

Cloud Backup and Recovery

Getting Started

Issue 01
Date 2022-09-30



Copyright © Huawei Technologies Co., Ltd. 2023. All rights reserved.

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

Trademarks and Permissions



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

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

Notice

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

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

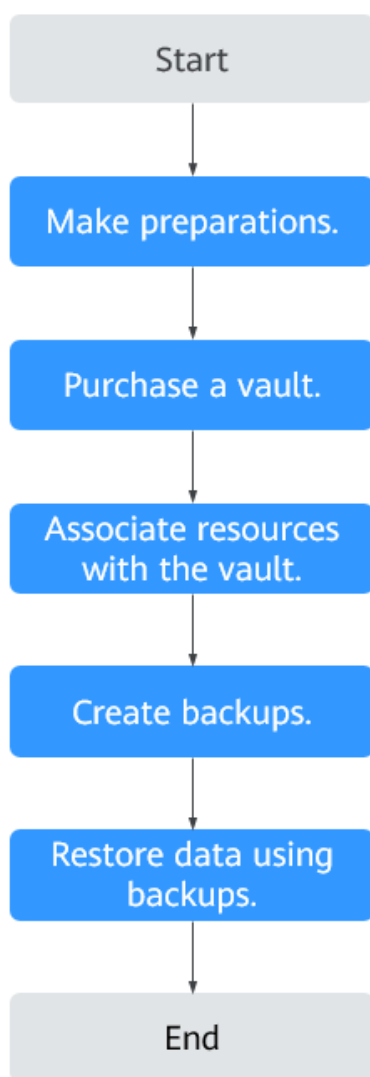
Contents

1 Overview.....	1
2 Step 1: Make Preparations.....	3
3 Step 2: Purchase a Vault.....	5
3.1 Purchasing a Server Backup Vault.....	5
3.2 Purchasing a Disk Backup Vault.....	8
3.3 Purchasing an SFS Turbo Backup Vault.....	10
4 Step 3: Associate a Resource with the Vault.....	13
5 Step 4: Create a Backup.....	15
5.1 Creating a Cloud Server Backup.....	15
5.2 Creating a Cloud Disk Backup.....	17
5.3 Creating an SFS Turbo Backup.....	20
6 Change History.....	23

1 Overview

This section describes how to use CBR to back up cloud servers, cloud disks, on-premises servers, and file systems. The following figure illustrates the process.

Figure 1-1 Backup process



1. Register with Huawei Cloud and top up the account. For details, see [2 Step 1: Make Preparations](#).
2. Purchase a backup vault of the right type based on the resources you want to protect. See the following sections for more information:
 - [3.1 Purchasing a Server Backup Vault](#)
 - [3.2 Purchasing a Disk Backup Vault](#)
 - [3.3 Purchasing an SFS Turbo Backup Vault](#)
3. Associate resources with the vault if you have not done so during vault purchase. For details, see [4 Step 3: Associate a Resource with the Vault](#).
4. Create backups for the associated resources. Backups are stored in vaults. See the following sections for more information:
 - [5.1 Creating a Cloud Server Backup](#)
 - [5.2 Creating a Cloud Disk Backup](#)
 - [5.3 Creating an SFS Turbo Backup](#)
5. Use backups to restore the resources from virus attacks or accidental deletion. See the following sections for more information:
 - [Restoring from a Cloud Server Backup](#)
 - [Restoring from a Cloud Disk Backup](#)

2 Step 1: Make Preparations

Before using CBR, make the following preparations:

- [Registering with Huawei Cloud](#)
- [Creating an IAM User](#)

Registering with Huawei Cloud

If you already have a Huawei Cloud account, skip this part. If you do not have a Huawei Cloud account, perform the following steps to create one:

1. Visit www.huaweicloud.com/eu/ and click **Register**.
2. On the displayed page, register an account as prompted.

After the registration is complete, you will be redirected to your personal information page.

Creating an IAM User

If you want to allow multiple users to manage your resources without sharing your password or private key, you can create IAM users and grant permissions to the users. These users can use specified links and their own accounts to access the public cloud and help you manage resources efficiently. You can also configure account security policies to ensure the security of these accounts.

If you have registered with the public cloud but have not created an IAM user, you can create one on the IAM console. For example, to create a CBR administrator, perform the following steps:

1. Enter your username and password to log in to the management console.
2. Hover the mouse over the username in the upper right corner and choose **Identity and Access Management** from the drop-down list.
3. In the navigation pane on the left, choose **Users**.
4. On the **Users** page, click **Create User**.
5. Enter user information on the **Create User** page.
 - **Username**: Enter a username, for example, **cbr_admin**.
 - **Email Address**: Email address of the IAM user. This parameter is mandatory if the access type is specified as **Set by user**.

- (Optional) **Mobile Number**: Mobile number of the IAM user.
 - (Optional) **Description**: Enter the description of the user, for example, **CBR administrator**.
6. Select **Management console access** for **Access Type** and **Set now** for **Password**. Enter a password and click **Next**.

 **NOTE**

A CBR administrator can log in to the management console and manage users. You are advised to select **Set now** for **Password Type** when you create a CBR administrator for your domain. If you create a CBR administrator for other users, you are advised to select **Set by user** for **Password Type** instead so that the users can set their own password.

7. (Optional) Add the user to the **admin** user group and click **Create**.

User group **admin** has all the operation permissions. If you want to grant fine-grained permissions to IAM users, see [Creating a User and Granting CBR Permissions](#).

The user is displayed in the user list. You can click the IAM user login link to log in to the console.

3 Step 2: Purchase a Vault

[3.1 Purchasing a Server Backup Vault](#)

[3.2 Purchasing a Disk Backup Vault](#)



[3.3 Purchasing an SFS Turbo Backup Vault](#)

3.1 Purchasing a Server Backup Vault

This section describes how to purchase 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 your region and project.
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 **Buy Server Backup Vault**.

Step 3 Select a protection type.

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

Step 4 (Optional) In the server list, select the servers or disks you want to back up. After the servers or disks are selected, they are added to the list of selected servers. See [Figure 3-1](#). You can also select specific disks on a server and associate them with the vault.

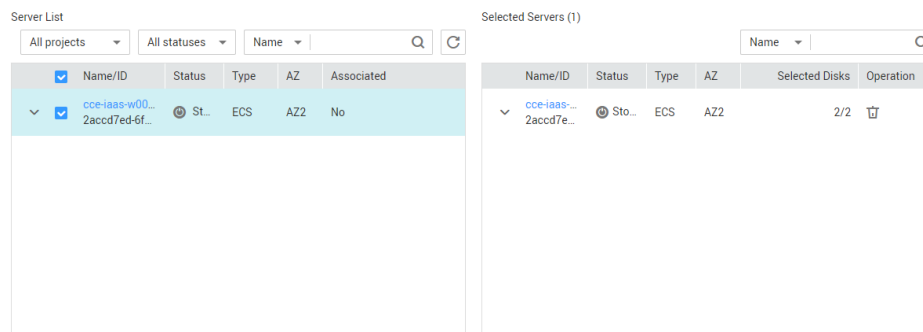
NOTICE

To avoid data inconsistency after restoration, you are advised to back up the entire server.

If you want to back up only some of the disks to reduce costs, ensure that the data on the backed up disks does not depend on the disks that are not backed up. Or, data inconsistency may occur.

For example, the data of an Oracle database is scattered across different disks. If only some of the disks are backed up, restoration restores only the data of the disks that have been backed up, with data on the rest of the disks unchanged. As a result, the data may be inconsistent and the Oracle database may fail to start.

Figure 3-1 Selecting servers



NOTE

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

Step 5 Specify a vault capacity ranging from 10 GB to 10,485,760 GB. **Properly plan the vault capacity**, which must be at least the same as the size of the servers you want to back up. Also, if a backup policy is applied to the vault, more capacity is required.

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

Step 6 Configure auto backup.

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

Figure 3-2 Configuring auto backup

Step 7 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 8 (Optional) Add tags to the vault.

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

Table 3-1 describes the parameters of a tag.

Table 3-1 Tag parameter description

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

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 payment 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 [Vault Management](#).



----End

3.2 Purchasing a Disk Backup Vault

This section describes how to purchase a disk backup vault.

Procedure

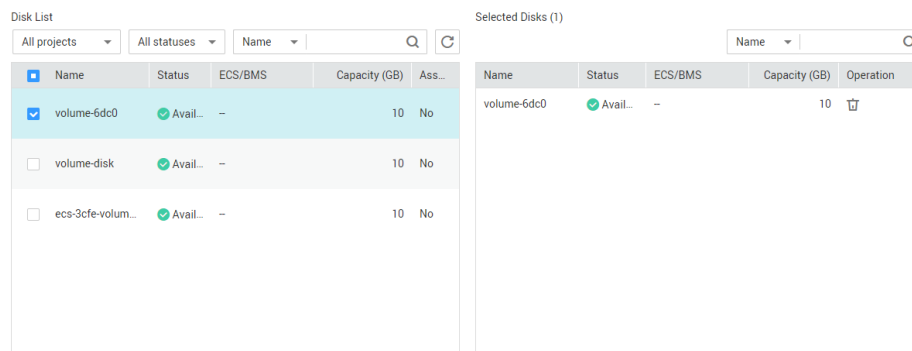
Step 1 Log in to CBR Console.

1. Log in to the management console.
2. Click  in the upper left corner and select your region and project.
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 **Buy 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 3-3](#).

Figure 3-3 Selecting disks



NOTE

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

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

Step 5 Configure auto backup.

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

Step 6 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 (Optional) Add tags to the vault.

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

[Table 3-2](#) describes the parameters of a tag.

Table 3-2 Tag parameter description

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

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 payment as prompted.

Step 10 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

3.3 Purchasing an SFS Turbo Backup Vault

This section describes how to purchase 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 your region and project.
3. Click  and choose **Storage > Cloud Backup and Recovery > SFS Turbo Backups**.

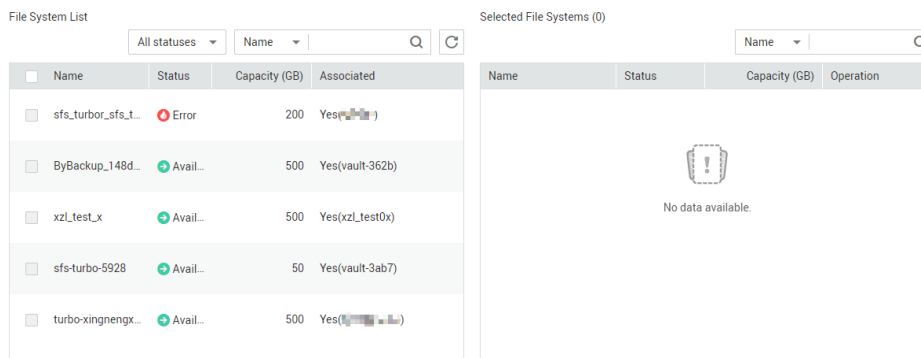
Step 2 In the upper right corner of the page, click **Buy SFS Turbo Backup Vault**.

Step 3 Select a protection type.

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

Step 4 (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 3-4](#).

Figure 3-4 Selecting file systems



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

Step 6 Configure auto backup.

- If you select **Configure**, you must then select an existing backup policy or create a new policy. After the vault is created, CBR will apply the policy to this vault, and all 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 7 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 8 (Optional) Add tags to the vault.

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

Table 3-3 describes the parameters of a tag.

Table 3-3 Tag parameter description

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

Parameter	Description	Example Value
Value	<p>A tag value can be repetitive or left blank.</p> <p>A tag value:</p> <ul style="list-style-type: none"> • Can contain 0 to 43 Unicode characters. • Can contain only letters, digits, hyphens (-), and underscores (_). 	Value_0001

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-612c**.

 **NOTE**

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

Step 10 Complete the payment as prompted.

Step 11 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

4 Step 3: Associate a Resource with the Vault

If you have already associated servers, file systems, or disks when purchasing 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

- The servers you plan to associate with a vault must be in the **Running** or **Stopped** state.
- The disks you plan to associate with a vault must be in the **Available** or **In-use** state.
- The SFS Turbo file systems you plan to associate with a vault must be in the **Available** state.
- 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.

Procedure

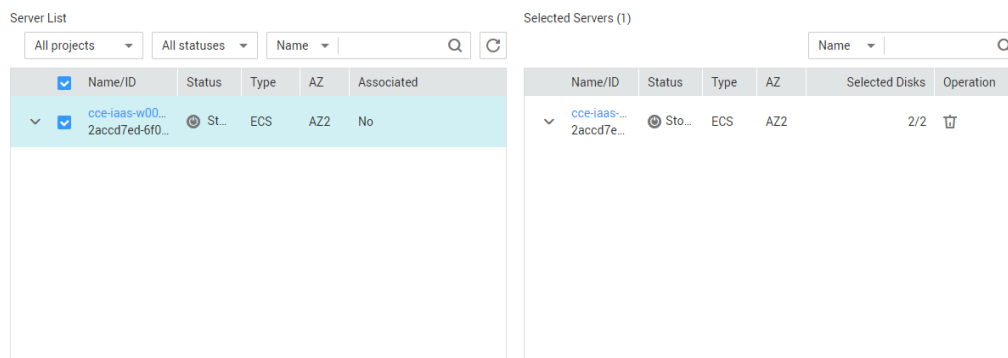
Step 1 Log in to CBR Console.

1. Log in to the management console.
2. Click  in the upper left corner and select your region and project.
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 4-1](#).

Figure 4-1 Associate Server



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

5 Step 4: Create a Backup

[5.1 Creating a Cloud Server Backup](#)

[5.2 Creating a Cloud Disk Backup](#)

[5.3 Creating an SFS Turbo Backup](#)

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

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.

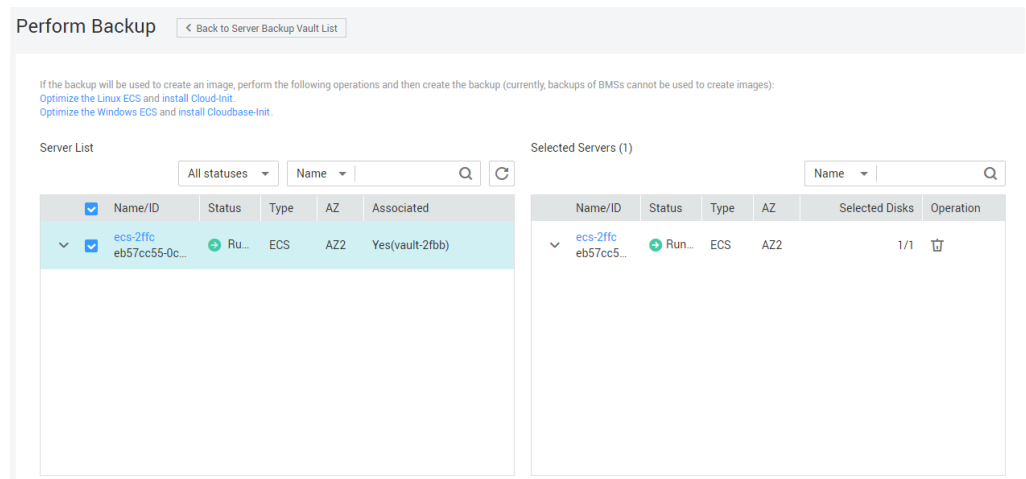
1. Log in to the management console.
2. Click  in the upper left corner and select your region and project.
3. Click  and choose **Storage > Cloud Backup and Recovery**. Select a backup type from the left navigation pane.

Step 2 On the **Cloud Server Backups** page, click the **Vaults** tab and find the vault to which the server is associated.

Step 3 Perform backup in either of the following ways:

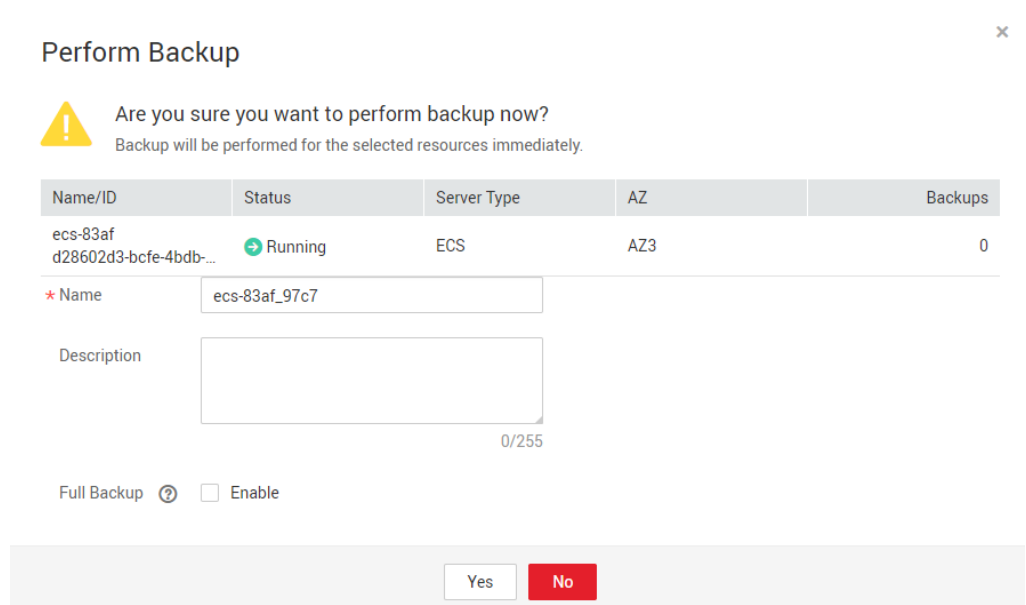
- Choose **More > Perform Backup** in the **Operation** column. In the server list, select the server you want to back up. After a server is selected, it is added to the list of selected servers. See [Figure 5-1](#).

Figure 5-1 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 5-2](#).

Figure 5-2 Perform Backup



Step 4 Set **Name** and **Description** for the backup. [Table 5-1](#) describes the parameters.

Table 5-1 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 5-3](#).

Figure 5-3 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 [Restoring from a Cloud Server Backup](#) and [Using a Backup to Create an Image](#).

----End

5.2 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 disk does not impact the disk performance. To ensure data integrity, you are advised to back up the disk during off-peak hours when no data is written to the disk.

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.

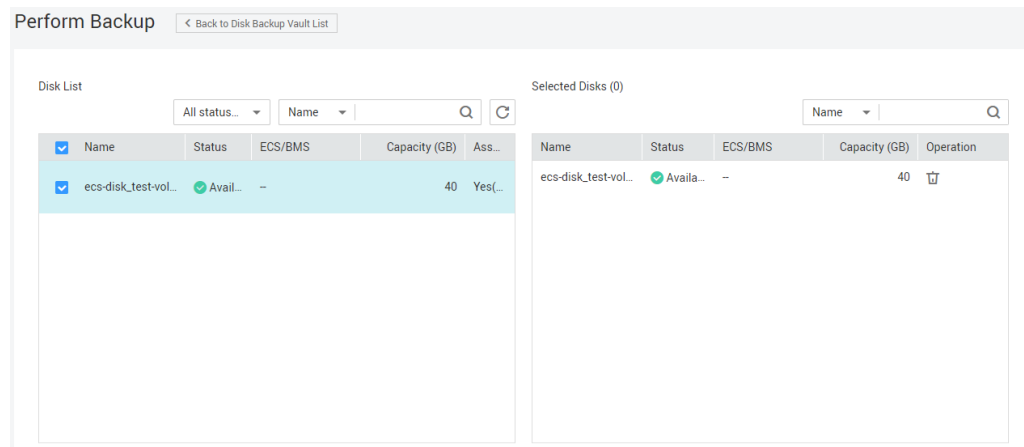
1. Log in to the management console.
2. Click  in the upper left corner and select your region and project.
3. Click  and choose **Storage > Cloud Backup and Recovery**. Select a backup type from the left navigation pane.

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:

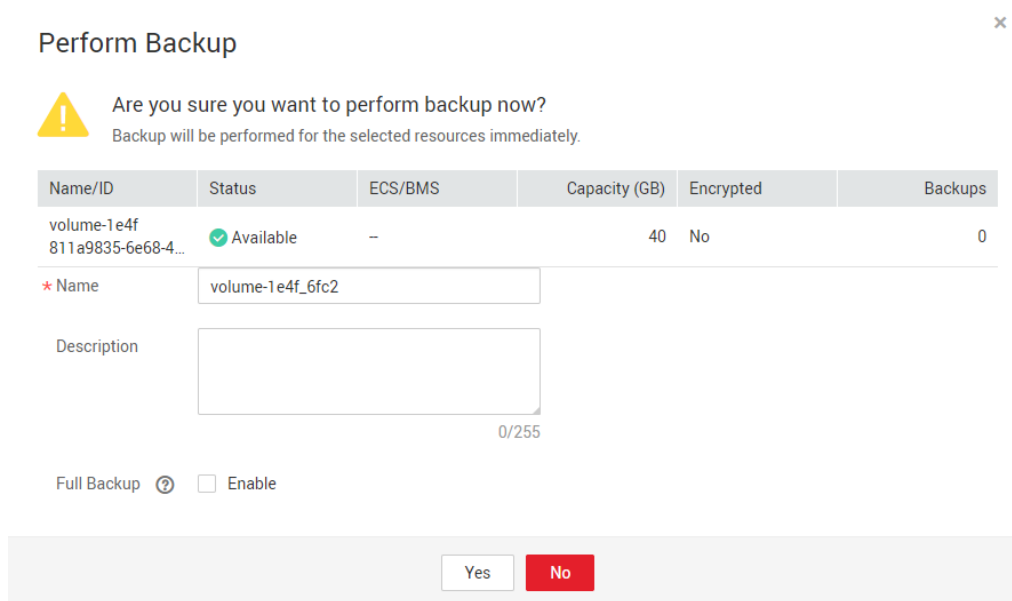
- Click **Perform Backup** in the **Operation** column. In the disk list, select the disk you want to back up. After a disk is selected, it is added to the list of selected disks. See [Figure 5-4](#).

Figure 5-4 Selecting the disk to be backed up



- 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 5-5](#).

Figure 5-5 Perform Backup



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 5-2](#) describes the parameters.

Table 5-2 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 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 5-6](#).

Figure 5-6 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 [Restoring Data Using a Cloud Disk Backup](#).

----End

5.3 Creating an SFS Turbo Backup

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



Backing up an SFS Turbo file system does not impact the file system performance. 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.

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.

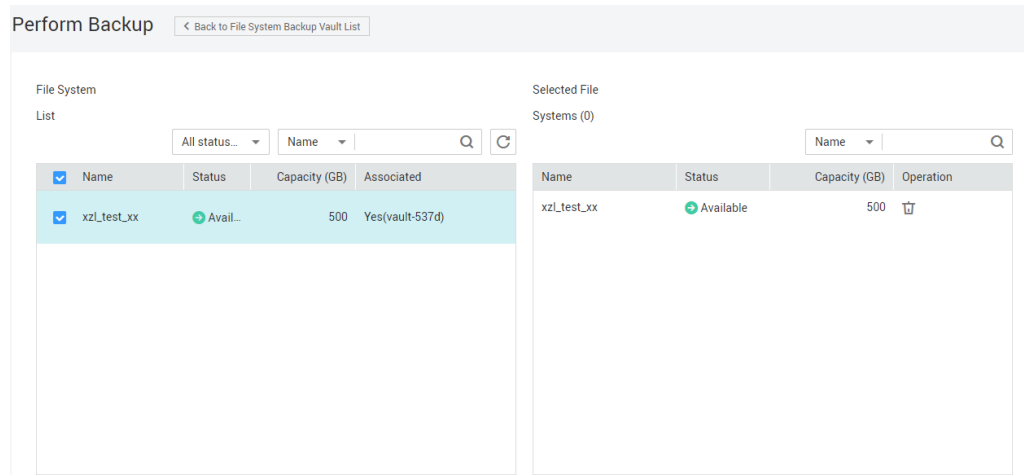
1. Log in to the management console.
2. Click  in the upper left corner and select your region and project.
3. Click  and choose **Storage > Cloud Backup and Recovery > SFS Turbo Backups**.

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:

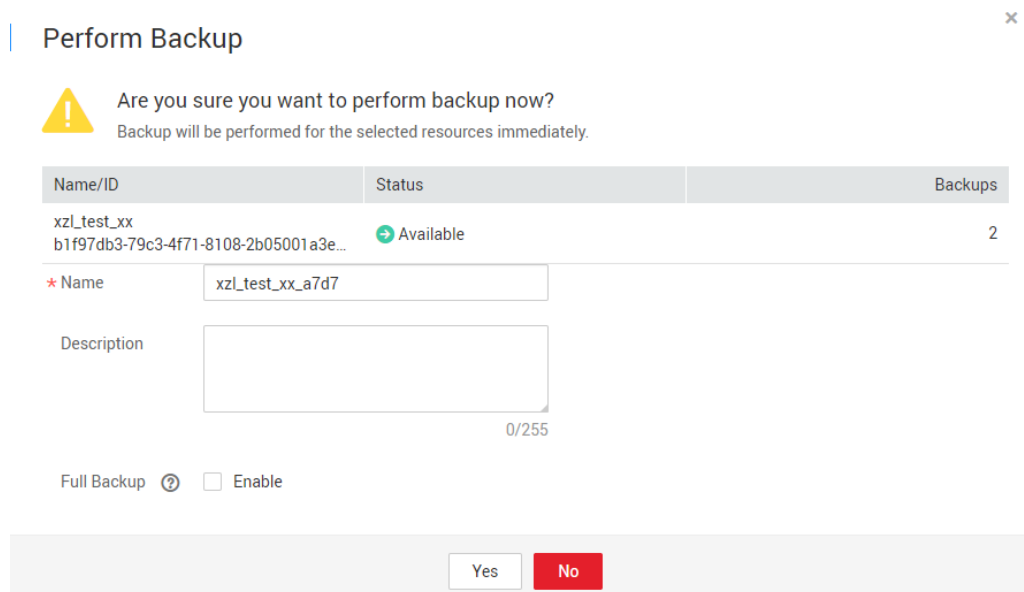
- Choose **More > Perform Backup** in the **Operation** column. In the file system list, select the file system to be backed up. After a file system is selected, it is added to the list of selected file systems. See [Figure 5-7](#).

Figure 5-7 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 5-8](#).

Figure 5-8 Perform Backup



Step 4 Set **Name** and **Description** for the backup. [Table 5-3](#) describes the parameters.

Table 5-3 Parameter description

Parameter	Description	Remarks
Name	<p>Name of the backup you are creating.</p> <p>A name must contain 1 to 64 characters including digits, letters, underscores (_), or hyphens (-).</p> <p>NOTE You can also use the default name manualbk_XXXX.</p> <p>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.</p>	manualbk_d819
Description	<p>Description of the backup.</p> <p>It cannot exceed 255 characters.</p>	--

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

----End

6 Change History

Released On	Description
2022-09-30	This issue is the first official release.