Cloud Backup and Recovery

Getting Started

Issue 01

Date 2022-09-30

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.

Security Declaration

Vulnerability

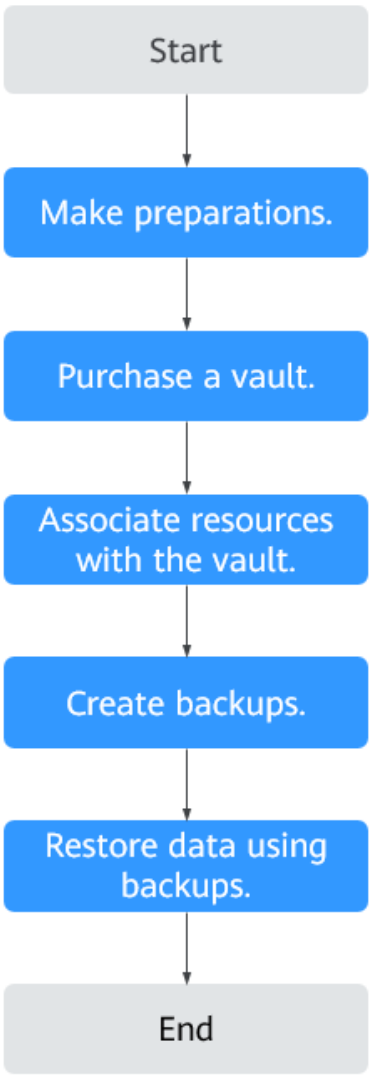
Huawei's regulations on product vulnerability management are subject to the *Vul. Response Process.* For details about this process, visit the following web page:
https://www.huawei.com/en/psirt/vul-response-process
For vulnerability information, enterprise customers can visit the following web page:
https://securitybulletin.huawei.com/enterprise/en/security-advisory

Contents

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 **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:
   - **Purchasing a Server Backup Vault**
   - **Purchasing a Disk Backup Vault**
   - **Purchasing an SFS Turbo Backup Vault**
   - **Purchasing a Hybrid Cloud Backup Vault**
   - **Purchasing a Desktop 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 during vault purchase. For details, see **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:
   - **Creating a Cloud Server Backup**
   - **Creating a Cloud Disk Backup**
   - **Creating an SFS Turbo Backup**
   - **Creating a Desktop Backup**
   - **Creating a File 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**
   - **Restoring from a Hybrid Cloud Backup**
   - **Restoring from a Desktop Backup**
   - **Restoring from a File Backup**

2 Step 1: Make Preparations

Before using CBR, 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 the registration is complete, you will be redirected 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 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

This section describes how to purchase a server backup vault.

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

Procedure

Step 1 Log in to the CBR console.

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

Step 2 In the upper right corner of the page, click **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 is ideal when the resource use duration is predictable. A longer subscription often means a lower cost.
- Pay-per-use is a postpaid billing mode. You are billed based on your resource usage and you can increase or delete resources any time.

Step 4 Select a protection type.

- **Backup**: A server backup vault stores server backups.
- **Replication**: A server replication vault stores replicas of 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 vault protection type. If you want to replicate backups of a server from one region to another, select **Replication** for the vault in this other region.

Step 5 Determine whether to enable application-consistent backup.

- If enabled, the vault can be used to store database server backups. For example, you can back up ECSs running MySQL or SAP HANA databases, because application-consistent backup ensures that the backed-up data is transactionally consistent. If an application-consistent backup task fails, CBR automatically performs a non-database server backup task instead. This non-database server backup will be stored in the database server backup vault.
- If disabled, only non-database server backup is performed on associated servers, which is usually used for ECSs not running databases.

Step 6 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 7 (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.

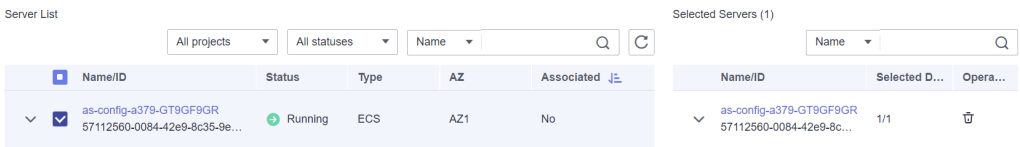
NOTICE

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

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

Step 9 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 10 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 11 (Optional) Configure automatic resource association.

- If you select **Configure**, in the next backup period, CBR will automatically scan all unprotected resources, associate them with the vault, and then perform backups.
- If you select **Skip**, CBR will not scan and associate unprotected resources with the vault you are creating.

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

Step 12 (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.

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

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: • 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: • Can contain 0 to 43 Unicode characters. • Can contain only letters, digits, hyphens (-), and underscores (_).	Value_0001

Step 13 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 14 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 15 Complete the payment as prompted.

Step 16 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 the CBR console.

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

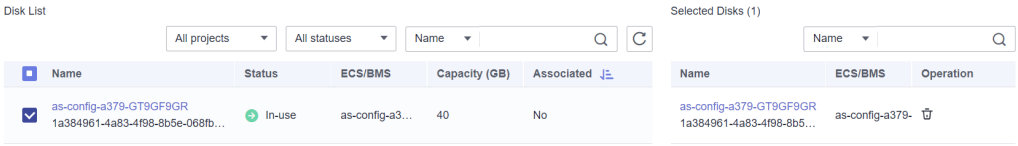
Step 2 In the upper right corner of the page, click **Buy Disk Backup Vault**.

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

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 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 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 disks 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 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 7 (Optional) Configure automatic resource association.

- If you select **Configure**, in the next backup period, CBR will automatically scan all unprotected resources, associate them with the vault, and then perform backups.
- If you select **Skip**, CBR will not scan and associate unprotected resources with the vault you are creating.

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

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

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 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 9 (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.

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

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: • Can contain 1 to 36 Unicode characters. • Can contain only letters, digits, hyphens (-), and underscores (_).	Key_0001

Parameter	Description	Example Value
Value	A tag value can be repetitive or left blank. A tag value: • Can contain 0 to 43 Unicode characters. • Can contain only letters, digits, hyphens (-), and underscores (_).	Value_0001

Step 10 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 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 Complete the payment 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 the CBR console.

1. Log in to the management console.
2. Click  in the upper left corner and select a region.
3. Click  and choose **Storage** > **Cloud Backup and Recovery** > **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 is ideal when the resource use duration is predictable. A longer subscription often means a lower cost.
- Pay-per-use is a postpaid billing mode. You are billed based on your resource usage and you can increase or delete resources any time.

Step 4 Select a protection type.

- **Backup**: An SFS Turbo backup vault stores SFS Turbo backups.
- **Replication**: An SFS Turbo replication vault stores replicas of SFS Turbo backups. If you select **Replication**, you do not need to select any SFS Turbo file system.

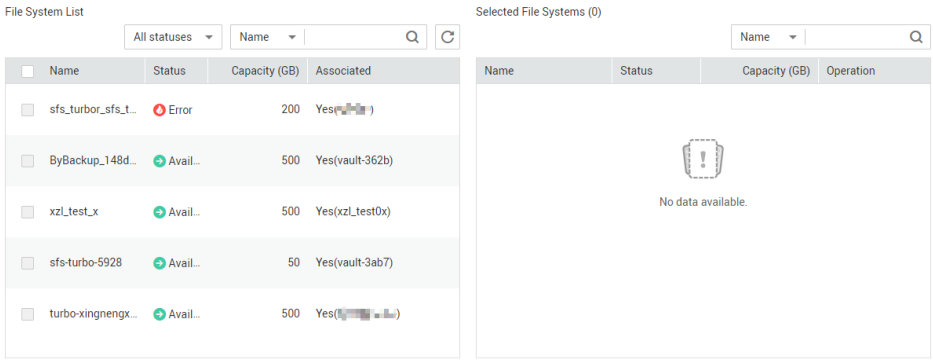
Step 5 Select a backup data redundancy policy.

- **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 6 (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 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 7 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 8 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 9 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 10 (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.

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

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 a key or select the key of an existing tag created in TMS. A tag key: • 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: • Can contain 0 to 43 Unicode characters. • Can contain only letters, digits, hyphens (-), and underscores (_).	Value_0001

Step 11 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 12 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 13 Complete the payment as prompted.

Step 14 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 Desktop Backup Vault

This section describes how to create a desktop backup vault.

Procedure

Step 1 Log in to the CBR console.

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

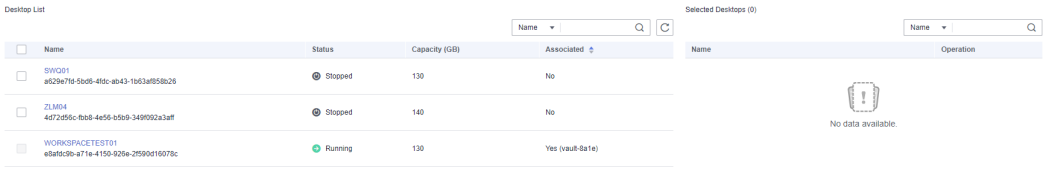
Step 2 In the upper right corner of the page, click **Buy Desktop Backup Vault**.

Step 3 Select a billing mode.

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

Step 4 (Optional) In the desktop list, select the Workspace desktops you want to back up. After desktops are selected, they are added to the list of selected desktops. See **Figure 3-4**.

Figure 3-4 Selecting desktops



NOTE

- The selected desktops must have not been associated with any vault and must be in the **Available** or **In-use** state.
- You can also associate desktops 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 desktops you want to back up.

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 desktops associated with this vault will be automatically backed up based on this policy.
- If you select **Skip**, desktops 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 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.

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

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 a key or select the key of an existing tag created in TMS. A tag key: • 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: • 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 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 11 Complete the payment as prompted.

Step 12 Return to the **Desktop Backups** page. You can see the created vault in the vault list.

You can associate Workspace desktops to the new vault or perform backup for the desktops. For details, see **Vault Management**.

----End

3.5 Purchasing a Hybrid Cloud Backup Vault

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

Hybrid cloud backup vaults store file backups, storage backups and VMware backups. Buy a hybrid cloud backup vault that suits your needs. In this section, a storage backup vault is purchased. Operations vary depending on the usage of a

hybrid cloud backup vault. This section is used for reference only. Follow the actual console operations.

For detailed backup processes, see **File Backup** and **Hybrid Cloud Backup**.

Procedure

Step 1 Log in to the CBR console.

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

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

Step 3 Select a billing mode.

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

Step 4 Select a protection type.

- **Backup**: A hybrid cloud backup vault stores backups.
- **Replication (cross-region)**: A hybrid replication vault stores replicas of backups.

Step 5 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 6 Specify a vault capacity ranging from 1 to 10,240 TB. The vault capacity cannot be less than the size of the server backups.

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.

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

Table 3-5 describes the parameters of a tag.

Table 3-5 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: • 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: • 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-98c8**.

NOTE

You can also use the default name **vault**_*xxxx*.

Step 10 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 11 Complete the payment as prompted.

Step 12 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 created, you can synchronize on-premises backups to the cloud and use the backups to restore or deploy services on the cloud when needed. But you cannot create hybrid cloud backups on the CBR console.

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

3.6 Purchasing a File Backup Vault

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

Procedure

Step 1 Log in to the CBR console.

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

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

Step 3 Select a billing mode.

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

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

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

Step 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 files associated with this vault will be automatically backed up based on this policy.

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

Step 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.

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

Table 3-6 describes the parameters of a tag.

Table 3-6 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: • 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: • 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-f61e**.

NOTE

You can also use the default name **vault**_*xxxx*.

Step 9 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 10 Complete the payment as prompted.

Step 11 Go back to the **File Backups** page. You can see the created vault in the vault list.

----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.

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**.

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

Prerequisites

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

Table 4-1 Resource statuses available for association

Resource Type	Status
Cloud server	Running or Stopped

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

Procedure

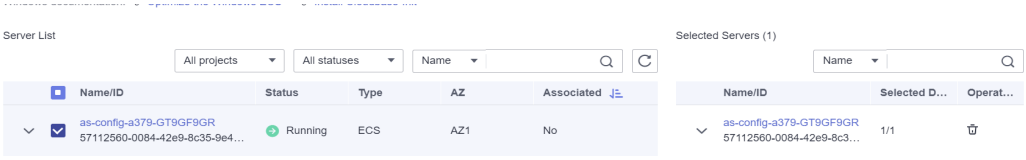
Step 1 Log in to the CBR console.

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

Step 2 On 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

Automatic Association

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

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

capacity and associated capacity in the **Basic Information** area on the details page of the vault. For example, if you have an 800-GB server backup vault and it has been associated with two 100 GB servers, its remaining capacity is 600 GB (800 GB – 200 GB). In this case, you can enable automatic association.

- If multiple vaults are enabled with automatic association, CBR scans their backup policies and associates resources with the vault whose next scheduled backup time is the earliest.
- If the capacity of the first selected vault is used up, resources will be associated with the vault whose next scheduled backup time is the second earliest.
- If a backup policy with the earliest scheduled backup time is applied to more than one vault, CBR randomly associates the resources with one of these vaults.
- If a vault has automatic association enabled but has no backup policy applied, no resources will be automatically associated with this vault. You can manually associate unprotected resources.
- After automatic association is disabled for a vault, the vault stops automatically scanning for unprotected resources. Associated resources are not affected.

Step 1 Log in to the CBR console.

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

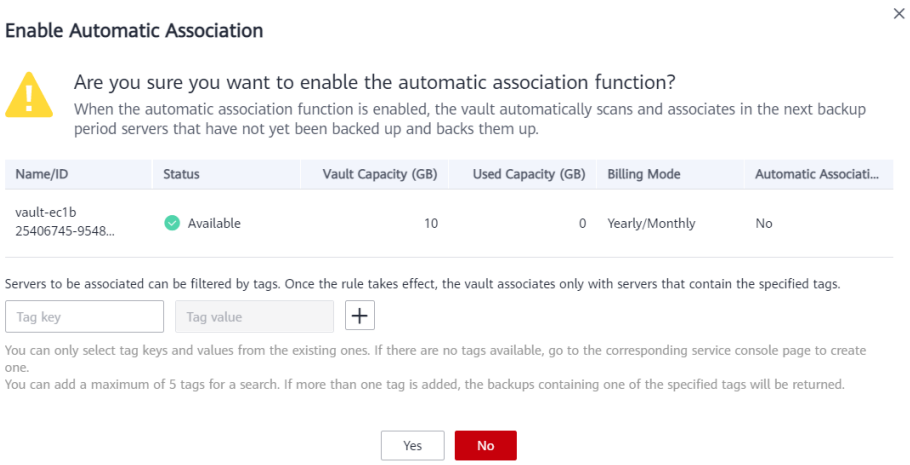
Step 2 On any backup page, locate the target vault.

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

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

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

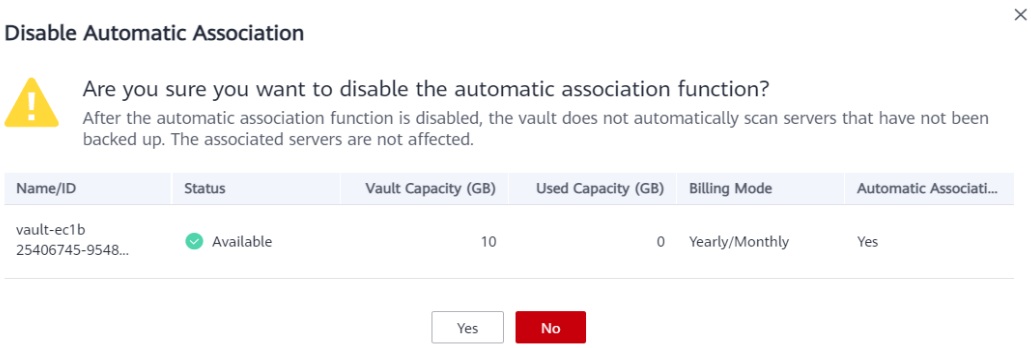
Figure 4-2 Enabling automatic association



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

Step 5 (Optional) If automatic association is not required, choose **More** > **Disable Automatic Association** in the **Operation** column of the vault. See **Figure 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. When you want an ECS later, you can create an image from the ECS backup and use the image to create ECSs.

Backing up a server does not impact the server performance.

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

Prerequisites

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

Procedure

Step 1 Log in to the CBR console.

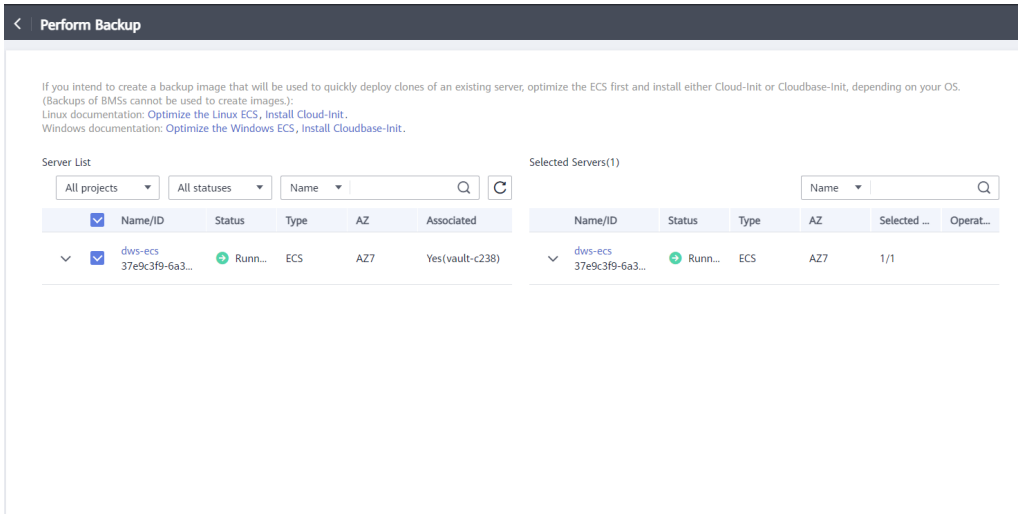
1. **Log in to the management console**.
2. Click  in the upper left corner and select a region.
3. Click  and choose **Storage** > **Cloud Backup and Recovery**. Select a backup type from the left navigation pane.

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

Step 3 Perform backup in either of the following ways:

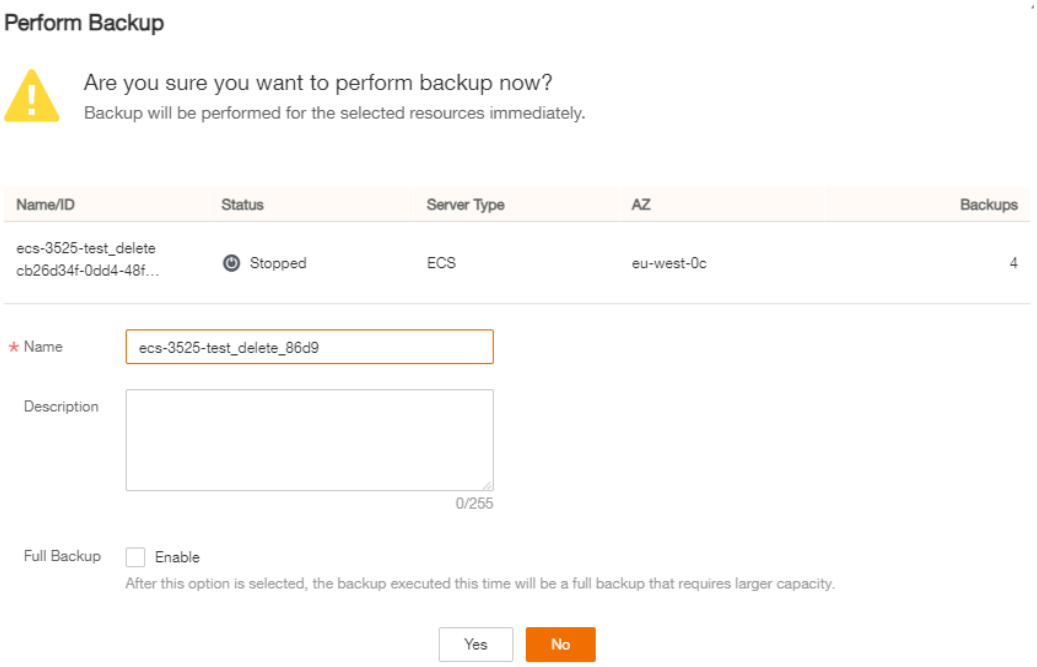
- Choose **More** > **Perform Backup** in the **Operation** column. In the server list, select the server you want to back up. After a server is selected, it is added to the list of selected servers. See **Figure 5-1**.

  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

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 server does not impact the disk performance.

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

Prerequisites

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

Procedure

Step 1 Log in to the CBR console.

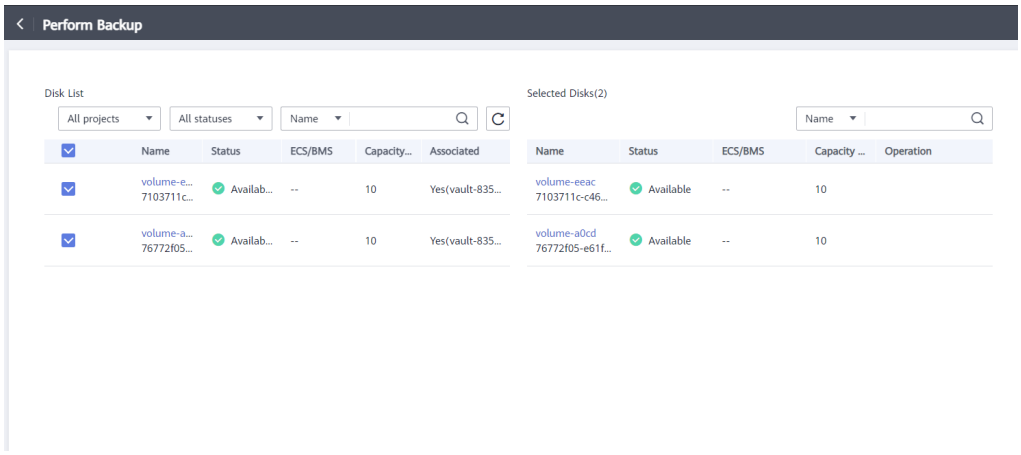
1. **Log in to the management console**.
2. Click  in the upper left corner and select a region.
3. Click  and choose **Storage** > **Cloud Backup and Recovery**. Select a backup type from the left navigation pane.

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

Step 3 Perform backup in either of the following ways:

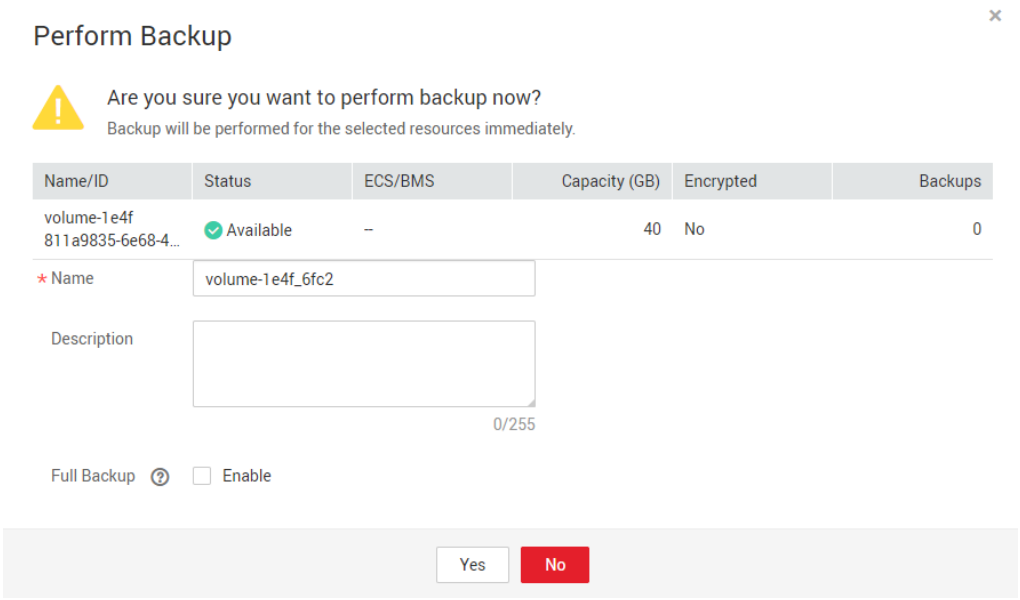
- Click **Perform Backup** in the **Operation** column. In the disk list, select the disk you want to back up. After a disk is selected, it is added to the list of selected disks. See **Figure 5-4**.

  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

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.

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

Prerequisites

A 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 the CBR console.

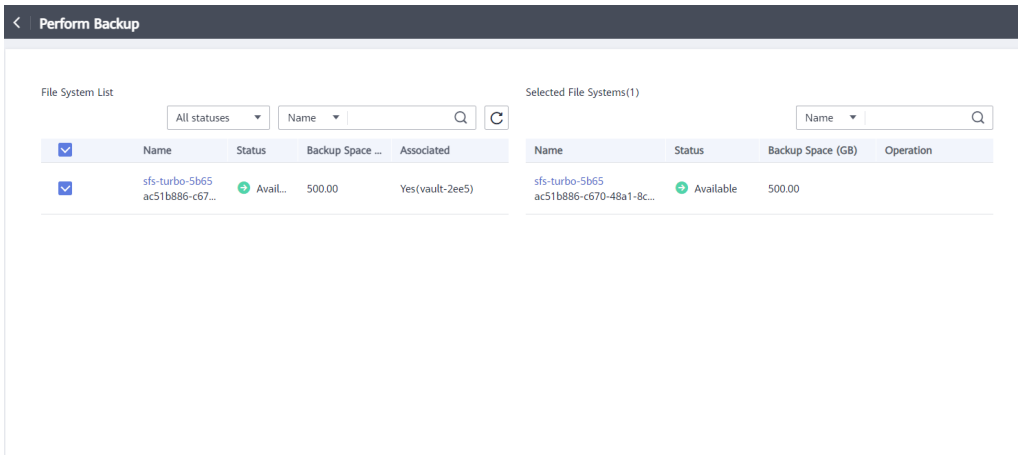
1. Log in to the management console.
2. Click  in the upper left corner and select a region.
3. Click  and choose **Storage** > **Cloud Backup and Recovery** > **SFS Turbo Backups**.

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:

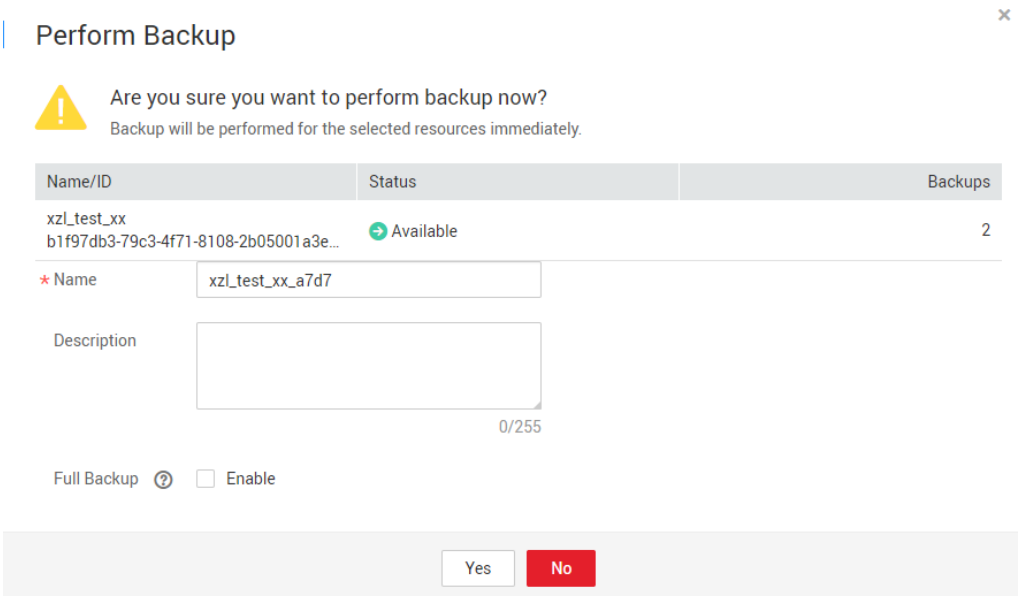
- Choose **More** > **Perform Backup** in the **Operation** column. In the file system list, select the file system to be backed up. After a file system is selected, it is added to the list of selected file systems. See **Figure 5-7**.

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	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 **Using a Backup to Create a File System**.

----End

5.4 Creating a Desktop Backup

This section describes how to quickly create a desktop backup.

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

Prerequisites

A Workspace desktop 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 desktop, refresh the page first to ensure that the operation is complete and then determine whether to back up the desktop.

Procedure

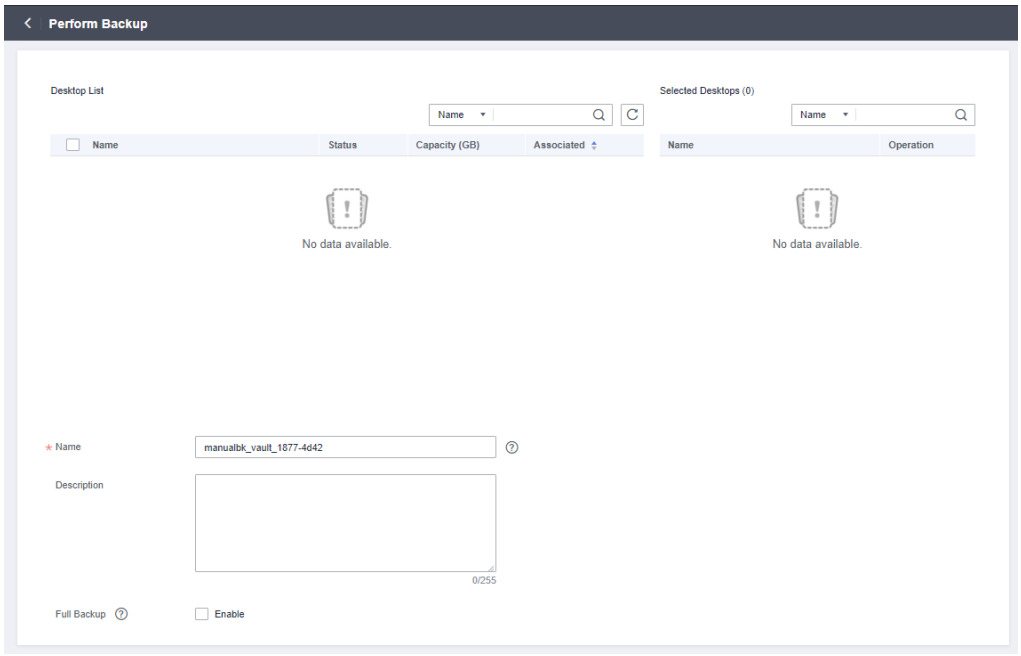
Step 1 Log in to the CBR console.

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

Step 2 On the **Desktop Backups** page, click the **Vaults** tab and find the vault to which the desktop is associated.

Step 3 Choose **More** > **Perform Backup** in the **Operation** column. In the desktop list, select the desktop you want to back up. After a desktop is selected, it is added to the list of selected desktops. See **Figure 5-9**.

Figure 5-9 Selecting desktops



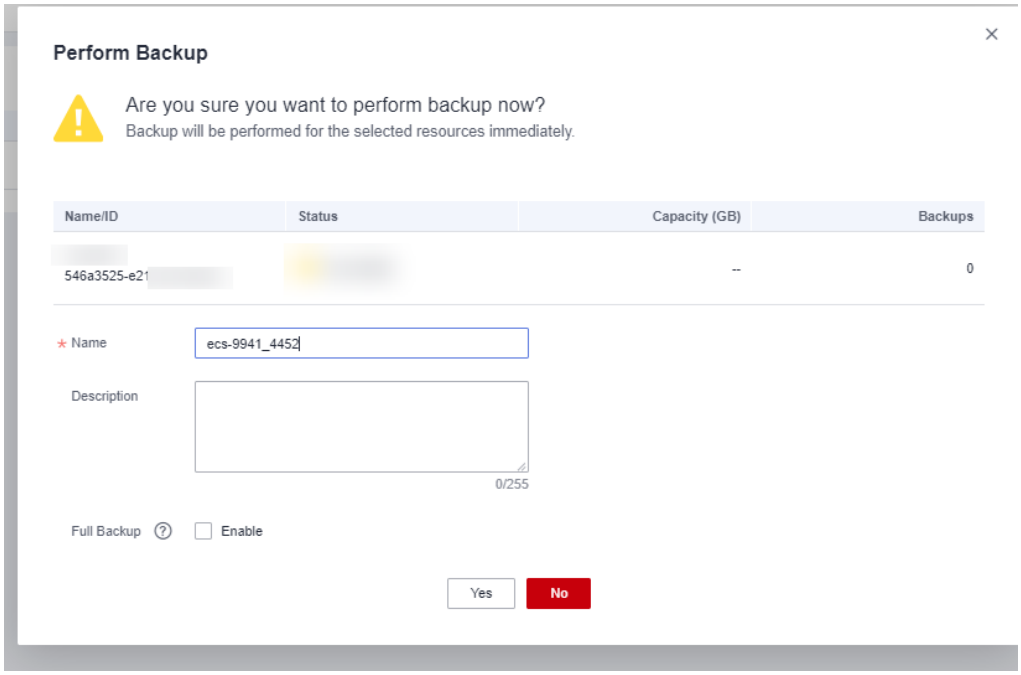
Step 4 Set **Name** and **Description** for the backup. **Table 5-4** describes the parameters.

Table 5-4 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 desktops 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) Click the vault name to go to the vault details page. On the **Associated Desktops** tab page, locate the target desktop. Click **Perform Backup** in the **Operation** column of the desktop. See **Figure 5-10**.

Figure 5-10 Perform Backup



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

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 desktop 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 desktop data. For details, see .

----End

5.5 Creating a File Backup

Scenarios

This section describes how to manually create file backups.

To implement automatic file 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.

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

Constraints

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

Procedure

Step 1 Log in to the CBR console.

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

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

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

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

NOTE

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

After the backup task is complete, you can restore 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 support for 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.

