Cloud Backup and Recovery

Getting Started

Issue 03

Date 2022-07-20

HUAWEI

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


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.

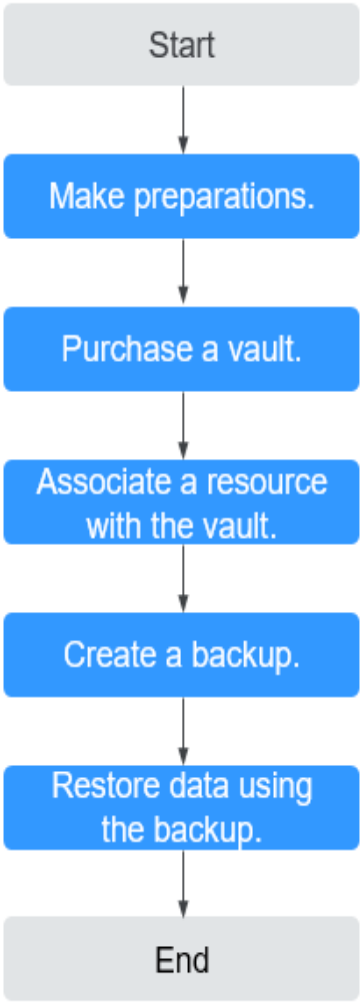
The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Contents

1 Overview

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

Figure 1-1 Backup process



1. Register with Huawei Cloud and top up the account. For details, see **Step 1: Make Preparations**.
2. Purchase a backup vault based on your needs. See the following sections for more information:
   - **Purchasing a Server Backup Vault**
   - **Purchasing a Disk Backup Vault**
   - **Purchasing an SFS Turbo Backup Vault**
   - **Purchasing a Hybrid Cloud Backup Vault**

   After purchasing a hybrid cloud backup vault, perform subsequent operations by referring to **Hybrid Cloud Backup**.
3. Associate resources with the vault if you have not done so. For details, see **Step 3: Associate a Resource with the Vault**.
4. After resources are associated, back up the resources. Generated backups are stored in the vault. See the following sections for more information:
   - **Creating a Cloud Server Backup**
   - **Creating a Cloud Disk Backup**
   - **Creating an SFS Turbo Backup**
   - **Creating File Backups**
5. After resources are successfully backed up, use backups to restore the resources if any data loss occurs due to virus attack or misoperation. See the following sections for more information:
   - **Restoring Data Using a Cloud Server Backup**
   - **Restoring Data Using a Cloud Disk Backup**
   - **Restoring Data Using a Hybrid Cloud Backup**
   - **Restoring Data Using a File Backup**

2 Step 1: Make Preparations

Before using CBR, you need to make the following preparations:

- **Registering with Huawei Cloud**
- **Topping Up an Account**
- **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/intl/en-us/** and click **Register**.
2. On the displayed page, register an account as prompted.

   After you have successfully registered, the system automatically redirects you to your personal information page.

Topping Up an Account

Ensure that your account has sufficient balance.

To view detailed CBR pricing, see **Product Pricing Details**.

To top up an account, see **Topping Up an Account**.

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 select **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

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. Choose **Storage** > **Cloud Backup and Recovery**. Select a backup tab from the left navigation pane.

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

Step 3 Select a billing mode.

- Yearly/monthly is a prepaid billing mode. You are billed based on the subscription duration you specify. This mode provides lower prices and is ideal when the resource use duration is predictable.
- Pay-per-use is a postpaid billing mode. You are billed based on your resource usage. With this mode, you can increase or delete resources at any time. Fees are deducted from your account balance.

Step 4 Select a protection type.

- **Backup**: The created vault is a server backup vault, which stores cloud server backups.
- **Replication**: The created vault is a cloud server replication vault, which stores the replicas of cloud server backups. If you select **Replication**, you do not need to select a server.

For example, if you want to back up a server, select **Backup** for the protection type of the vault. If you want to replicate backups of the server from region 1 to region 2, the destination vault in region 2 must be of the **Replication** protection type.

Step 5 Enable or disable application-consistent backup.

- If application-consistent backup is enabled, the vault can be used to store database backups. Backing up memory data through application-consistent backup ensures application system consistency, which is suitable for ECSs containing MySQL or SAP HANA databases. If an application-consistent backup task fails, the system automatically performs a common server backup task instead. The common server backup will be stored in the application-consistent backup vault.
- If application-consistent backup is disabled, only common server backup is performed on associated servers, which is usually used for ECSs that do not run databases.

Step 6 (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 may also select only some of the disks of a server and associate them with the vault.

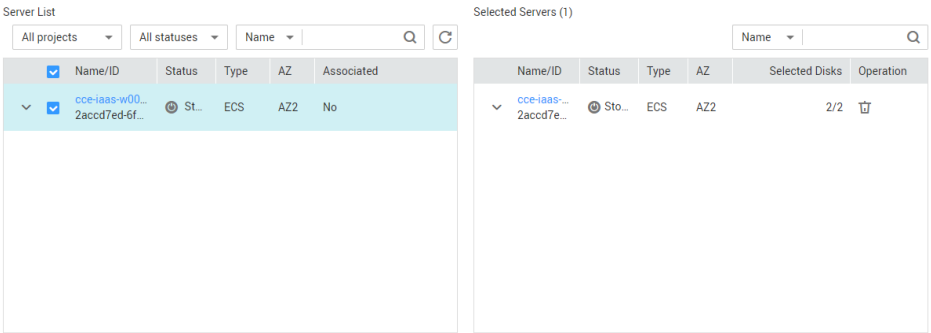
NOTICE

To ensure post-restoration data consistency, 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 the rest of the data unchanged. As a result, the data may be inconsistent and applications may fail to start.

Figure 3-1 Selecting servers



NOTE

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

Step 7 Specify the vault capacity, which ranges from 10 GB to 10,485,760 GB. You need to **properly plan the vault capacity**, which must be at least the same as the size of the servers you want to back up. Also, if automatic association is enabled and a backup policy is applied to the vault, more capacity is required.

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

Step 8 Determine whether to 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, the system 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 it.

Step 9 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 project name is **default**.

NOTE

If the **CBR FullAccess** policy has been assigned to IAM users, enterprise projects cannot be displayed and selected when you create a vault. Go to the Enterprise Project Management console and assign the **CBR FullAccess** policy to the target user group.

Step 10 (Optional) Configure automatic resource association.

- If you select **Configure**, in the next backup period, unprotected resources will be automatically scanned and associated with the vault, and backups will be automatically executed.
- If you select **Skip**, resources will not be automatically associated with the vault you are creating.

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

Only existing tags can be selected. If no tag is available, create tags on the corresponding resource page. You can select a maximum of 5 tags to search for vaults. If you select more than one tag, the vaults containing any of the specified tags will be returned.

Step 11 (Optional) Add tags to the vault.

A tag is represented in the form of a key-value pair. Tags are used to identify, classify, and search for vaults. Vault tags are used to filter and manage vaults only. A vault can have a maximum of 10 tags.

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 the key or select the key of an existing tag created in TMS. The naming rules for a tag key are as follows: • It contains 1 to 36 Unicode characters. • It can contain only letters, digits, hyphens (-), and underscores (_).	Key_0001
Value	A tag value can be repetitive or left blank. The naming rules for a tag value are as follows: • It contains 0 to 43 Unicode characters. • It can contain only letters, digits, hyphens (-), and underscores (_).	Value_0001

Step 12 Specify a name for the vault.

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

NOTE

You can use the default name, which is in the format of **vault**_*xxxx*.

Step 13 Specify the required duration if you select yearly/monthly billing. The validity period ranges from 1 month to 5 years.

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

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

Step 14 Pay for the order as prompted.

Step 15 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. Choose **Storage** > **Cloud Backup and Recovery**. Select a backup tab from the left navigation pane.

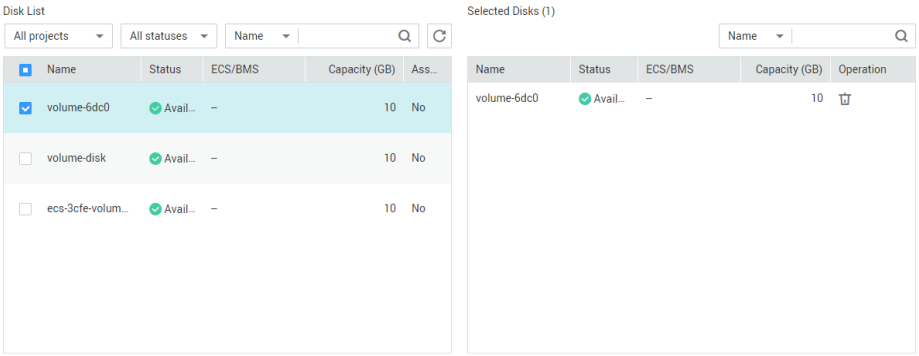
Step 2 In the upper right corner of the page, click **Buy Disk Backup Vault**.

Step 3 Select a billing mode.

- Yearly/monthly is a prepaid billing mode. You are billed based on the subscription duration you specify. This mode provides lower prices and is ideal when the resource use duration is predictable.
- Pay-per-use is a postpaid billing mode. You are billed based on your resource usage. With this mode, you can increase or delete resources at any time. Fees are deducted from your account balance.

Step 4 (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 3-2**.

Figure 3-2 Selecting disks



NOTE

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

Step 5 Specify the vault capacity. This capacity indicates the total size of the disks that you want to associate with this vault. You need to **properly plan the vault capacity**, which must be at least the same as the size of the disks you want to back up. The capacity ranges from 10 GB to 10485760 GB.

Step 6 Determine whether to 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, the system 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 it.

Step 7 (Optional) Configure automatic resource association.

- If you select **Configure**, in the next backup period, unprotected resources will be automatically scanned and associated with the vault, and backups will be automatically executed.
- If you select **Skip**, resources will not be automatically associated with the vault you are creating.

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

Only existing tags can be selected. If no tag is available, create tags on the corresponding resource page. You can select a maximum of 5 tags to search for vaults. If you select more than one tag, the vaults containing any of the specified tags will be returned.

Step 8 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 project name is **default**.

NOTE

If the **CBR FullAccess** policy has been assigned to IAM users, enterprise projects cannot be displayed and selected when you create a vault. Go to the Enterprise Project Management console to add the permissions.

Step 9 (Optional) Add tags to the vault.

A tag is represented in the form of a key-value pair. Tags are used to identify, classify, and search for vaults. Vault tags are used to filter and manage vaults only. A vault can have a maximum of 10 tags.

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 the key or select the key of an existing tag created in TMS. The naming rules for a tag key are as follows: • It contains 1 to 36 Unicode characters. • It can contain only letters, digits, hyphens (-), and underscores (_).	Key_0001
Value	A tag value can be repetitive or left blank. The naming rules for a tag value are as follows: • It contains 0 to 43 Unicode characters. • It can contain only letters, digits, hyphens (-), and underscores (_).	Value_0001

Step 10 Specify a name for the vault.

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

NOTE

You can use the default name, which is in the format of **vault**_*xxxx*.

Step 11 Specify the required duration if you select yearly/monthly billing. The validity period ranges from 1 month to 5 years.

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

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

Step 12 Pay for the order as prompted.

Step 13 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. 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 billing mode.

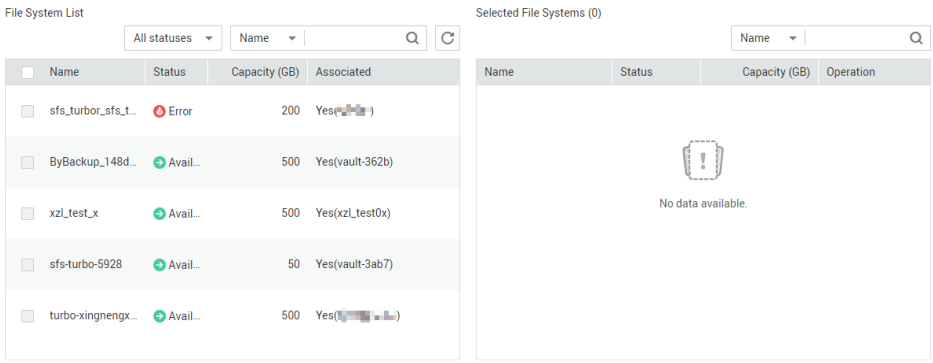
- Yearly/monthly is a prepaid billing mode. You are billed based on the subscription duration you specify. This mode provides lower prices and is ideal when the resource use duration is predictable.
- Pay-per-use is a postpaid billing mode. You are billed based on your resource usage. With this mode, you can increase or delete resources at any time. Fees are deducted from your account balance.

Step 4 Select a protection type.

- **Backup**: The created vault is an SFS Turbo backup vault, which stores backups of SFS Turbo file systems.
- **Replication**: The created vault is an SFS Turbo replication vault, which stores the replicas of SFS Turbo file system backups. If you select **Replication**, you do not need to select an SFS Turbo file system.

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 3-3**.

Figure 3-3 Selecting file systems



NOTE

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

Step 6 Specify the vault capacity. This capacity indicates the total size of the file systems that you want to associate with this vault. You need to **properly plan the vault**

capacity, which must be at least the same as the size of the file systems you want to back up. The capacity ranges from 10 GB to 10485760 GB.

Step 7 Determine whether to 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, the system 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 it.

Step 8 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 project name is **default**.

NOTE

If the **CBR FullAccess** policy has been assigned to IAM users, enterprise projects cannot be displayed and selected when you create a vault. Go to the Enterprise Project Management console to add the permissions.

Step 9 (Optional) Add tags to the vault.

A tag is represented in the form of a key-value pair. Tags are used to identify, classify, and search for vaults. Vault tags are used to filter and manage vaults only. A vault can have a maximum of 10 tags.

Table 3-3 describes the parameters of a tag.

Table 3-3 Tag parameter description

Parameter	Description	Example Value
Key	Each tag has a unique key. You can customize the key or select the key of an existing tag created in TMS. The naming rules for a tag key are as follows: • It contains 1 to 36 Unicode characters. • It can contain only letters, digits, hyphens (-), and underscores (_).	Key_0001
Value	A tag value can be repetitive or left blank. The naming rules for a tag value are as follows: • It contains 0 to 43 Unicode characters. • It can contain only letters, digits, hyphens (-), and underscores (_).	Value_0001

Step 10 Specify a name for the vault.

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

NOTE

You can use the default name, which is in the format of **vault**_*xxxx*.

Step 11 Specify the required duration if you select yearly/monthly billing. The validity period ranges from 1 month to 5 years.

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

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

Step 12 Pay for the order as prompted.

Step 13 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

3.4 Purchasing a Hybrid Cloud Backup Vault

This section describes how to purchase a hybrid cloud backup vault.

Hybrid cloud backup vaults can be used to store file backups, storage backups, and VMware backups. Buy a hybrid cloud backup vault that suits your needs. For more information, see **File Backup** and **Hybrid Cloud 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 your region and project.
3. Choose **Storage** > **Cloud Backup and Recovery** > **Hybrid Cloud Backups**.

Step 2 Select a type of hybrid cloud backup. In the upper right corner of the page, click **Buy Hybrid Cloud Backup Vault**.

Step 3 Select a billing mode.

- Yearly/monthly is a prepaid billing mode. You are billed based on the subscription duration you specify. This mode provides lower prices and is ideal when the resource use duration is predictable.
- Pay-per-use is a postpaid billing mode. You are billed based on your resource usage. With this mode, you can increase or delete resources at any time. Fees are deducted from your account balance.

Step 4 Select a protection type.

- **Backup**: The created vault is a backup vault which stores backups.

- **Replication**: The created vault is a replication vault which stores backup replicas.

Step 5 Specify the vault capacity. The vault capacity cannot be less than the size of the server to be backed up. The value ranges from 1 to 10240, and the unit is TB.

Step 6 (Optional) Add tags to the vault.

A tag is represented in the form of a key-value pair. Tags are used to identify, classify, and search for vaults. Vault tags are used to filter and manage vaults only. A vault can have a maximum of 10 tags.

Table 3-4 describes the parameters of a tag.

Table 3-4 Tag parameter description

Parameter	Description	Example Value
Key	Each tag has a unique key. You can customize the key or select the key of an existing tag created in TMS. The naming rules for a tag key are as follows: • It contains 1 to 36 Unicode characters. • It can contain only letters, digits, hyphens (-), and underscores (_).	Key_0001
Value	A tag value can be repetitive or left blank. The naming rules for a tag value are as follows: • It contains 0 to 43 Unicode characters. • It can contain only letters, digits, hyphens (-), and underscores (_).	Value_0001

Step 7 Specify a name for the vault.

A name must contain 1 to 64 characters including digits, letters, underscores (_), or hyphens (-), for example, **vault-98c8**.

NOTE

You can use the default name, which is in the format of **vault**_*xxxx*.

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

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

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

Step 9 Pay for the order as prompted.

Step 10 Go back to the file backup or hybrid cloud backup page. You can see the created vault in the vault list.

You can expand the vault capacity. For details, see **Vault Management**.

----End

Follow-up Procedure

After a hybrid cloud backup vault is available, you can synchronize the backup data for restoration and service deployment on the cloud. However, you cannot directly perform hybrid cloud backup on CBR Console.

For detailed hybrid cloud backup operations, see **Hybrid Cloud Backup**.

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.

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

File backup does not require resource association. You only need to install the Agent and configure backup. For more information, see **File Backup Process**.

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 to be associated must be in the same region.
- The total capacity of the resources to be associated cannot be greater than the capacity of the vault.

Procedure

Step 1 Log in to CBR Console.

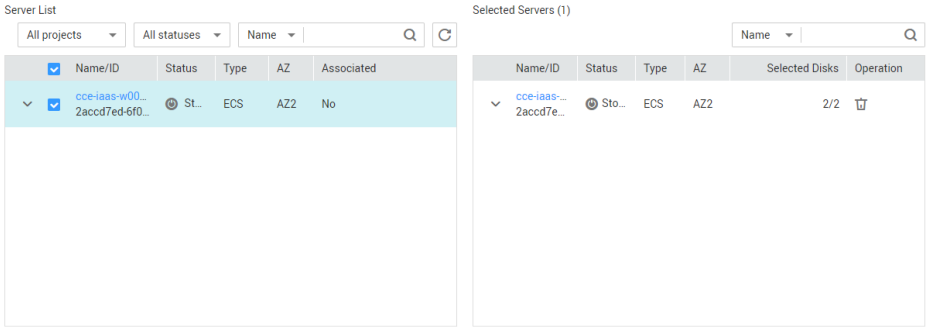
1. **Log in to the management console**.
2. Click  in the upper left corner and select your region and project.

3. Choose **Storage** > **Cloud Backup and Recovery**. Select a backup tab 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 in the **Associated Servers** column in the vault list, you can view the number of resources that have been successfully associated.

NOTE

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

----End

Automatic Association

Backup vaults support automatic association with resources that are not backed up. After successful association, resources will be backed up according to the backup policy applied to the vault.

- You can enable automatic association only when the vault's remaining capacity is greater than 40 GB. Remaining capacity of a vault = Total capacity of the vault - Capacity of resources associated with the vault. You can obtain the vault capacity and associated capacity in the **Basic Information** area on the details page of the vault. Specifically, if the capacity of a server backup vault is 800 GB and it has been associated with two 100 GB servers, the remaining capacity is 600 GB (800 GB – 200 GB). In this case, you can enable automatic association.
- If multiple vaults are enabled with automatic association, the system scans their backup policies and associates resources with the vault whose next scheduled backup time is the earliest.

- When the capacity of the vault selected by the system is used up, resources will be associated with the vault whose next scheduled backup time is the second earliest.
- If a backup policy with the earliest scheduled backup time is applied to more than one vault, the system randomly associates the resources with one of these vaults.
- If a vault is enabled with automatic association but no backup policy has been applied to it, no resources will be automatically associated with this vault. You can manually associate resources that have not been backed up with the vault.
- After the automatic association function is disabled for a vault, the vault stops automatically scanning for resources that have not been backed up. The associated resources are not affected.

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. Choose **Storage** > **Cloud Backup and Recovery**.

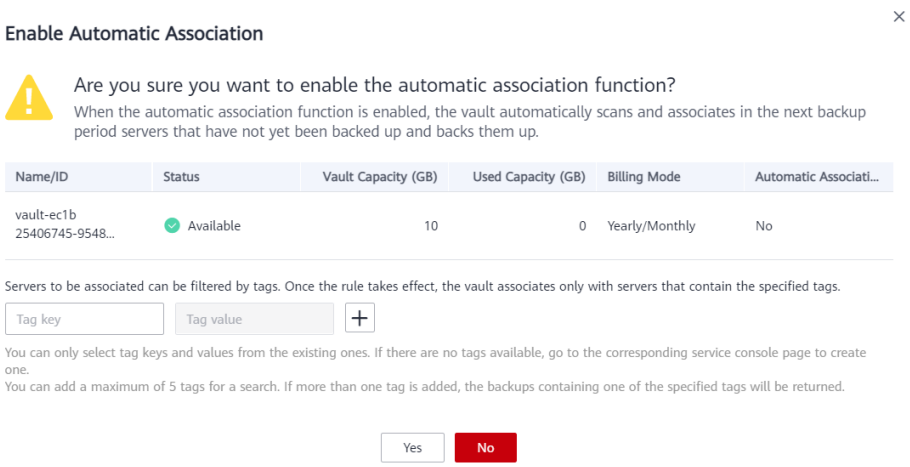
Step 2 On any backup page, locate the target vault.

Step 3 Choose **More** > **Enable Automatic Association** in the **Operation** column of the vault. See **Figure 4-2**.

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

Only existing tags can be selected. If no tag is available, create tags on the corresponding resource page. You can select a maximum of 5 tags to search for vaults. If you select more than one tag, the vaults containing any of the specified tags will be returned.

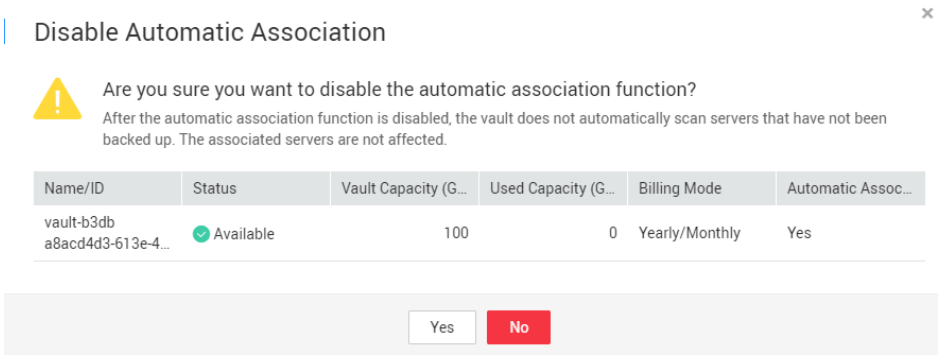
Figure 4-2 Enabling automatic association



Step 4 After the function is enabled, you can see **Automatic association** in the **Associated Servers** column of the vault list.

Step 5 (Optional) If the automatic association function is not required, choose **More** > **Disable Automatic Association** in the **Operation** column of the vault. See **Figure 4-3**.

Figure 4-3 Disabling automatic association



----End

5 Step 4: Create a 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. Then, create an image from the ECS backup and use the image to create an ECS as needed.

During the cloud server backup, the performance of the server is not affected. To ensure data integrity, back up the server during off-peak hours when no write operation is performed on the disks.

Prerequisites

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

Procedure

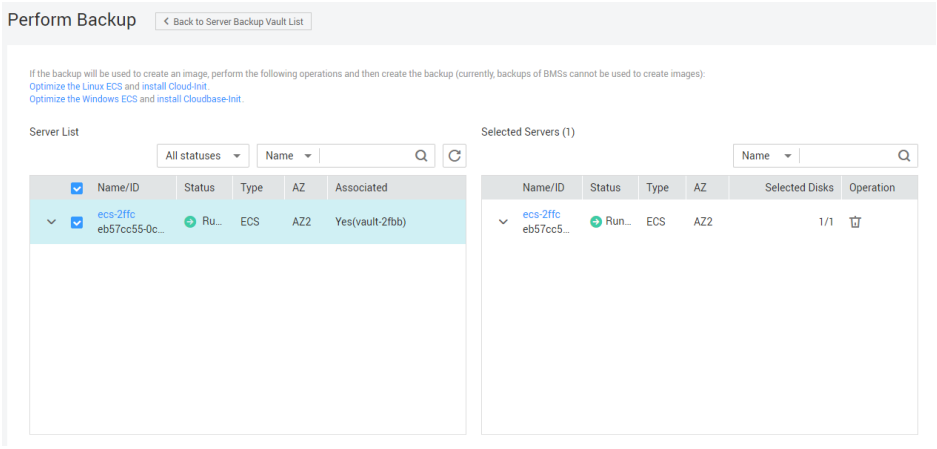
Step 1 Log in to CBR Console.

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



Step 4 Set the **Name** and **Description** for the backup. **Table 5-1** describes the parameters.

Table 5-1 Parameter description

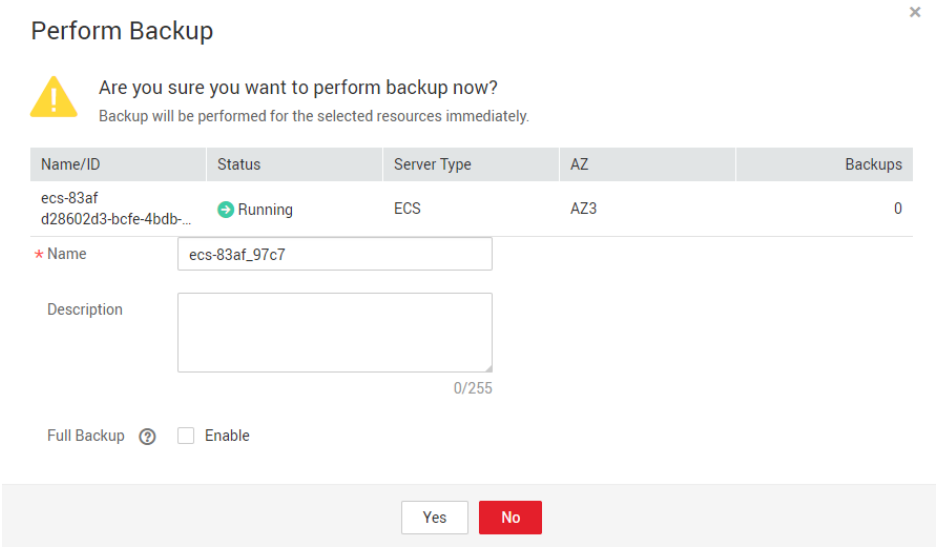
Parameter	Description	Remarks
Name	Name of the backup you are creating. A name must contain 1 to 64 characters including digits, letters, underscores (_), or hyphens (-). **NOTE** You can use the default name, which is in the format of **manualbk**_*xxxx*. If multiple servers are to be backed up, the 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, the system performs a full backup on every associated server, which requires a larger capacity compared to an incremental backup. See **Figure 5-2**.

Figure 5-2 Selecting full backup

Step 6 (Optional) You can also click the vault name to open the detailed page of the vault. On the **Associated Servers** tab page, locate the target server. Click **Perform Backup** in the **Operation** column of the server. See **Figure 5-3**.

Figure 5-3 Perform Backup



Step 7 Click **Yes**. The system 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

You can restart a server if necessary after the backup progress exceeds 10%. However, to ensure data integrity, you are advised to 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 Data Using 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. You cannot manually encrypt or cancel encrypting backups.

During the cloud disk backup, the performance of the disk is not affected. To ensure data integrity, back up the disk during off-peak hours when no write operation is performed on 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

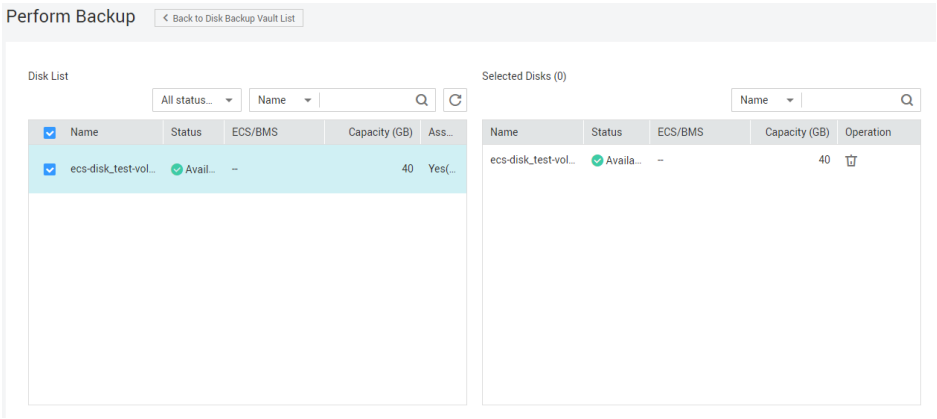
Step 1 Log in to CBR Console.

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



NOTE

The system will identify whether the selected disk is encrypted. If it is encrypted, its backup data will be stored in encrypted mode.

Step 4 Set the **Name** and **Description** for the backup. **Table 5-2** describes the parameters.

Table 5-2 Parameter description

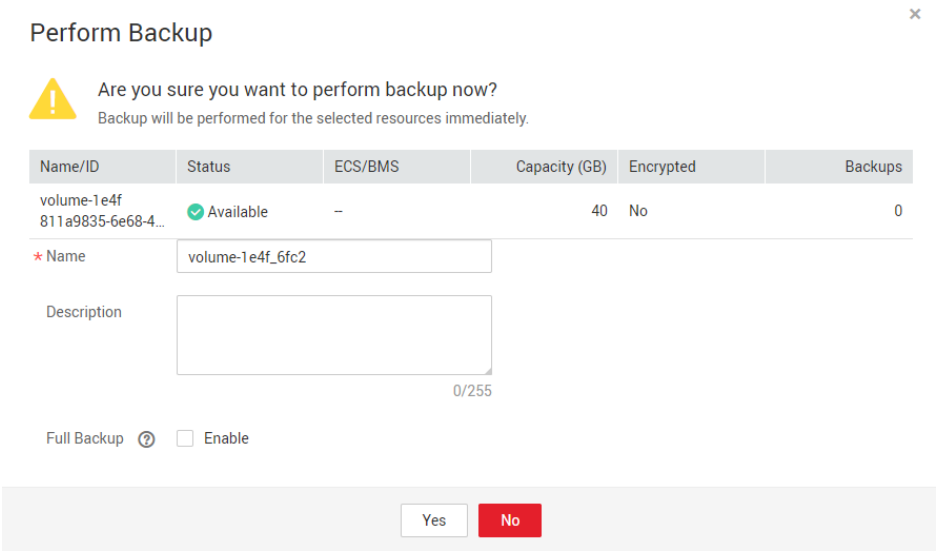
Parameter	Description	Remarks
Name	Name of the backup you are creating. A name must contain 1 to 64 characters including digits, letters, underscores (_), or hyphens (-). **NOTE** You can use the default name, which is in the format of **manualbk**_*xxxx*. If multiple disks are to be backed up, the system 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, the system performs a full backup on every associated disk, which requires a larger capacity compared to an incremental backup. See **Figure 5-5**.

Figure 5-5 Selecting full backup

Step 6 (Optional) You can also click the vault name to open the detailed page of the vault. On the **Associated Disks** tab page, locate the target disk. Click **Perform Backup** in the **Operation** column of the disk. See **Figure 5-6**.

Figure 5-6 Perform Backup



Step 7 Click **Yes**. The system 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 files from the disk during the backup, backup of the deleted files may fail. To ensure data integrity, you are advised to wait until the backup task is complete and then delete data and perform a backup again.

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.

During the SFS Turbo file system backup, the performance of the file system is not affected. To ensure data integrity, back up the file system during off-peak hours when no write operation is performed on 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

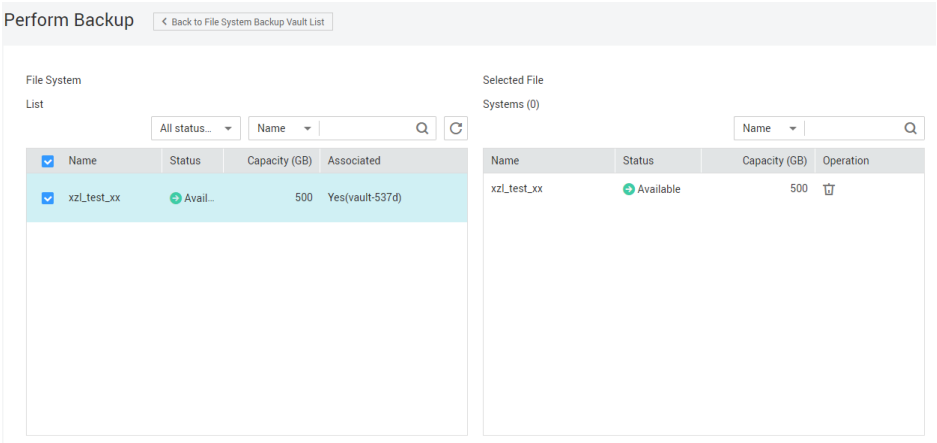
Step 1 Log in to CBR Console.

1. Log in to the management console.
2. Click  in the upper left corner and select your region and project.
3. 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 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



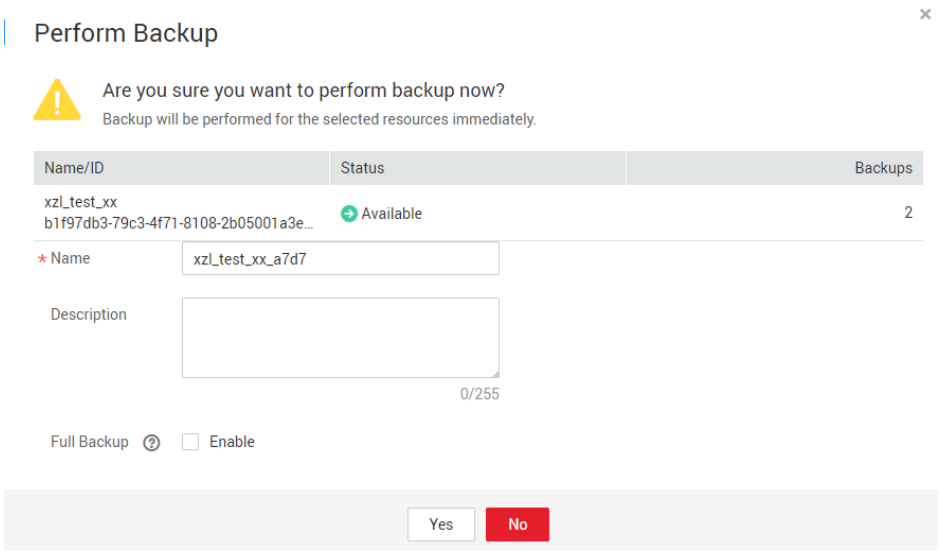
Step 4 Set the **Name** and **Description** for the backup. **Table 5-3** describes the parameters.

Table 5-3 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 use the default name, which is in the format of **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 (Optional) You can also click the vault name to open the detailed page of the vault. On the **Associated File Systems** tab page, locate the target file system. Click **Perform Backup** in the **Operation** column of the file system. See **Figure 5-8**.

Figure 5-8 Perform Backup



Step 6 Click **Yes**. The system 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 files from the file system during the backup, backup of the deleted files may fail. To ensure data integrity, you are advised to wait until the backup task is complete and then delete data and perform a backup again.

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

5.4 Creating File Backups

Scenarios

This section describes how to manually create file backups.

To implement automatic backup, create a policy and apply it to a vault by referring to **Creating a Backup Policy**. Then, the system will automatically perform backups at the time points specified in the policy.

Constraints

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

Procedure

Step 1 Log in to CBR Console.

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

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

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

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

NOTE

If you make changes to a file during the backup, backup of that file may fail. To ensure data integrity, you are advised to wait until the backup task is complete and then change the file and perform a backup again.

After the backup task is complete, you can restore the file data by referring to **Restoring Data Using a File Backup** as needed.

----End

6 Change History

Released On	Description
2022-07-20	This issue is the third official release, which incorporates the following change: Added the content of file backup.
2020-04-08	This issue is the second official release, which incorporates the following change: Added the content of file system backup.
2019-07-31	This issue is the first official release.

