service: Main proc
Aug 17 07:12:20 ecs-wjq-ubuntu14 systemd[1]: Failed to start Initial cloud-init
Aug 17 07:12:20 ecs-wjq-ubuntu14 systemd[1]: cloud-init-local.service: Unit ente
Aug 17 07:12:20 ecs-wjq-ubuntu14 systemd[1]: cloud-init-local.service: Failed wi
lines 1-11/11 (END)
```

Figure 12-9 Checking Cloud-Init status

```

* cloud-init-local.service - Initial cloud-init job (pre-networking)
   Loaded: loaded (/lib/systemd/system/cloud-init-local.service; enabled; vendor
   preset: enabled)
   Active: failed (Result: exit-code) since Fri 2018-08-17 07:12:20 UTC; 59s ago
   Process: 4418 ExecStart=/usr/bin/cloud-init init --local (code=exited, status=
203/EXEC)
   Main PID: 4418 (code=exited, status=203/EXEC)

Aug 17 07:12:20 ecs-wjq-ubuntu14 systemd[1]: Starting Initial cloud-init job (pr
e-networking)...
Aug 17 07:12:20 ecs-wjq-ubuntu14 systemd[1]: cloud-init-local.service: Main proc
ess exited, code=exited, status=203/EXEC
Aug 17 07:12:20 ecs-wjq-ubuntu14 systemd[1]: Failed to start Initial cloud-init
job (pre-networking).
Aug 17 07:12:20 ecs-wjq-ubuntu14 systemd[1]: cloud-init-local.service: Unit ente
red failed state.
Aug 17 07:12:20 ecs-wjq-ubuntu14 systemd[1]: cloud-init-local.service: Failed wi
th result 'exit-code'.

```

- d. Run the **cp /usr/local/cloud-init /usr/bin/** command to copy the **cloud-init** file to the **usr/bin** directory, and then run the following command to restart Cloud-Init:

```
# systemctl restart cloud-init-local.service cloud-init.service cloud-
config.service cloud-final.service
```

Figure 12-10 Restarting Cloud-Init

```

root@ecs-wjq-ubuntu14: # systemctl start cloud-init-local.service; systemctl sta
tus cloud-init-local.service
* cloud-init-local.service - Initial cloud-init job (pre-networking)
   Loaded: loaded (/lib/systemd/system/cloud-init-local.service; enabled; vendor
   preset: enabled)
   Active: active (exited) since Fri 2018-08-17 07:18:01 UTC; 4ms ago
   Process: 4491 ExecStart=/usr/bin/cloud-init init --local (code=exited, status=
0/SUCCESS)
   Main PID: 4491 (code=exited, status=0/SUCCESS)

Aug 17 07:18:01 ecs-wjq-ubuntu14 cloud-init[4491]: [CLOUDINIT] util.py[DEBUG]: R
Aug 17 07:18:01 ecs-wjq-ubuntu14 cloud-init[4491]: [CLOUDINIT] util.py[DEBUG]: R
Aug 17 07:18:01 ecs-wjq-ubuntu14 cloud-init[4491]: [CLOUDINIT] __init__.py[DEBUG
Aug 17 07:18:01 ecs-wjq-ubuntu14 cloud-init[4491]: [CLOUDINIT] util.py[DEBUG]: R
Aug 17 07:18:01 ecs-wjq-ubuntu14 cloud-init[4491]: [CLOUDINIT] util.py[DEBUG]: R
Aug 17 07:18:01 ecs-wjq-ubuntu14 cloud-init[4491]: [CLOUDINIT] util.py[DEBUG]: F
Aug 17 07:18:01 ecs-wjq-ubuntu14 cloud-init[4491]: [CLOUDINIT] cloud-init[DEBUG]
Aug 17 07:18:01 ecs-wjq-ubuntu14 cloud-init[4491]: [CLOUDINIT] util.py[DEBUG]: R
Aug 17 07:18:01 ecs-wjq-ubuntu14 cloud-init[4491]: [CLOUDINIT] util.py[DEBUG]: R
Aug 17 07:18:01 ecs-wjq-ubuntu14 cloud-init[4491]: [CLOUDINIT] util.py[DEBUG]: c
lines 1-16/16 (END)

```

- e. Run the following commands to check the Cloud-Init status:
- ```
systemctl status cloud-init-local.service cloud-init.service cloud-
config.service cloud-final.service
```

## Ubuntu14.04: chkconfig and systemctl Not Installed

- Symptom  
chkconfig is not installed.
- Solution  
Run the following commands to install chkconfig:  
# apt-get update  
# apt-get install sysv-rc-conf  
# cp /usr/sbin/sysv-rc-conf /usr/sbin/chkconfig

After the installation completes, run the following command to query the Cloud-Init version:

```
cloud-init -v
```

Information similar to the following is displayed:

```
-bash:/usr/bin/cloud-init: not found this command
```

Solution: Run the following command to copy the **cloud-init** file to the **usr/bin** directory:

```
cp /usr/local/bin/cloud-init /usr/bin/
```

## Debian 9.5: Failed to Query the Cloud-Init Version and Set Automatic Start

1. After Cloud-Init is installed, run the following command to query its version:

```
cloud-init -v
```

Information similar to the following is displayed:

```
-bash:/usr/bin/cloud-init: not found this command
```

Solution: Run the **# cp /usr/local/bin/cloud-init /usr/bin/** command to copy the **cloud-init** file to the **usr/bin** directory.

2. Run the **cloud-init init --local** command.

Information similar to the following is displayed:

**Figure 12-11** Information returned when Cloud-Init automatic start is successfully set

```
root@ecs-debian-9:/tmp/CLDUP-INIT/haueicloud-cloud-init# cloud-init init --local
/usr/local/lib/python2.7/dist-packages/Cheetah-2.4.4-py2.7.egg/Cheetah/Compiler.py:1509: UserWarning:
You don't have the C version of NameMapper installed! I'm disabling Cheetah's useStackFrames option as it is painfully slow with
the Python version of NameMapper. You should get a copy of Cheetah with the compiled C version of NameMapper.
"\nYou don't have the C version of NameMapper installed! "
Cloud-init v. 0.7.6 running 'init-local' at Mon, 20 Aug 2018 02:31:45 +0000. Up 704.40 seconds.
root@ecs-debian-9:/tmp/CLDUP-INIT/haueicloud-cloud-init#
```

Cause analysis: The compilation fails because the GNU compiler collection (GCC) is not installed.

Solution

After GCC is installed, run the following command to install Cloud-Init:

```
yum -y install gcc
```

3. After Cloud-Init is installed, run the following command to set Cloud-Init automatic start:

```
systemctl enable cloud-init-local.service cloud-init.service cloud-
config.service cloud-final.service
```

Information similar to the following is displayed:

**Figure 12-12** Failed to set Cloud-Init automatic start

```
Failed to enable unit: Unit file /etc/systemd/system/cloud-init-local.service is masked.
```

Solution

- a. Run the following command:

```
systemctl unmask cloud-init-local.service cloud-init.service cloud-
config.service cloud-final.service
```

- b. Run the following commands to set automatic start again:

```
systemctl enable cloud-init-local.service cloud-init.service cloud-
config.service cloud-final.service
```

- c. Run the following command to restart Cloud-Init:

```
systemctl restart cloud-init-local.service cloud-init.service cloud-
config.service cloud-final.service
```

Run the **systemctl status** command to check the Cloud-Init status.  
Information similar to the following is displayed:

Figure 12-13 Checking the Cloud-Init status

```
cloud-init-local.service - Initial cloud-init job (pre-networking)
Loaded: loaded (/lib/systemd/system/cloud-init-local.service; enabled; vendor preset: enabled)
Active: active (exited) since Mon 2018-08-20 02:48:37 UTC; 6s ago
Process: 1082 ExecStart=/usr/bin/cloud-init init --local (code=exited, status=0/SUCCESS)
Main PID: 1082 (code=exited, status=0/SUCCESS)
Tasks: 0 (limit: 4915)
CGroup: /system.slice/cloud-init-local.service

Aug 20 02:48:37 ecs-debian-9 cloud-init[1082]: [CLOUDINIT] util.py[DEBUG]: Running command ['blkid', '-tLABEL=config-2', '-odev
Aug 20 02:48:37 ecs-debian-9 cloud-init[1082]: [CLOUDINIT] init.py[DEBUG]: Seeing if we can get any data from class 'cloudi
Aug 20 02:48:37 ecs-debian-9 cloud-init[1082]: [CLOUDINIT] util.py[DEBUG]: Reading from /proc/mounts (Quiet=False)
Aug 20 02:48:37 ecs-debian-9 cloud-init[1082]: [CLOUDINIT] util.py[DEBUG]: Read 1947 bytes from /proc/mounts
Aug 20 02:48:37 ecs-debian-9 cloud-init[1082]: [CLOUDINIT] util.py[DEBUG]: Fetched {'depts': {'/dev/pts', 'opts':
Aug 20 02:48:37 ecs-debian-9 cloud-init[1082]: [CLOUDINIT] cloud-init[DEBUG]: No local datasource found
Aug 20 02:48:37 ecs-debian-9 cloud-init[1082]: [CLOUDINIT] util.py[DEBUG]: Reading from /proc/uptime (Quiet=False)
Aug 20 02:48:37 ecs-debian-9 cloud-init[1082]: [CLOUDINIT] util.py[DEBUG]: Read 14 bytes from /proc/uptime
Aug 20 02:48:37 ecs-debian-9 cloud-init[1082]: [CLOUDINIT] util.py[DEBUG]: cloud-init mode 'init' took 0.104 seconds (0.10)
Aug 20 02:48:37 ecs-debian-9 systemd[1]: Started Initial cloud-init job (pre-networking).

cloud-init.service - Initial cloud-init job (metadata service crawler)
Loaded: loaded (/lib/systemd/system/cloud-init.service; enabled; vendor preset: enabled)
Active: active (exited) since Mon 2018-08-20 02:48:40 UTC; 2s ago
Process: 1096 ExecStart=/usr/bin/cloud-init init (code=exited, status=0/SUCCESS)
Main PID: 1096 (code=exited, status=0/SUCCESS)
Tasks: 0 (limit: 4915)
CGroup: /system.slice/cloud-init.service

Aug 20 02:48:40 ecs-debian-9 cloud-init[1096]: [CLOUDINIT] helpers.py[DEBUG]: config-ca-certs already ran (freq=once-per-instanc
Aug 20 02:48:40 ecs-debian-9 cloud-init[1096]: [CLOUDINIT] stages.py[DEBUG]: Running module rsyslog (module 'cloudinit.config.c
Aug 20 02:48:40 ecs-debian-9 cloud-init[1096]: [CLOUDINIT] helpers.py[DEBUG]: config-rsyslog already ran (freq=once-per-instanc
Aug 20 02:48:40 ecs-debian-9 cloud-init[1096]: [CLOUDINIT] stages.py[DEBUG]: Running module users-groups (module 'cloudinit.con
Aug 20 02:48:40 ecs-debian-9 cloud-init[1096]: [CLOUDINIT] helpers.py[DEBUG]: config-users-groups already ran (freq=once-per-ins
Aug 20 02:48:40 ecs-debian-9 cloud-init[1096]: [CLOUDINIT] cloud-init[DEBUG]: Ran 13 modules with 0 failures
Aug 20 02:48:40 ecs-debian-9 cloud-init[1096]: [CLOUDINIT] util.py[DEBUG]: Reading from /proc/uptime (Quiet=False)
Aug 20 02:48:40 ecs-debian-9 cloud-init[1096]: [CLOUDINIT] util.py[DEBUG]: Read 14 bytes from /proc/uptime
Aug 20 02:48:40 ecs-debian-9 cloud-init[1096]: [CLOUDINIT] util.py[DEBUG]: cloud-init mode 'init' took 2.657 seconds (2.66)
Aug 20 02:48:40 ecs-debian-9 systemd[1]: Started Initial cloud-init job (metadata service crawler).

cloud-config.service - Apply the settings specified in cloud-config
Loaded: loaded (/lib/systemd/system/cloud-config.service; enabled; vendor preset: enabled)
Active: active (exited) since Mon 2018-08-20 02:48:41 UTC; 2s ago
Process: 1140 ExecStart=/usr/bin/cloud-init modules --mode=config (code=exited, status=0/SUCCESS)
Main PID: 1140 (code=exited, status=0/SUCCESS)
Tasks: 0 (limit: 4915)
CGroup: /system.slice/cloud-config.service
```

## CentOS 7/Fedora 28: Required C Compiler Not Installed

- Symptom

After Cloud-Init is installed, run the following command:

**cloud-init init --local**

The following information is displayed:

```
/usr/lib/python2.5/site-packages/Cheetah/Compiler.py:1532: UserWarning:
You don't have the C version of NameMapper installed! I'm disabling Cheetah's useStackFrames
option as it is painfully slow with the Python version of NameMapper. You should get a copy of
Cheetah with the compiled C version of NameMapper.
""\nYou don't have the C version of NameMapper installed!
```

- Possible Cause

This alarm is generated because the C version of NameMapper needs to be compiled when installing Cloud-Init. However, GCC is not installed in the system, and the compilation cannot be performed. As a result, the C version of NameMapper is missing.

- Solution

Run the following command to install GCC:

**yum -y install gcc**

Reinstall Cloud-Init.

## CentOS 7/Fedora: Failed to Use the New Password to Log In to the Server Created from a Backup After Cloud-Init Is Successfully Installed

- Symptom

After Cloud-Init is installed, the new password cannot be used to start the new server. After logging in to the server using the old password, you find the NIC is not started.

**Figure 12-14** NIC not started

```
root@ecs-fedora28-wjq-test ~]# ifconfig
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
 inet 127.0.0.1 netmask 255.0.0.0
 inet6 ::1 prefixlen 128 scopeid 0x10<host>
 loop txqueuelen 1000 (Local Loopback)
 RX packets 0 bytes 0 (0.0 B)
 RX errors 0 dropped 0 overruns 0 frame 0
 TX packets 0 bytes 0 (0.0 B)
 TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

- Solution

Log in to the server, open the DHCP configuration file `/etc/sysconfig/network-scripts/ifcfg-ethX`, and comment out `HWADDR`.

## 12.5.2 What Can I Do If Injecting the Key or Password Using Cloud-Init Fails After NetworkManager Is Installed?

A major cause is that the version of Cloud-Init is incompatible with that of NetworkManager. In Debian 9.0 and later versions, NetworkManager is incompatible with Cloud-Init 0.7.9.

### Solution

Uninstall the current version of Cloud-Init and install Cloud-Init 0.7.6 or an earlier version.

For details, see [Installing Cloud-Init](#).

## 12.5.3 What Can Cloud-Init Do?

Cloud-Init initializes specified custom configurations, such as the host name, key, and user data, of a newly created server.

### Installation Methods

If you have restored a server using a backup, it is recommended that you install Cloud-Init or Cloudbase-Init on the server.

- For Windows OSs, download and install Cloudbase-Init.  
For details, see [Installing and Configuring Cloudbase-Init](#).
- For Linux OSs, download and install Cloud-Init.  
To install Cloud-init, see [Installing Cloud-Init](#).  
To configure Cloud-Init, see [Configuring Cloud-Init](#).

## 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.

## 12.6.3 How Do I Delete a Backup That Has Been Used to Create an Image While Retaining the Image?

Use the image to create a server and the server to create another image. Delete the original image and then you can delete the backup.

## 12.6.4 What Can I Do If the Vault Capacity Is Not Enough?

If the storage capacity of a vault is used up, the system will not continue to back up your resources. New backups will never overwrite previous backups. Take the following measures when the storage capacity of your vault is not enough:

1. Locate the target vault and delete unwanted backups by following instructions in [5.3 Deleting a Backup](#).
2. If you want to retain the generated backups, expand the vault capacity. For details, see [4.5 Expanding Vault Capacity](#).
3. If a backup policy has been applied to the vault, disable the backup policy or remove the policy from the vault. To disable the policy, see [6.2 Modifying a Policy](#). To remove the policy, see [6.5 Removing a Policy from a Vault](#). Then, automatic backup is disabled, and the storage capacity of the vault will not change. Alternatively, you can prolong the automatic backup interval or reduce the number of backups to be retained by editing the backup policy, or reduce the number of servers associated with the vault.

## 12.6.5 Will Backup Continue If the Usage of a Vault Reaches the Upper Limit?

If the usage of a vault just reached the upper limit, or has not reached yet but its remaining capacity is insufficient for the next backup, backup can still be executed for once.

However, backup stops once the usage of the vault exceeds the upper limit.

## 12.6.6 Can I Export Disk Backup Data to Another Server?

You can export disk backup data by creating a new disk using a disk backup and then attaching the new disk to a server.

## 12.6.7 Why Do I Need a Vault to Accept the Image Shared to Me?

Before accepting a shared full-ECS image, you need a vault to store the image. Later, this vault is used to store the ECSs provisioned.

An accepted full-ECS image does not occupy the vault space. Do not delete this vault. Or, ECSs will fail to be provisioned using the accepted image.

## 12.6.8 Can I Download Backup Data to a Local PC?

No. CBR backup data cannot be downloaded to a local PC.

## 12.6.9 How Do I Copy Disk Data to Another Account?

If two accounts are in the same region, you can use CBR backup sharing to copy disk data to another account. For details, see [5.2 Sharing a Backup](#). Cross-region backup sharing is currently not supported.

# 13 Troubleshooting Cases

---

[13.1 Failed to Attach Disks](#)

[13.2 Data Disks Are Not Displayed After a Windows Server Is Restored](#)

[13.3 A Server Created Using an Image Enters Maintenance Mode After Login](#)

## 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.

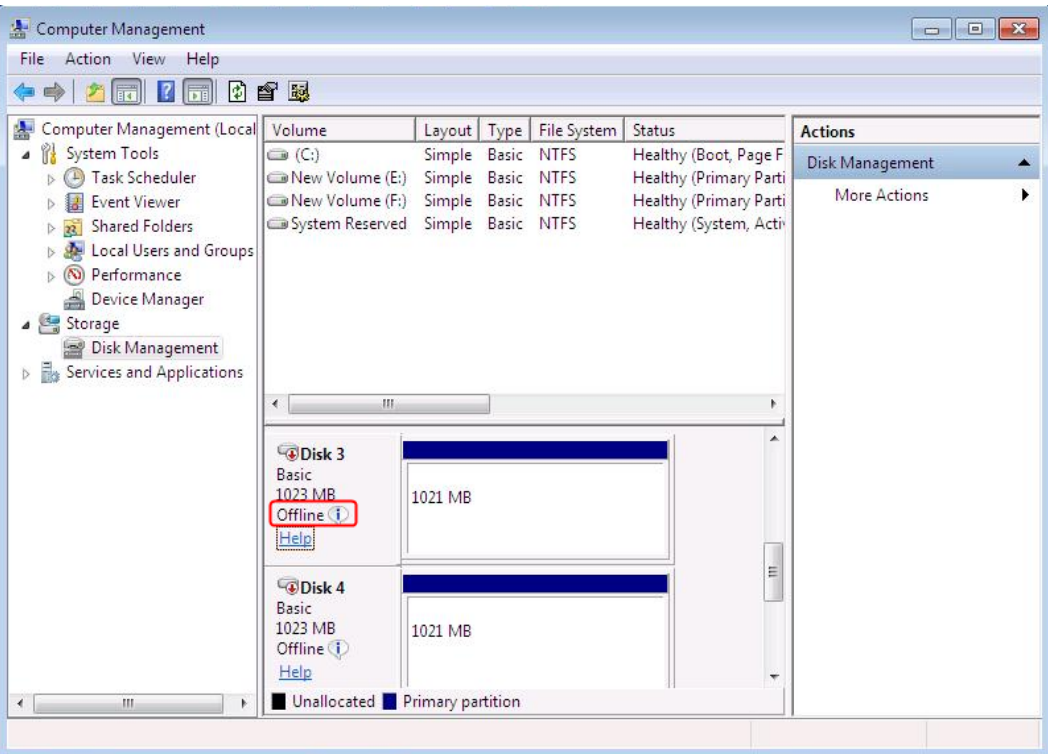
### Possible Cause

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

### Solution

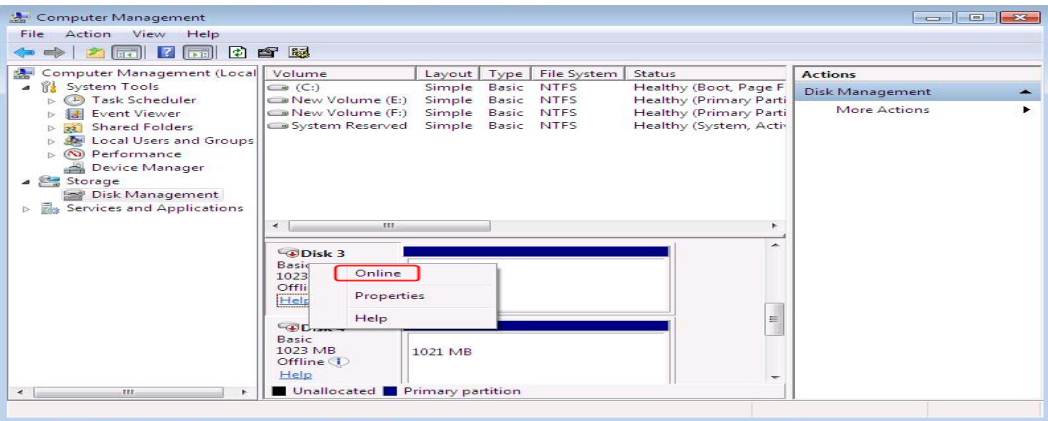
- Step 1** On the Windows desktop, right-click the **My Computer** icon.
- Step 2** Choose **Manage** from the shortcut menu. The **Computer Management** page is displayed.
- Step 3** In the navigation tree, choose **Storage > Disk Management**.  
Data disks are in the offline state, as shown in [Figure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

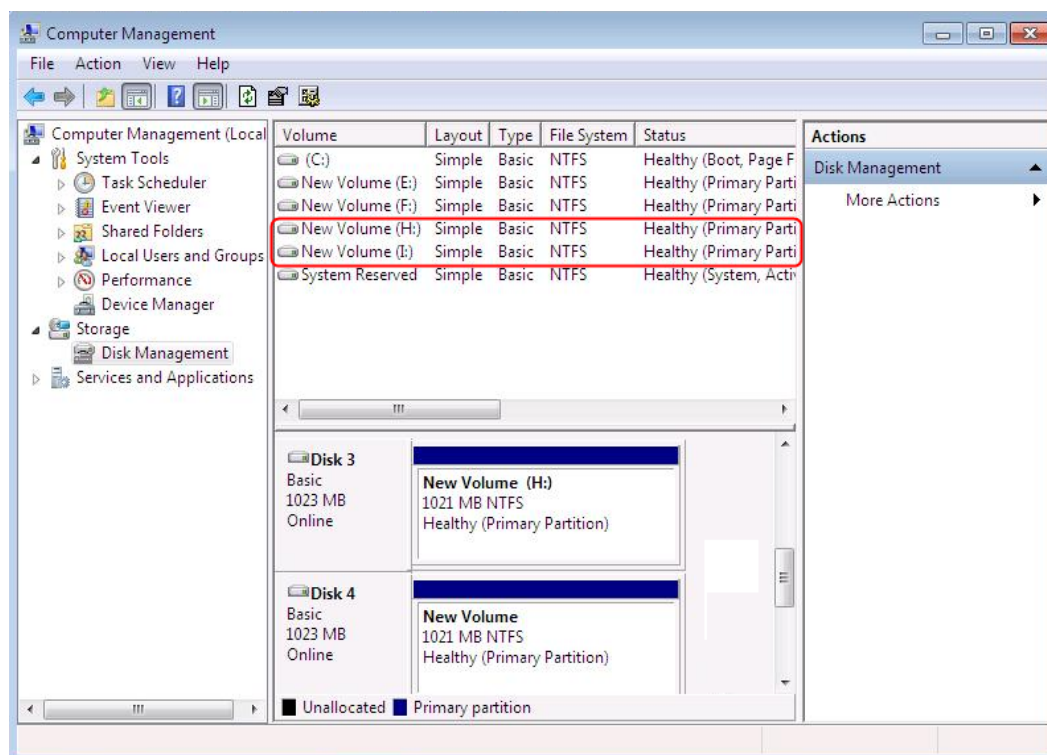
Figure 13-2 Setting a data disk to be online



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 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 13-4** 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 13-5** 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 13-6** /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 13-7 Normal bootstrap 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 13-8 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 13-9 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 13-10 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 ~]# 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

- For O&M security purposes, you are advised to change the user **rdadmin**'s password of the Agent 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 2012. For other versions, change the password according to actual situation.

#### Prerequisites

- You have obtained a username and its password for logging in to the management console.
- 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** Click **User Accounts**. The **User Account Control** dialog box is displayed. Select **rdadmin** and click **Reset Password**.

**Step 4** Enter the new password and click **OK**.

**Step 5** In **Task Manager**, click the **Services** tab and then click **Open Service**.

- Step 6** Select RdMonitor and RdNginx respectively. In the displayed dialog box, select **Login**, change the password to the one entered in [Step 4](#), and click **OK**.

----End

## A.1.2 Changing the Password of the Account for Reporting Alarms (SNMP v3)

To enhance the system O&M security, you are advised to change the password of the account for reporting alarms.

### Prerequisites

- You have obtained a username and its password for logging in to the management console.
- The username and password for logging in to a server have been obtained.

### Context

This section introduces the procedures in Windows and Linux.

#### NOTICE

If the authentication password and data encryption password for SNMP v3 of the Agent are the same, security risks exist. To ensure system security, you are advised to set different passwords for authentication and data encryption.

Obtain the initial authentication password from technical support.

#### NOTE

The password must meet the following complexity requirements:

- Contains 8 to 16 characters.
- Contains at least one of the following special characters: `~!@#\$%^&\*()-\_+=+|[{}];:","<.>/?
- Contains at least two of the following types of characters:
  - Uppercase letters
  - Lowercase letters
  - Numeric characters
- Cannot be the same as the username or the username in reverse order.
- Cannot be the same as the old passwords.
- Cannot contain spaces.

### Procedure (Windows)

- Step 1** Log in to the server where the Agent is installed.
- Step 2** Open the CLI and go to the *installation path\bin* directory.
- Step 3** Run the **agentcli.exe chgsnmp** command. Type the login password of the Agent and press **Enter**.

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

 **NOTE**

**admin** is the username configured during the Agent installation.

**Step 4** Select the SN of the authorization 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 the preceding command is executed, the system remains running even when no operation is performed, which results in security risks. For security purposes, run the **exit** command to exit the system after you finish performing operations.

**Step 3** Run the **su - rdadmin** command to switch to user **rdadmin**.

**Step 4** Run the **/home/rdadmin/Agent/bin/agentcli chgsnmp** command. Type the login password of the Agent 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 authorization 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

- You have obtained a username and its password for logging in to the management console.
- 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 the preceding command is executed, the system remains running even when no operation is performed, which results in security risks. For security purposes, run the **exit** command to exit the system after you finish performing 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*\nginx\conf directory.

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

**Step 6** Copy the new CA certificate file into the *Installation path*\nginx\conf directory and rename the file **bcmagentca.crt**.

**Step 7** Go to the *Installation path*\bin directory.

**Step 8** Run the **agent\_start.bat** script to start the Agent.

-----End

## A.2 Change History

| Released On | Description                                                                                                                                                                                                                                |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2023-08-30  | <p>This issue is the sixth official release, which incorporates the following changes:</p> <ul style="list-style-type: none"><li>• Added multi-AZ redundancy support for vaults.</li><li>• Added support for resource migration.</li></ul> |

| Released On | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2023-05-08  | <p>This issue is the fifth official release, which incorporates the following changes:</p> <ul style="list-style-type: none"> <li>• Added the content about BMS and the link to the <i>Cloud Backup and Recovery API Reference</i> in section "What Is CBR?"</li> <li>• Added section "Advantages."</li> <li>• Added the disk management description and link under cloud disk backup in section "Functions."</li> <li>• Added limitations under "General", "Cloud Disk Backup", "Cloud Server Backup", and "SFS Turbo Backup" in section "Constraints."</li> <li>• Added the description about BMS in section "CBR and Other Services."</li> <li>• Added the content about Instant Restore and enhanced backup in section "CBR Concepts."</li> <li>• Added section "Project and Enterprise Project."</li> <li>• Added the step of adding the vault to an existing enterprise project in sections "Creating a Server Backup Vault" and "Creating a Disk Backup Vault."</li> <li>• Added the description about BMS in section "Creating a Cloud Server Backup."</li> <li>• Added the disk encryption description in section "Creating a Cloud Disk Backup."</li> <li>• Added the description of the frozen status of a vault in section "Viewing a Vault."</li> <li>• Added the description of auto capacity expansion in section "Expanding Vault Capacity."</li> <li>• Added section "Changing Vault Specifications."</li> <li>• Added descriptions of querying backups by enterprise project and exporting the backup list in section "Querying a Vault."</li> <li>• Added descriptions and reference links about image deletion and subsequent operations in section "Sharing a Backup."</li> <li>• Added constraints in section "Restoring from a Cloud Disk Backup."</li> <li>• Added conceptual FAQs "What Are the Differences Between Backups and Images?" and "Why Does the Used Capacity of a Vault Change Only Slightly After I Deleted Unwanted Backups?"</li> <li>• Added backup FAQs "Can I Back Up Two Disks to One Target Disk?", "How Do I Replicate a Disk to the Same AZ in a Region as the Source Disk?", "How Many Backups Can I Create for a Resource?", "How Do I Reduce the Vault Space Occupied by Backups?", "How Do I View the Size of Each Backup?", "How Do I View My Backup Data?", and "How Long Will My Backups Be Kept?"</li> </ul> |

| Released On | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|             | <ul style="list-style-type: none"> <li>Added restoration FAQs "How Do I Restore Data on the Original Server to a New Server?", "How Do I Restore a Data Disk Backup to a System Disk?", and "Can I Use CBR to Restore Data to Any Point When the Data Was Backed Up?"</li> <li>Added policy FAQs "How Do I Retain My Backups Permanently?", "How Can I Cancel Auto Backup?", "How Can I Have the System Automatically Delete Backups That I No Longer Need?", and "Why Aren't My Backups Deleted Based on the Retention Rule?"</li> <li>Added reference links in optimization FAQs "What Are Common Problems During Cloud-Init Installation?", "What Can I Do If Injecting the Key or Password Using Cloud-Init Fails After NetworkManager Is Installed?", and "What Can Cloud-Init Do?"</li> <li>Added other FAQs "How Do I Delete a Backup That Has Been Used to Create an Image While Retaining the Image?", "What Can I Do If the Vault Capacity Is Not Enough?", "Will Backup Continue If the Usage of a Vault Reaches the Upper Limit?", "Can I Export Disk Backup Data to Another Server?", "Why Do I Need a Vault to Accept the Image Shared to Me?", "Can I Download Backup Data to a Local PC?", and "How Do I Copy Disk Data to Another Account?"</li> <li>Added appendix sections "Changing the Password of User rdadmin", "Changing the Password of the Account for Reporting Alarms (SNMP v3)", "Replacing the Server Certificate", and "Replacing CA Certificates."</li> </ul> |
| 2022-08-10  | <p>This issue is the fourth official release, which incorporates the following change:</p> <p>Added section "Monitoring."</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| 2021-09-30  | <p>This issue is the third official release, which incorporates the following change:</p> <p>Added descriptions of permission management.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| 2021-02-08  | <p>This issue is the second official release, which incorporates the following change:</p> <p>Added descriptions of SFS Turbo backup.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| 2020-02-26  | <p>This issue is the first official release.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |