ALIBABA CLOUD

Alibaba Cloud

Hybrid Backup

Back up NAS

Document Version: 20220401

Alibaba Cloud

Legal disclaimer

Alibaba Cloud reminds you to carefully read and fully understand the terms and conditions of this legal disclaimer before you read or use this document. If you have read or used this document, it shall be deemed as your total acceptance of this legal disclaimer.

1. You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.

2. No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company or individual in any form or by any means without the prior written consent of Alibaba Cloud.

3. The content of this document may be changed because of product version upgrade, adjustment, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and an updated version of this document will be released through Alibaba Cloud-authorized channels from time to time. You should pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.

4. This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides this document based on the "status quo", "being defective", and "existing functions" of its products and services. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity, applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not take legal responsibility for any errors or lost profits incurred by any organization, company, or individual arising from download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, take responsibility for any indirect, consequential, punitive, contingent, special, or punitive damages, including lost profits arising from the use or trust in this document (even if Alibaba Cloud has been notified of the possibility of such a loss).

5. By law, all the contents in Alibaba Cloud documents, including but not limited to pictures, architecture design, page layout, and text description, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of this document shall be used, modified, reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates. The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates.

6. Please directly contact Alibaba Cloud for any errors of this document.

Document conventions

Style	Description	Example
⚠ Danger	A danger notice indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	⚠ **Danger:** Resetting will result in the loss of user configuration data.
🔔 Warning	A warning notice indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	🔔 **Warning:** Restarting will cause business interruption. About 10 minutes are required to restart an instance.
📢 Notice	A caution notice indicates warning information, supplementary instructions, and other content that the user must understand.	📢 **Notice:** If the weight is set to 0, the server no longer receives new requests.
? Note	A note indicates supplemental instructions, best practices, tips, and other content.	? **Note:** You can use Ctrl + A to select all files.
>	Closing angle brackets are used to indicate a multi-level menu cascade.	Click **Settings**> **Network**> **Set network type**.
Bold	Bold formatting is used for buttons , menus, page names, and other UI elements.	Click **OK**.
`Courier font`	Courier font is used for commands	Run the `cd /d C:/window` command to enter the Windows system folder.
Italic	Italic formatting is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	This format is used for an optional value, where only one item can be selected.	`ipconfig [-all|-t]`
{} or {a|b}	This format is used for a required value, where only one item can be selected.	`switch {active|stand}`

Table of Contents

1.Back up a NAS file system

This topic describes how to use Hybrid Backup Recovery (HBR) to back up the data of an Apsara File Storage NAS file system. After you back up the data, you can restore the data at the earliest opportunity if the data is lost or damaged.

Prerequisites

A Network File System (NFS) or Server Message Block (SMB) file system is created. For more information, see Create a NAS file system.

Context

- Unless otherwise specified, NAS in this topic refers to Apsara File Storage NAS.
- HBR allows you to back up NFS and SMB file shares regardless of whether NAS file systems are mounted. HBR uses an efficient backup mechanism that scans files in NAS file systems. This eliminates the need to create snapshots for NAS file systems.
- When you back up a NAS file system, the access control list (ACL) feature of NAS SMB files system is not supported. For more information, see Features.
- If you do not have the required permissions to back up an NAS SMB file system by using HBR, the backup operation fails. In this case, we recommend that you grant HBR the required permissions on an Elastic Compute Service (ECS) instance. For more information, see Grant HBR the permissions to read data from SMB file systems in NAS.
- You can also back up Apsara File Storage NAS file systems by using a backup client for ECS. For more information, see Overview.

Create a backup plan

> **Note** We recommend that you include no more than 50 million files or 8 million files and subdirectories in each directory for a single backup job.

To back up files in a NAS file system to a backup vault in the same region as the file system, perform the following steps:

1.
2. In the left-side navigation pane, choose **Backup > NAS Backup**.
3. In the top navigation bar, select a region.
4. On the **Alibaba NAS** tab, click **Back Up File System** in the upper-right corner.
5. In the **Backup File System** panel, set the parameters and click **OK**.

   > **Note** The first time you use HBR, you can apply for a 30-day free trial of backup plans. The free trial period starts from the day when a backup plan is created.

i. The following table describes the basic parameters.

Parameter	Description
File System	The NAS file system that you want to back up.
Plan Name	The name of the backup plan. By default, a random name is used.
Start Time	The time at which the backup plan starts. The time is accurate to seconds.
Pay After Trial Ends	Specifies whether to pay for the backup plan after the free trial ends.

ii. Click **Switch to Paid Plan** to configure the advanced settings. The following table describes the advanced parameters.

Parameter	Description
Source Paths	The path to the folder that you want to back up, for example, `/nas/folder` .
Backup Interval	The interval at which HBR performs incremental backups. Unit: days or weeks.
Retention Policy	The retention policy for the backup data. Valid values: ▪ *Limited* (default value): The backup data is retained for a specified period of time. If you select Limited, you must set the **Retention Period** parameter. ▪ *Permanent*: The backup data is permanently retained.
Retention Period	This parameter is required only if the **Retention Policy** parameter is set to *Limited*. The retention period of the backup data. Valid values: By default, the backup data is retained for 1 week. Unit: days, weeks, months, or years.
Backup Vault	The backup vault where you want to store the backup data. ▪ *Create Vault* (default value): If you select this option, specify the Vault Name field. By default, a random name is used. ▪ *Select Vault*: If you select this option, select a backup vault from the Vault Name drop-down list.
Backup Vault Resource Group	This parameter is required only if the **Backup Vault** parameter is set to *Create Vault*. The resource group to which the backup vault belongs. Resource groups allow you to sort the resources of your Alibaba Cloud account for easier resource and permission management. For more information, see Create a resource group.

Parameter	Description
Source Encryption Type	This parameter is required only if the **Backup Vault** parameter is set to *Create Vault*. The method that is used to encrypt the data in the backup vault. ■ *HBR-managed* (default value): The default encryption method of HBR is used. ■ *KMS*: Key Management Service (KMS) is used to encrypt the data. **Notice** If you select this option, you cannot delete or disable the KMS key.
KMS KeyId	This parameter is required only if the **Source Encryption Type** parameter is set to *KMS-managed*. The ID of the KMS key that is used to encrypt the data stored in the backup vault. **Note** Before you use the KMS key to encrypt the data stored in the backup vault, you must create a key ID in the KMS console. For more information, see Create a CMK.

After you create a backup plan, HBR backs up files in the source NAS file system from the specified start time at the specified interval.

On the **Backup Plans** tab, you can perform the following operations:

- To start a backup job, find the backup plan and click **Run Now** in the Actions column.
- To suspend a backup job that is running, find the backup plan and choose **More > Suspend Plan** in the Actions column. To resume a backup job that is suspended, find the backup plan and choose **More > Resume Plan** in the Actions column.
- To delete a backup plan, find the backup plan and choose **More > Delete Plan** in the Actions column. After you delete a backup plan, HBR no longer runs backup jobs for the plan but the backup data is retained.
- To view all backups of a file system or the backups created within the last three months, find the backup plan and choose **More > Backups** in the Actions column.
- To modify a backup plan, find the backup plan and click **Edit** in the Actions column.

> **Note** You can view the progress of each backup job on the **Backup Jobs** tab. After a backup job is complete, you can restore the backup data of the source NAS file system to the same or a different NAS file system.

Create a restore job

To restore backup data from a backup vault to a NAS file system in the same region as the vault, perform the following steps:

1. In the upper-right corner of the **Restore Jobs** tab, click **Create Restore Job**.

2. In the **Create Restore Job** panel, set the following parameters.

    i. Select the backup that you want to restore, and click **Next**.

Parameter	Description
Source Vault	The backup vault where the backup data that you want to restore is stored.
Source File System	The source NAS file system. Select a NAS file system that has been backed up by using HBR.
Select a backup to restore	The backup that you want to restore. Select a backup that you want to restore from the drop-down list.

    ii. In the **Select Restore Item** step, set the **Restore Policy** parameter and click **Next**.

Parameter	Description
Restore Items	Select the files or directories that you want to restore. Valid values: ■ *Include All Files*: HBR restores all backup files from the source NAS file system. ■ *Include Files*: Select the files or folders that you want to restore. You can also click **Enter Paths** to specify the files that you want to restore. ■ *Exclude Files*: Select the files or folders that you do not want to restore. You can also click **Enter Paths** to specify the files that you do not want to restore. Enter one path in each line and make sure that each path starts with the lowest-level directory in the source path. For example, to restore the file.txt file and the abc folder in the /test/data directory, enter the following paths: `/data/file.txt /data/abc`

    iii. In the **Restore Destination** step, select a **file system** in the specified region and click **Next**.

iv. In the **Destination Path** step, specify the recovery path and click **Create**.

Parameter	Description
Restore Path Type	The type a recovery path. ▪ *Specify Path*: Specify a new path and restore the file system to the path. ▪ *Origin Path*: Restore the file system to the original path.
Destination Path	This parameter is required only if the **Restore Path Type** parameter is set to *Specify Path*. The path to which the file system is restored. For example, you can restore the file system to */nas/abc*.

After the restore job is created, you can view the job progress in the **Status** column on the **Restore Jobs** tab.

Create a remote mirror vault for the backup vault

A backup vault is a repository in which HBR stores backup data in the cloud. To implement disaster recovery, you can create a remote mirror vault for a backup vault and back up data from the backup vault to the mirror vault.

To back up data to a mirror vault, perform the following steps:

1.
2. In the left-side navigation panel, click **Overview**. On the Overview page, select a region, such as China (Hangzhou). Find the backup vault for which you want to create a mirror vault and click **Cross-Region Backup** in the upper-right corner of the backup vault section.
3. In the **Create Mirror Vault** pane, select the region where the mirror vault resides, enter the name and description of the mirror vault, and then click **Create**.

> Note
>
> - You can create only one mirror vault for each backup vault.
> - You can back up data to a remote mirror vault and restore backup data from the mirror vault. However, you cannot create backup plans for the mirror vault. The historical backup data stored in the source backup vault is synchronized to a mirror vault 90 minutes after the mirror vault is created.
> - When a mirror vault is created, the mirror vault contains all the backup data that is stored in the source backup vault.

After you create a mirror vault, you can view the progress of data synchronization. After the data is synchronized, you can restore the data in a NAS file system from the mirror vault.

Restore data from a remote mirror vault

A backup vault is a repository in which HBR stores backup data in the cloud. To implement disaster recovery, you can restore data from a remote mirror vault to a NAS file system. Perform the following steps:

1. On the NAS Backup page, select the region where the mirror vault resides and then select a file system.
2. Click the **Restore Jobs** tab. In the upper-right corner of the Restore Jobs tab, click **Create Restore Job**.
3. In the **Select Backup** step, set the parameters.

   You must select the mirror vault from the **Source Vault** drop-down list. The name of a mirror vault is prefixed by [COPY]. For information about how to set other parameters, see Create a restore job.

More

In the upper-right corner of the **NAS Backup** page, click **Manage Mounts**. In the Manage Mounts panel, you can perform the following operations:

- View all the file systems for which you have created backup plans in the selected region. You can click a file system to view the information of the NAS file system. The information includes the protocol type and the number of mount targets.
- **Unmount a file system**. After you create a backup plan for a NAS file system, HBR creates a mount target for the file system. You cannot directly delete the mount target in the NAS console because it is created by using an internal service of Alibaba Cloud. If you want to delete the mount target, find the file system in the **Manage Mounts** panel and click **Unmount** in the Actions column. After the mount target is deleted, the backup jobs that are running fail. Before you delete the mount target, make sure that all backup plans are deleted and no backup jobs or restore jobs of the file system are running.

2.Isilon (PowerScale) Backup

2.1. Overview

Hybrid Backup Recovery (HBR) is a fully managed online backup service that allows you to back up data to the cloud in an efficient, secure, and cost-effective manner. You can use an HBR backup client to back up files from an on-premises NAS file system in the HBR console. You can then restore the files if they are lost or damaged. The NAS file system can be an OneFS distributed file system designed by Isilon (PowerScale).

You can perform the following operations to back up files from and restore files to on-premises NAS file systems:

- Prepare for a data backup
- Back up an on-premises NAS file system
- Restore files to a local NAS file system

2.2. Prepare for a data backup

You can use Hybrid Backup Recovery (HBR) to back up files from local NAS file systems. Then, you can use the backup files to restore data based on your business requirements. This topic describes how to prepare for a data backup.

(Recommended) Create an AccessKey pair for a RAM user

Resource Access Management (RAM) is an Alibaba Cloud service that allows you to manage user identities and control access to resources. RAM allows you to create and manage multiple identities for an Alibaba Cloud account, and grant multiple permissions to a single identity or a group of identities. This way, you can authorize different identities to access different Alibaba Cloud resources.

An AccessKey pair is an identity credential and is required when you activate an HBR client. If you use the AccessKey pair of your Alibaba Cloud account, the AccessKey pair may be leaked and all cloud resources that belong to the account may be exposed to risks. Therefore, we recommend that you use the AccessKey pair of a RAM user to activate HBR clients. For more information, see Create a RAM user and Create an AccessKey pair for a RAM user.

Download and activate an HBR client for Windows

1.
2. In the left-side navigation pane, choose **Backup > NAS Backup**.
3. On the left of the top navigation bar, select a region.

   > ⓘ **Note** Alibaba Cloud continuously updates HBR to support more regions. You can log on to the HBR console to view the regions in which HBR is supported.

4. On the **NAS Backup** page, click **Local NAS**.
5. In the upper-right corner of the page, click **Add Client**.
6. Download the HBR client for Windows.

   You can download the installation package of the HBR client for **Windows (64-bit)** or **Windows (32-bit)**. Record the activation code. The activation code is used to install and activate the client.

7. Install and activate the HBR client for Windows.
   i. Double-click the installation package of the HBR client and select the language that you want to use.
   ii. Select the path in which you want to install the client and click **Next**.
   iii. Select **Local client connecting to Alibaba Cloud**, and then click **Next**.
   iv. Configure the logon identity.
      - If you want to back up or archive the files only from local paths, select **Local System**.
      - If you want to back up or archive files that are shared over a network, select **This user**. The user must meet the following requirements:
         - The user has the permissions of the local administrator.
         - The user has the permissions to log on as a service.

           To configure the logon user, perform the following steps:

           a. Open the **Control Panel**. In the window that appears, click **Administrative Tools**.
           b. Open **Local Security Policy** and choose **Local Policies > User Rights Assignment** .
           c. Turn on **Logon as a service**. In the dialog box that appears, add a user.
         - The user has the permissions to access files that are shared over a network.
   v. If you want to use a proxy server, enter the IP address of the proxy server. Click **Next**.
   vi. Enter the activation code that you recorded in the **Activation token** field and click **Next**.
   vii. Click **Install**.

      After the client is installed, **Activated** is displayed in the Client Status column on the **On-premises Backup** page.

Download and activate an HBR client for Linux

1.
2. In the left-side navigation pane, choose **Backup > NAS Backup**.
3. On the left of the top navigation bar, select a region.

   > **Note** Alibaba Cloud continuously updates HBR to support more regions. You can log on to the HBR console to view the regions in which HBR is supported.

4. In the upper-right corner of the page, click **Add Client**.
5. Download and decompress the HBR client for Linux.

   You can download the installation package of the HBR client for **Linux (64-bit)** or **Linux (32-bit)**. Record the activation code. The activation code is used to install and activate the client.
6. Manually or automatically activate the HBR client for Linux.

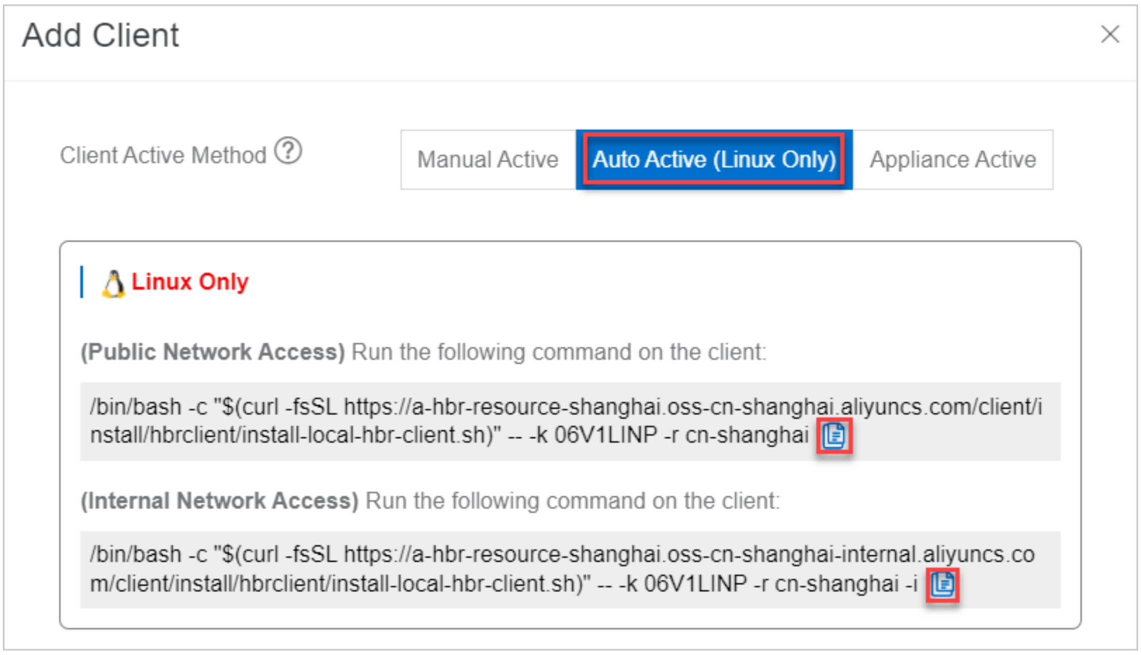
   In the following example, `05M72DYX` is the dynamic activation code that is obtained from the HBR console.

   - Manually activate the HBR client for Linux.

In the path to which the HBR client is decompressed, run the `./setup -t local -k 05M72DYX` command to activate the client.

- Automatically activate the HBR client for Linux.

  In the Add Client panel, click **Auto Active (Linux Only)** and copy one of the commands based on your network. Then, paste and run the command on the client for Linux to activate the client.

  (Public Network Access) Run the following command on the client:

  ```
  /bin/bash -c "$(curl -fsSL https://a-hbr-resource-shanghai.oss-cn-shanghai.aliyuncs.com/client/install/hbrclient/install-local-hbr-client.sh)" -- -k 06V1LINP -r cn-shanghai
  ```

  (Internal Network Access) Run the following command on the client:

  ```
  /bin/bash -c "$(curl -fsSL https://a-hbr-resource-shanghai.oss-cn-shanghai-internal.aliyuncs.com/client/install/hbrclient/install-local-hbr-client.sh)" -- -k 06V1LINP -r cn-shanghai -i
  ```

After the client is installed, perform the following steps to view the status of the client: Go to the **On-Premises Backup** page, click File (New), and then click the **Clients** tab. On the Clients tab, **Activated** is displayed in the **Client Status** column.

7. Run one of the following commands to install the tool that is required to back up and restore local NAS file systems.

   The Network File System (NFS) and Server Message Block (SMB) protocols are supported. You can select a tool based on the protocol of your NAS file system.

   - NFS tool
     - CentOS

       ```
       sudo yum install nfs-utils
       ```

     - Ubuntu

       ```
       sudo apt-get install nfs-common
       ```

   - SMB tool
     - Centos

       ```
       sudo yum install cifs-utils
       ```

     - Ubuntu

       ```
       sudo apt-get install cifs-utils
       ```

- openSUSE

  ```
  sudo zypper install cifs-utils
  ```

What's next

Back up an on-premises NAS file system

2.3. Back up an on-premises NAS file system

This topic describes how to use Hybrid Backup Recovery (HBR) to back up files in an on-premises NAS file system.

Prerequisites

The preparations are complete. For more information, see Prepare for a data backup.

Create a backup plan

The first time you create a backup plan, we recommend that you use NAS Backup Wizard to perform a complete backup. Supported NAS types include **Isilon (PowerScale)** and **other NAS types**. In this topic, a backup plan for an Isilon NAS file system is created.

1. Log on to the HBR console.
2. In the left-side navigation pane, choose **Backup > NAS Backup**.
3. On the **NAS Backup** page, click **Local NAS**.
4. On the **Local NAS** tab, click **NAS Backup Wizard** in the upper-right corner of the tab.
   i. Add a NAS file system and click **Next**.
      a. In the **Backup Source NAS** step of the Create Backup Plan panel, set Backup NAS Instance to **New NAS Instance**.

         You can also select an existing NAS file system.

b. The following table describes the basic parameters.

Parameter	Description
NAS Type	The type of the NAS file system. Valid values: ■ **Isilon (PowerScale)**: Isilon NAS file systems ■ **Others**: other NAS file systems
NAS Instance Name	The name of the NAS file system that you want to back up.
NAS Management Username	The username of the account that is used to manage the NAS file system.
NAS Management Password	The password of the account.
NAS Network Address	The IP address of the NAS file system.
NAS Management Port	The port number of the NAS file system.
NAS Share Path	The path to the files that you want to back up. The path is relative to /ifs, for example, /myshare. The path can contain letters, digits, and the following special characters: `,-_=/.:\`.
Protocol Type	The protocol type of the file system. Valid values: NFS and SMB. In this topic, the Protocol Type parameter is set to NFS.

c. Optional. Click **Advanced Settings**, and then click **+Set Mount Parameters**.

You can add multiple mount parameters when you mount a file system. The following table describes the mount parameters.

Parameter	Description
vers	Specifies the protocol version of the file system. ■ vers=3 : uses NFSv3 to mount the file system. ■ vers=4 : uses NFSv4 to mount the file system.
nolock	Specifies whether to enable file locking.
proto	Specifies the protocol that is used to mount the file system.
rsize	Specifies the size of data blocks that the client reads from the file system. Recommended value: 1048576. Unit: bytes.
wsize	Specifies the size of data blocks that the client writes to the file system. Recommended value: 1048576. Unit: bytes.
hard	Specifies that applications no longer access a file system when the file system is unavailable and access the file system again when the file system becomes available. We recommend that you enable the parameter.
timeo	Specifies the period in deciseconds (tenths of a second) for which the NFS client waits before the client retries to send a request. Recommended value: 600 (60 seconds).
retrans	Specifies the number of retries after the NFS client fails to send a request. Recommended value: 2.

ii. Create a client group and click **Next**.

If you want multiple HBR clients to concurrently run a backup job, you can add the clients to a backup client group. Set Backup Client Group to **New Backup Client Group**. Specify **Client Group Name** and select the clients that you want to add to the client group.

If you want to modify or delete the clients that are included in a client group, you can choose **More > Edit Backup Clients Group** in the Actions column on the **NAS Instance** tab.

For information about how to install an HBR client, see Download and activate an HBR client for Linux.

iii. Create a backup plan and click **OK**.

a. The following table describes the basic parameters of the backup plan.

Parameter	Description
Backup Vault	If backup vaults are created, click **Select Vault** and select a backup vault from the Vault Name drop-down list. If no backup vaults are created, click **Create Vault** and specify Vault Name. The name must be 1 to 64 characters in length. **Note** A backup vault is a cloud repository that is used by HBR to store backup data. You can back up files from multiple HBR backup clients to a vault. Backup vaults reside in different regions. You can select or create a backup vault only in the specified region.
Vault Name	Select a backup vault.
Plan Name	The name of the backup plan. If you do not specify a value for the parameter, a random name is generated and specified for the parameter.
Source Paths	The path to the files that you want to back up. You can specify only one path. The path cannot include wildcard characters.
Backup Rule	You can specify the following three backup rules: ■ **Include All Files**: All files in the source path are backed up.

Parameter	Description
	- **Include Files** or **Exclude Files**: You must enter the names of the files that you want to include or exclude in the Enter Paths field. HBR backs up files based on the specified rule. The file names that you enter in the Enter Paths field are subpaths relative to the source path. HBR matches the file names based on the following rules: - If a file name that is specified in the Enter Paths field starts with a forward slash (/), HBR combines the relative path and the source path into a complete path. Then, the files in the complete path are specified. Example 1: If the source path is */ifs/dataset* and */subdir/data* is entered in the Enter Paths field, files and directories in */ifs/dataset/subdir/data* are specified. Example 2: If the source path is */ifs/dataset* and */abc** is entered in the Enter Paths field, files and directories whose names are prefixed with abc in the */ifs/dataset/abc* path are specified. - If a file name that is specified in the Enter Paths field does not start with a forward slash (/), HBR uses the name as a condition. All files and directories that match the condition in the source path are specified. Example 1: If the source path is */ifs/dataset* and *abc** is entered in the Enter Paths field, files and directories whose names are prefixed with abc in the */ifs/dataset* path are specified. Example 2: If the source path is */ifs/dataset* and *abc* is entered in the Enter Path field, files and directories whose names are abc in */ifs/dataset* are specified.
Start Time	The point in time at which the backup plan starts. The time is accurate to the second.
Backup Interval	The interval at which HBR performs incremental backups. Unit: hours, days, or weeks.
Retention Policy	The retention period of the backup data. - **Limited**: The backup data is stored for a specified period of time. Unit: days, weeks, months, or years. - **Permanent**: The backup data is permanently stored.

b. Optional. Click **Show Advanced Settings** and set the parameters. The following table describes the parameters.

Parameter	Description
Switch to full backup when incremental backup fails	If you turn on this switch, an incremental backup is automatically converted to a full backup when the incremental backup fails. An incremental backup may fail because of the following reasons: ■ The backup rule that specifies files of the backup plan is modified. ■ Data that is last backed up to the backup vault expires. ■ The snapshot that was last created for the Isilon (PowerScale) instance is deleted.
Backup Sub-task Slice Size	You can add multiple HBR clients into a backup client group. Then, the clients can concurrently run a backup job. If you set this parameter, the number of files that are backed up by a client is greater than or equal to the value of this parameter.

If you want to create more backup plans for the NAS file system, click **New Backup Plan** in the Actions column on the **NAS Instance** tab.

After the backup plan is created, you can view the status of each backup job on the **Backup Jobs** tab.

What's next

Restore files to a local NAS file system

2.4. Restore files to a local NAS file system

You can restore files that are backed up on an HBR backup client to a local NAS file system. You can also restore files that are backed up on another backup client in the same backup vault to the NAS file system.

Prerequisites

The local NAS file system is backed up. For more information, see Back up an on-premises NAS file system.

Create a restore job

1.
2. In the left-side navigation pane, choose **Backup > NAS Backup**.
3. On the left side of the top navigation bar, select a region.
4. On the **NAS Backup** page, click **Local NAS**.
5. On the **NAS Instance** tab, click the + icon next to a NAS file system that is backed up.
6. Click a backup and click **Restore**.

   You can also click **Browse** to view all the files on the client that you can restore.

7. In the **Create Subscription** dialog box, set the following parameters and click **OK**.

   i. Select the files that you want to restore and click **Next**.

      The following restore policies are supported:

      - **Include All Files**: All files on the client are restored.
      - **Include Files** or **Exclude Files**: You can select or enter the paths of directories or files that you want to include in or exclude from the restore job. HBR restores files on the client based on the specified restore policy.
        - Select the files that you want to include in or exclude from the restore job

          You can select files by using one of the following two methods:

          - Browse all the files that are backed up from the NAS file system and select the files that you want to include in or exclude from the restore job.
          - Enter the file names in the **Search** box and turn on **Advanced**.

            To search for files, you can specify one or more of the following conditions: **Search Type**, **Min Size**, **Max Size**, and **Modify Time**. For example, if you want to restore a file whose name is test.txt, enter test.txt in the Search box and click Search. After you click Search, the test.txt file is returned.

        - Specify the files that you want to include in or exclude from the restore job

          Enter one path in each line and make sure that each path starts with the lowest-level directory in the source path that is backed up.

          - Restore specific files

            For example, if you want to restore the file.txt and abc.png files in the *folder/test/data* directory, enter the following paths:

            ```
            /data/file.txt /data/abc.png
            ```

          - Restore specific directories

            For example, if you want to restore all the files and subdirectories in the *folder/test/data* directory, enter the following path:

            ```
            /data/
            ```

          - Restore files or directories that match a condition including wildcards

            For example, if you want to restore the files and subdirectories whose names are prefixed with abc in the *folder/test/data* directory, enter the following path:

            ```
            /data/abc*
            ```

   ii. In the **Restore Destination** step, set the Destination Type parameter to **Local NAS**. Select an existing NAS file system to which you want to restore files, and then click **Next**.

       You can also add a new NAS instance to restore the files.

   iii. In the **Destination Path** step, specify the Restore Path Type and **Destination Path** parameters.

   After a restore job is created, you can view the job progress in the **Status** column on the **Restore Jobs** tab.

3.Use file backup

3.1. Back up NFS NAS using ECS file backup

3.1.1. Overview

You can use an ECS backup client of HBR to back up NFS NAS files in an ECS instance and restore the files when they are lost or damaged.

For more information about how to use an ECS file backup client to back up NFS NAS files, see the following topics:

- Prepare for a data backup
- Back up NAS files
- Restore NAS files

3.1.2. Prepare for a data backup

You can use Hybrid Backup Recovery (HBR) to back up the data of an Apsara File Storage NAS Network File System (NFS) file system and restore the data based on your business requirements. This topic describes how to prepare for a data backup.

Step 1: Create and assign the AliyunServiceRoleForHbrEcsBackup role

Before you use HBR to back up files from ECS, you must create the AliyunServiceRoleForHbrEcsBackup role and assign the role to HBR. To create and assign the role, perform the following steps:

1.
2. In the left-side navigation pane, choose **Backup > ECS File Backup**.
   In the dialog box that appears, create and assign the role as prompted.
3. In the **Hybrid Cloud Backup Service Authorization** dialog box, click **Confirm Authorization**.

   For more information, see Service-linked roles.

Step 2: Install Cloud Assistant

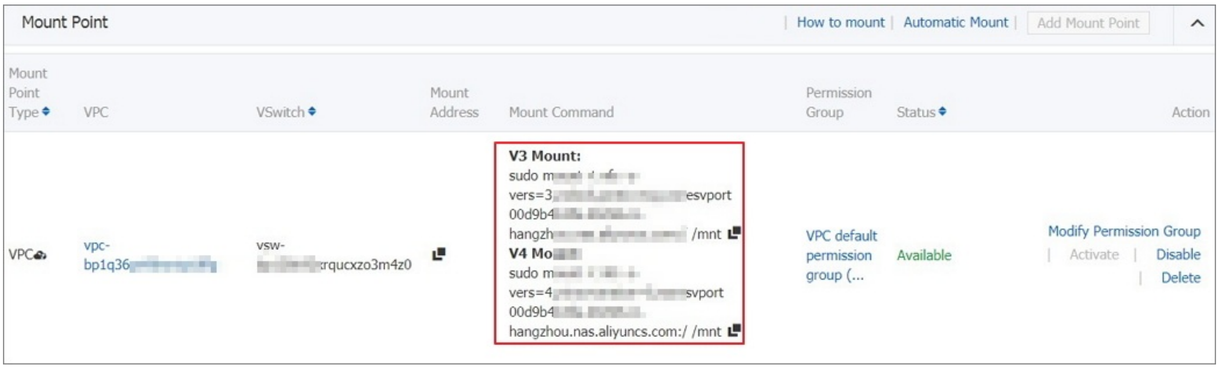
An HBR backup client for ECS must be used together with Cloud Assistant.

- If the ECS instance that you need to back up was purchased before December 1, 2017, you must install the Cloud Assistant client. For more information, see Install the Cloud Assistant client.
- If the ECS instance that you need to back up was purchased on or after December 1, 2017, the Cloud Assistant client is pre-installed.

Step 3: Create a mount target

In the NAS console, create a VPC mount target for the NFS file system. For more information, see Create a mount target.

After the mount target is created, you can perform the following steps to view the path of the mount target: In the NAS console, find the NFS file system, and click **Manage** in the Actions column. In the left-side navigation pane of the page that appears, click Mounting Use. On the Mount Target page, view the path of the mount target.



Mount Point Type	VPC	VSwitch	Mount Address	Mount Command	Permission Group	Status	Action
VPC	vpc- bp1q36[redacted]	vsw- [redacted]rqucxzo3m4z0		**V3 Mount:** sudo m[redacted] vers=3,[redacted]esvport 00d9b4[redacted] hangzh[redacted] /mnt **V4 Mo**[redacted] sudo m[redacted] vers=4[redacted]svport 00d9b4[redacted] hangzhou.nas.aliyuncs.com:/ /mnt	VPC default permission group (...	Available	Modify Permission Group Activate | Disable Delete

Step 4: Create an Elastic Compute Service (ECS) instance

Create an ECS instance in the VPC where the mount target of the NFS file system resides. For more information, see Create an instance by using the wizard. In this example, CentOS is used.

Step 5: Mount the NAS NFS file system on the ECS instance

Procedure

1. Run the **sudo yum install nfs-utils** command to install the NFS client. For more information about how to install an NFS client in Linux, see Mount an NFS file system on a Linux ECS instance.
2. After the NFS client is installed, install the NAS NFS file system on the NFS client. For more information, see Mount an NFS file system on a Linux ECS instance.

What's next

Back up NAS files

3.1.3. Back up NAS files

You can use Hybrid Backup Recovery (HBR) to back up Apsara File Storage Network Attached Storage (NAS) files from Elastic Compute Service (ECS) instances and restore these files if they are lost or damaged. This topic describes how to back up NAS files from an ECS instance.

Prerequisites

Preparations are completed.

Step 1: Create an ECS file backup client

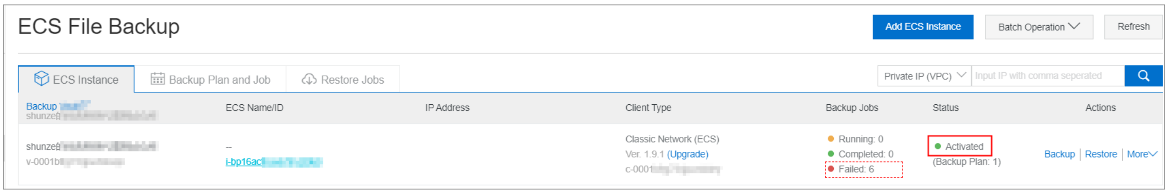
To create an ECS file backup client, follow these steps:

1. Log on to the HBR console.
2. In the left-side navigation pane, choose **Backup > ECS File Backup**.
3. In the top navigation bar, select the region where the ECS instance to be backed up resides.
4. On the ECS File Backup page, click the **ECS Instance** tab. On the ECS Instance tab, click **Add ECS Instance** in the upper-right corner.
5. In the **Add ECS Instance** pane that appears, select an existing backup vault or select **Create**

Vault to create one. Then, select the ECS instance that you created in preparations.

6. Click **Create**.

   Wait for several minutes until the status of the target ECS instance becomes Activated on the **ECS Instance** tab.



ECS File Backup

Backup [redacted] shunze[redacted]	ECS Name/ID	IP Address	Client Type	Backup Jobs	Status	Actions
shunze[redacted] v-0001b[redacted]	-- i-bp16ac[redacted]		Classic Network (ECS) Ver. 1.9.1 (Upgrade) c-0001[redacted]	● Running: 0 ● Completed: 0 ● Failed: 6	● Activated (Backup Plan: 1)	Backup | Restore | More

Step 2: Create a backup plan

After the ECS file backup client is created, follow these steps to create a backup plan:

1. On the ECS Instance tab, find the target ECS instance and click **Backup** in the Actions column.
2. In the **Create Backup Plan** pane that appears, set parameters as required and click **OK**.

   The following table describes the parameters.

Parameter	Description
Plan Name	The name of the backup plan. If you do not specify this parameter, a random name is set by default.
Source File Path	The path of the mount point for the NAS file system.
Start Time	The start time of the backup plan. The time is accurate to seconds.
Plan Run Interval	The interval for backing up incremental data. Valid units: hours, days, and weeks.
Retention	The retention period of backup data. Valid units: days, weeks, months, and years.
Using Flow Control	Specifies whether to enable throttling. You can enable throttling to set bandwidth limits for backing up data from a directory during peak hours. This guarantees business continuity. **Note** If you set the value to **Use**, select a throttling period and enter the maximum bandwidth that can be used for backup during the throttling period based on business requirements. Then, click **Add**.

   After the backup plan is created, you can check it on the **Backup Plan and Job** tab. A NAS backup job starts based on the configured backup plan. You can also click **Execute** to run a backup job immediately.

Then, you can check the progress of the backup job on the **Backup Plan and Job** tab.

3.1.4. Restore NAS files

You can restore Apsara File Storage NAS files to the source Elastic Compute Service (ECS) instance or another ECS instance that uses the same backup vault. You can also restore NAS files that are backed up by using a backup client for on-premises files to an ECS instance.

Procedure

1. Log on to the Hybrid Backup Recovery (HBR) console.
2. In the left-side navigation pane, choose **Backup > ECS File Backup**.
3. On the **ECS Instances** tab, find the destination ECS instance, and click **Restore** in the **Actions** column.
4. In the **Create Restore Job** pane, set the Restore From parameter to one of the following values:
   - **Current ECS Instance**

     Select this option if you need to restore files from the current ECS instance. Then, perform the following steps:

     a. Click **Next**.

     b. In the Select Backup step, select a backup and click **Next**.

     c. In the Configure Restore Policy step, enter a destination path, select a restore policy, specify the files that you want to restore based on the policy, and then click **Create**.
   - **Other ECS Instance**

     Select this option if you need to restore files from another ECS instance that uses the same backup vault as the current ECS instance. Then, perform the following steps:

     a. Select the source ECS instance and click **Next**.

     b. In the Select Backup step, select a backup and click **Next**.

     c. In the Configure Restore Policy step, enter a destination path, select a restore policy, specify the files that you want to restore based on the policy, and then click **Create**.
   - **On-premises Server**

     Select this option if you need to restore NAS files that are backed up by using a backup client for on-premises files. Then, perform the following steps:

     a. Select the client that is used to back up files from the on-premises server and click **Next**.

     b. In the Select Backup step, select a backup and click **Next**.

     c. In the Configure Restore Policy step, enter a destination path, select a restore policy, specify the files that you want to restore based on the policy, and then click **Create**.

> **Note** You can view the progress of a restore job on the **Restore Jobs** tab of the **ECS File Backup** page.

3.2. Back up SMB file systems by using backup clients for ECS

3.2.1. Overview

You can use Hybrid Backup Recovery (HBR) backup clients for Elastic Compute Service (ECS) to back up files from Server Message Block (SMB) file systems of Apsara File Storage NAS. You can then restore the files if they are lost or damaged.

You can use the following procedure to back up files from an SMB file system:

- Preparations
- Back up NAS files
- Restore NAS files

3.2.2. Preparations

You can use Hybrid Backup Recovery (HBR) to back up files from Server Message Block (SMB) file systems of Apsara File Storage NAS. You can then restore the files if needed. This topic describes the preparations that you must make before backup.

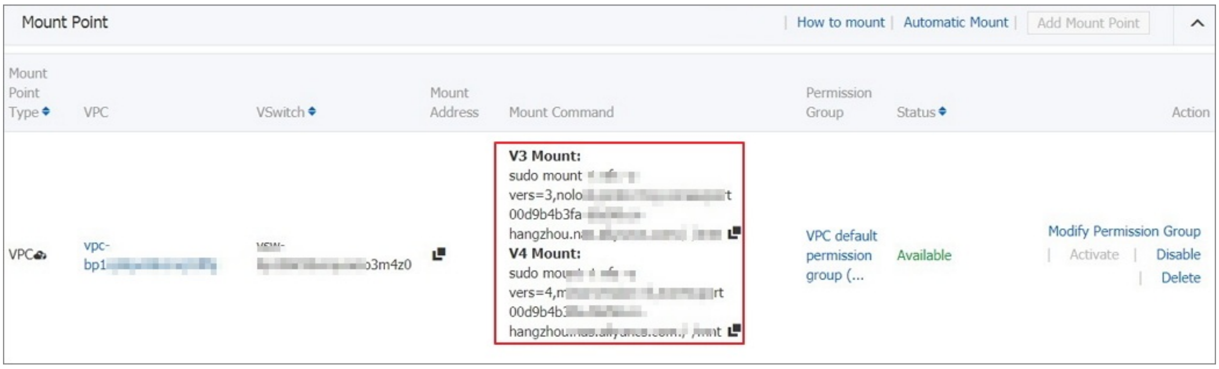
Step 2: Install and configure Cloud Assistant

A backup client for ECS requires interaction with Cloud Assistant. By default, Cloud Assistant is installed on ECS instances that are created after December 1, 2017. However, you must manually install Cloud Assistant on ECS instances that are created before December 1, 2017.

Step 3: Create a mount target

Log on to the NAS console and create a VPC mount target for the SMB file system that you want to back up. For more information, see Create a mount target.

After the mount target is created, you can perform the following steps to view the path to the mount target: Find the SMB file system in the NAS console, and click **Management** in the Operations column. In the left-side navigation pane of the page that appears, click Mounting Use. You can view the path on the Mount Target page.



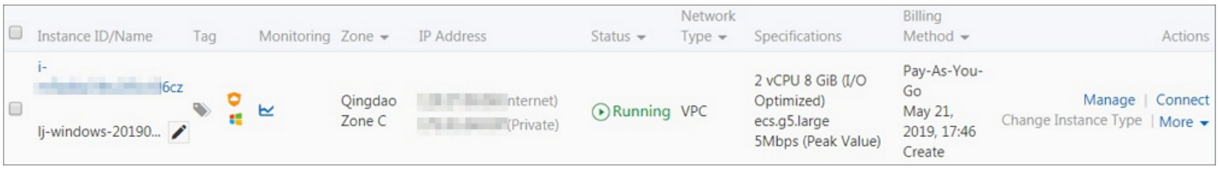
Mount Point | How to mount | Automatic Mount | Add Mount Point

Mount Point Type	VPC	VSwitch	Mount Address	Mount Command	Permission Group	Status	Action
VPC	vpc-bp1[redacted]	[redacted]3m4z0		**V3 Mount:** sudo mount [redacted] vers=3,nolo[redacted]t 00d9b4b3fa[redacted] hangzhou.n[redacted] **V4 Mount:** sudo mou[redacted] vers=4,m[redacted]rt 00d9b4b3[redacted] hangzhou[redacted]nt	VPC default permission group (...	Available	Modify Permission Group Activate | Disable Delete

Step 4: Create an ECS instance

Create an ECS instance in the VPC where the mount target of the SMB file system resides. For more information, see Create an instance by using the wizard.

> **Notice** We recommend that you create an ECS instance that runs Windows 2012. If the created ECS instance runs Windows 2016, you must use HBR as the administrator due to permission control of the operating system.



□	Instance ID/Name	Tag	Monitoring	Zone	IP Address	Status	Network Type	Specifications	Billing Method	Actions
□	i-[redacted]6cz lj-windows-20190...			Qingdao Zone C	[redacted]nternet) [redacted](Private)	Running	VPC	2 vCPU 8 GiB (I/O Optimized) ecs.g5.large 5Mbps (Peak Value)	Pay-As-You-Go May 21, 2019, 17:46 Create	Manage | Connect Change Instance Type | More

3.2.3. Back up NAS files

You can use Hybrid Backup Recovery (HBR) to back up Apsara File Storage NAS files from Elastic Compute Service (ECS) instances. You can then restore these files if they are lost or damaged. This topic describes how to back up NAS files from an ECS instance.

Prerequisites

Preparations are completed.

Step 1: Install a backup client for ECS files

To create a file backup client for an ECS instance, perform the following steps:

1. Log on to the HBR console.
2. In the left-side navigation pane, choose **Backup > ECS File Backup**.
3. In the top navigation bar, select the region where the ECS instance resides.
4. In the upper-right corner of the **ECS Instances** tab, click **Add ECS Instance**.
5. In the **Add ECS Instance** pane, select an existing backup vault. If you need to create a backup vault, click **Create Vault**. Then, select the ECS instance that you created in Preparations.
6. Click **Create**.

   Wait for several minutes until the status of the ECS instance becomes Activated on the **ECS Instances** tab.

Step 2: Create a backup plan

After the backup client for ECS files is installed, perform the following steps to create a backup plan:

1. On the ECS Instances tab, find the ECS instance, and click **Back Up** in the Actions column.
2. In the **Create Backup Plan** pane, set the parameters and click **OK**.

   Notice Volume Shadow Copy Service (VSS) is not supported for backup of files from NAS file systems.

   The following table describes the parameters.

Parameter	Description
Plan Name	The name of the backup plan. By default, a random name is used.
Source Paths	The paths to the source files in the file system.
Start Time	The start time of the backup plan. The time is accurate to seconds.

Parameter	Description
Backup Interval	The interval at which data backup is performed. Unit: hours, days, or weeks.
Retention Period	The retention period of the backup data. Unit: days, weeks, months, or years.
Throttle Bandwidth	Specifies whether to throttle the bandwidth. You can throttle the bandwidth that is used for data backup during peak hours. This guarantees business continuity. ? **Note** If you select **Yes**, you must set the Throttling Period (Hour) and Max Bandwidth parameters. Then, click **Add**.

After the backup plan is created, you can view the backup plan on the **Backup Plans and Jobs** tab. Backup jobs run based on the backup plan. You can also click **Run Immediately** to immediately run a backup job.

You can view the progress of backup jobs on the **Backup Plans and Jobs** tab.

3.2.4. Restore NAS files

You can restore Apsara File Storage NAS files to the source Elastic Compute Service (ECS) instance or another ECS instance that uses the same backup vault. You can also restore NAS files that are backed up by using a backup client for on-premises files to an ECS instance.

Procedure

1. Log on to the Hybrid Backup Recovery (HBR) console.
2. In the left-side navigation pane, choose **Backup > ECS File Backup**.
3. On the **ECS Instances** tab, find the destination ECS instance, and click **Restore** in the **Actions** column.
4. In the **Create Restore Job** pane, set the Restore From parameter to one of the following values:
    - **Current ECS Instance**

      Select this option if you need to restore files from the current ECS instance. Then, perform the following steps:

      a. Click **Next**.
      b. In the Select Backup step, select a backup and click **Next**.
      c. In the Configure Restore Policy step, enter a destination path, select a restore policy, specify the files that you want to restore based on the policy, and then click **Create**.
    - **Other ECS Instance**

      Select this option if you need to restore files from another ECS instance that uses the same backup vault as the current ECS instance. Then, perform the following steps:

   a. Select the source ECS instance and click **Next**.
   b. In the Select Backup step, select a backup and click **Next**.
   c. In the Configure Restore Policy step, enter a destination path, select a restore policy, specify the files that you want to restore based on the policy, and then click **Create**.

- **On-premises Server**

  Select this option if you need to restore NAS files that are backed up by using a backup client for on-premises files. Then, perform the following steps:

   a. Select the client that is used to back up files from the on-premises server and click **Next**.
   b. In the Select Backup step, select a backup and click **Next**.
   c. In the Configure Restore Policy step, enter a destination path, select a restore policy, specify the files that you want to restore based on the policy, and then click **Create**.

> ? **Note** You can view the progress of a restore job on the **Restore Jobs** tab of the **ECS File Backup** page.

3.2.5. Grant HBR the permissions to read data from SMB file systems in NAS

Hybrid Backup Recovery (HBR) does not have the permissions to read data from a Server Message Block (SMB) file system. This file system is based on Active Directory (AD) permission control. Therefore, HBR cannot be used to back up the data of SMB file systems. To back up the data of SMB file systems, you first must grant HBR the permissions to read data from the SMB file systems. This topic describes how to grant HBR the permissions to read data from SMB file systems on a Windows-based Elastic Compute Service (ECS) instance.

Context

- You cannot use HBR to back up the data of an SMB file system that is based on AD permission control. HBR has no permissions to read data from the file systems. To fix this issue, we recommend that you mount the SMB file system to a Windows-based ECS instance. Then, you can authorize HBR to access the SMB file system.
- Before you start the following procedure, you must install a file backup client for ECS. For more information about the billing of the backup client, see Hybrid Backup Recovery (HBR) Pricing.

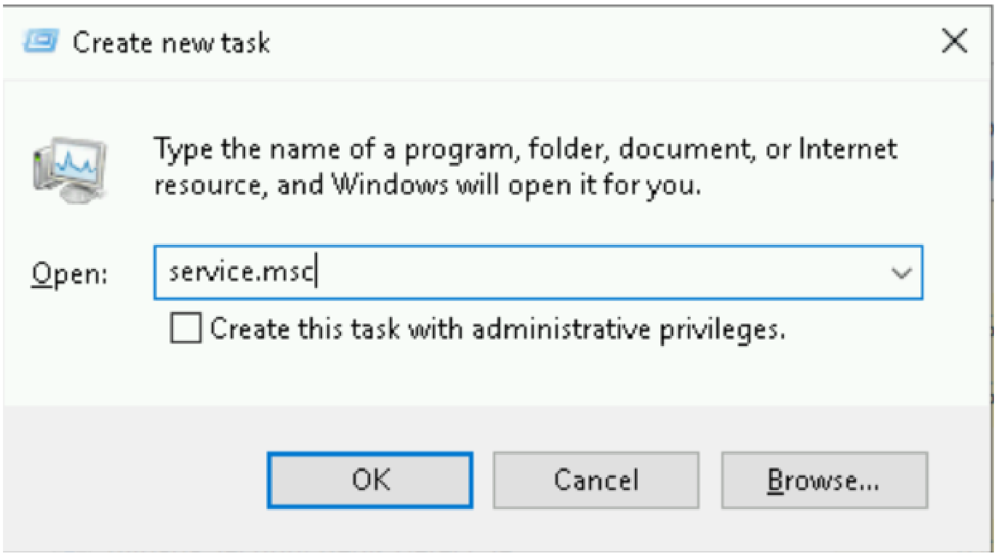
Step 1: Install a file backup client for ECS

Install a file backup client for ECS. For more information, see Step 1: Install a backup client for ECS files.

Step 2: Grant permissions to the HBR client

Perform the following steps to grant the HBR client the permissions to read files from the SMB file system.

1. Connect to the ECS instance. For more information, see Connect to an ECS instance.
2. Press `Win+R`. In the **Run** dialog box, enter `services.msc` and click **OK**.



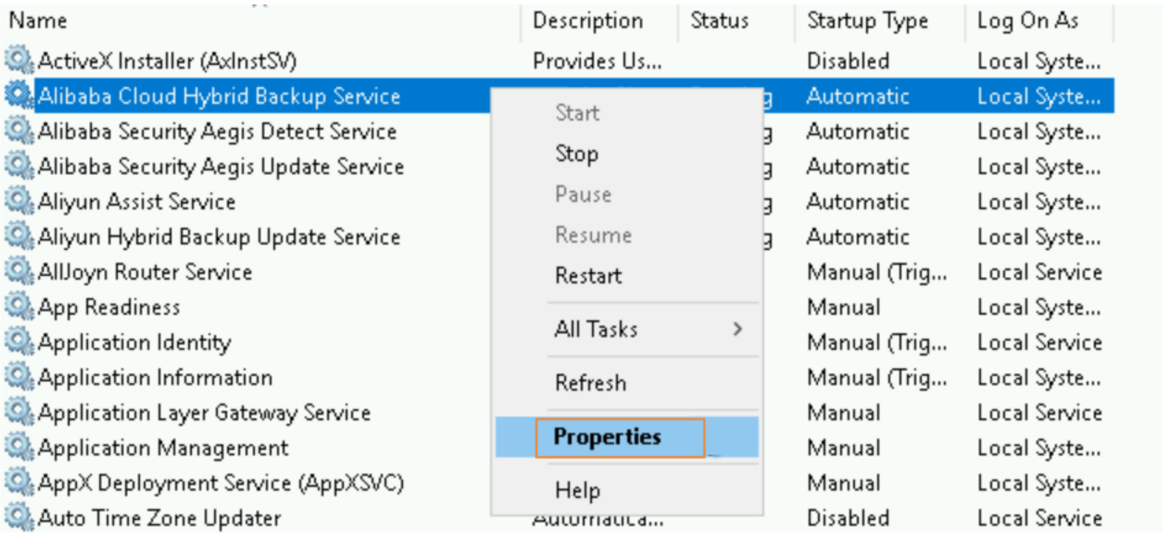
Create new task

Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: service.msc

☐ Create this task with administrative privileges.

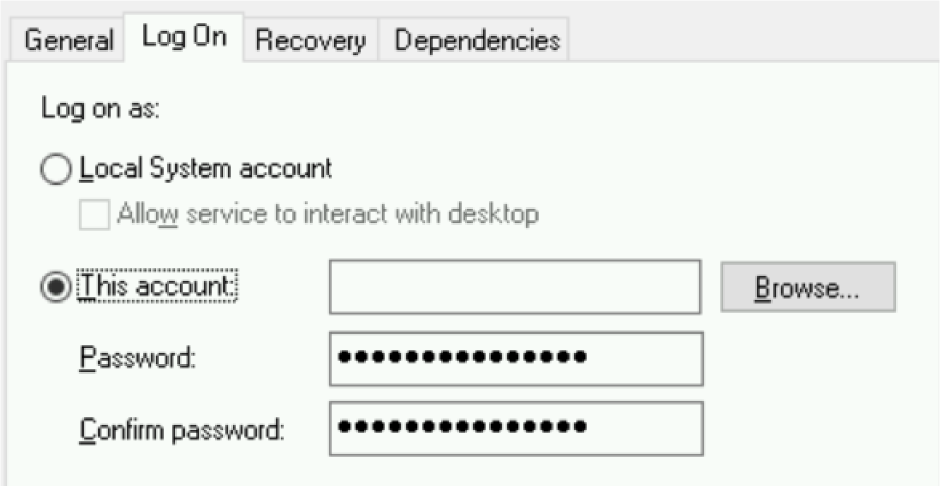
3. Find Aliyun Hybrid Backup Service in the service list. Right-click the service and select **Properties**.



Name	Description	Status	Startup Type	Log On As
ActiveX Installer (AxInstSV)	Provides Us...		Disabled	Local Syste...
Alibaba Cloud Hybrid Backup Service			Automatic	Local Syste...
Alibaba Security Aegis Detect Service			Automatic	Local Syste...
Alibaba Security Aegis Update Service			Automatic	Local Syste...
Aliyun Assist Service			Automatic	Local Syste...
Aliyun Hybrid Backup Update Service			Automatic	Local Syste...
AllJoyn Router Service			Manual (Trig...	Local Service
App Readiness			Manual	Local Syste...
Application Identity			Manual (Trig...	Local Service
Application Information			Manual (Trig...	Local Syste...
Application Layer Gateway Service			Manual	Local Service
Application Management			Manual	Local Syste...
AppX Deployment Service (AppXSVC)			Manual	Local Syste...
Auto Time Zone Updater	Automatica...		Disabled	Local Service

4. In the dialog box that appears, click the **Log On** tab.

5. Select **This account**, click browse, and then enter the account and password to gain full access to the SMB system. Click **OK**.



Log on as:

○ Local System account

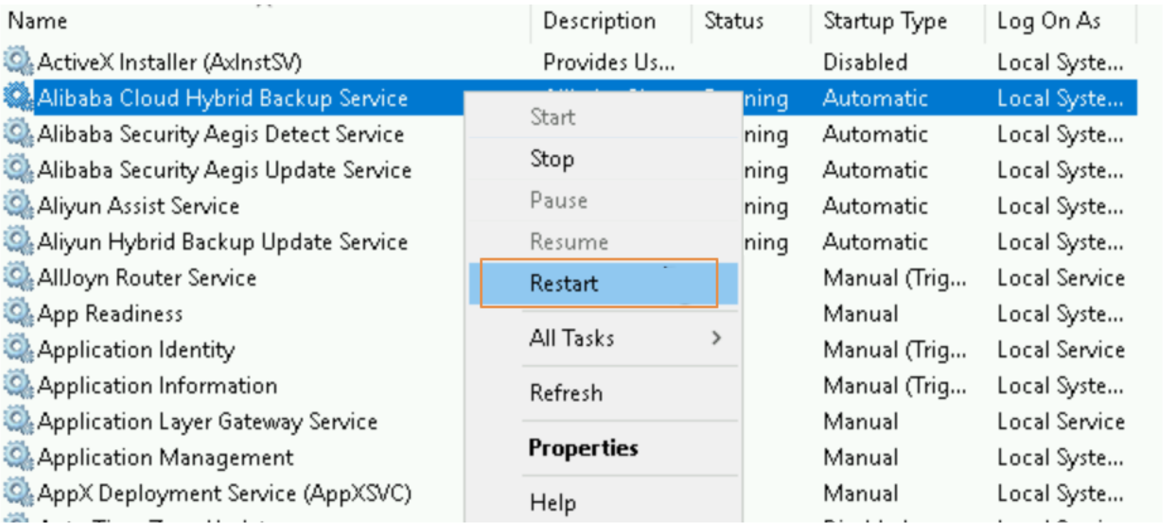
☐ Allow service to interact with desktop

● This account:

Password: ●●●●●●●●●●●●●●●

Confirm password: ●●●●●●●●●●●●●●●

6. Restart Aliyun Hybrid Backup Service.



Name	Description	Status	Startup Type	Log On As
ActiveX Installer (AxInstSV)	Provides Us...		Disabled	Local Syste...
Alibaba Cloud Hybrid Backup Service		ning	Automatic	Local Syste...
Alibaba Security Aegis Detect Service		ning	Automatic	Local Syste...
Alibaba Security Aegis Update Service		ning	Automatic	Local Syste...
Aliyun Assist Service		ning	Automatic	Local Syste...
Aliyun Hybrid Backup Update Service		ning	Automatic	Local Syste...
AllJoyn Router Service			Manual (Trig...	Local Service
App Readiness			Manual	Local Syste...
Application Identity			Manual (Trig...	Local Service
Application Information			Manual (Trig...	Local Syste...
Application Layer Gateway Service			Manual	Local Service
Application Management			Manual	Local Syste...
AppX Deployment Service (AppXSVC)			Manual	Local Syste...

Step 3: Create a backup plan

Create a backup plan. For more information, see Step 2: Create a backup plan.

3.3. Back up NFS file systems by using HBR backup clients for on-premises files

3.3.1. Overview

You can use Hybrid Backup Recovery (HBR) backup clients for on-premises files to back up files from user-created Network File System (NFS) file systems. You can then restore the files if they are lost or damaged.

> **Note** This backup method is only applicable to regions where ECS backup is not supported. For regions that support ECS backup, we recommend that you use an HBR backup client for ECS to back up files from NFS file systems.

You can use the following procedure to back up files from an NFS file system:

- Preparations
- Back up NAS files
- Restore NAS files

3.3.2. Preparations

You can use Hybrid Backup Recovery (HBR) backup clients for on-premises files to back up files from user-created Network File System (NFS) file systems. You can then restore the files if they are lost or damaged. This topic describes the preparations that you must make before backup.

Prerequisites

An NFS file system is created.

Background information

Before you use HBR to back up files from an NFS file system, note the following information:

- To achieve the optimal backup performance, we recommend that you run a backup client on a host that has the following configurations: 64-bit processors, two or more CPU cores, and more than 8 GB available memory.
- The volume of data that can be backed up depends on the available memory. If a host has 4 GB available memory, a maximum of one million files or 8 TB data can be backed up.

(Recommended) Prepare an AccessKey pair for a RAM user

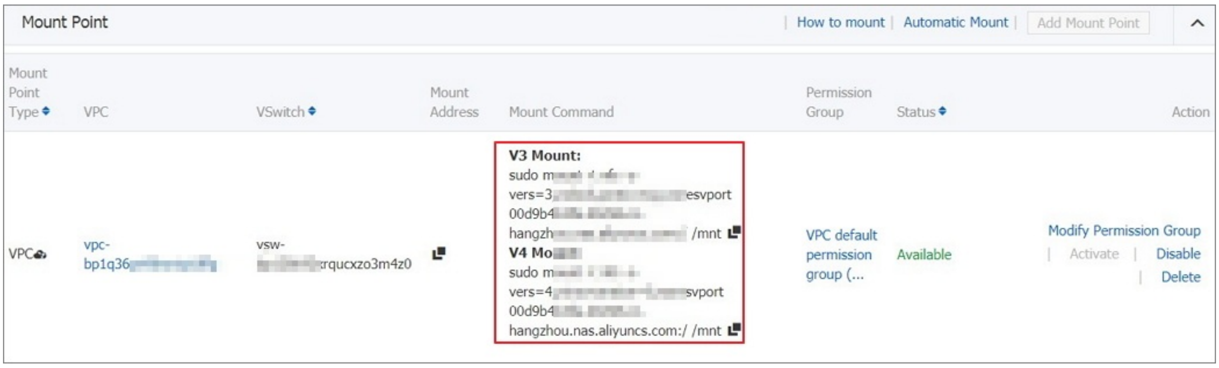
Resource Access Management (RAM) is a service provided by Alibaba Cloud. It allows you to create and manage multiple identities under an Alibaba Cloud account and then grant diverse permissions to a single identity or a group of identities. In this way, you can authorize different identities to access different Alibaba Cloud resources.

An AccessKey pair is required when you activate a backup client. The AccessKey pair is an identity credential. If an AccessKey pair of your Alibaba Cloud account is used, all cloud resources that belong to the account are exposed to risks. Therefore, we recommend that you use an AccessKey pair of a RAM user to activate backup clients. Before you back up data, make sure that a RAM user is created and an AccessKey pair is created for the RAM user. For more information, see Create a RAM user and Create an AccessKey pair for a RAM user.

Step 1: Create a mount target

Log on to the NAS console and create a mount target for the NFS file system that you want to back up. For more information, see Create a mount target.

On the **Mount Target** page of the file system, verify that the mount target is created.



Mount Point Type	VPC	VSwitch	Mount Address	Mount Command	Permission Group	Status	Action
VPC	vpc- bp1q36[redacted]	vsw- [redacted]rqucxzo3m4z0		**V3 Mount:** sudo m[redacted] vers=3[redacted]esvport 00d9b4[redacted] hangzh[redacted] /mnt **V4 Mo**[redacted] sudo m[redacted] vers=4[redacted]svport 00d9b4[redacted] hangzhou.nas.aliyuncs.com:/ /mnt	VPC default permission group (...	Available	Modify Permission Group | Activate | Disable | Delete

Step 2: Mount the NFS file system

After the mount target is created, perform the following steps to mount the NFS file system:

1. Install an NFS client.

   For more information about how to install an NFS client in the Linux operating system, see Mount an NFS file system on a Linux ECS instance.

2. Mount the NFS file system.

   For more information, see Mount an NFS file system on a Linux ECS instance.

Step 3: Create a backup client for files

Notice

- The host that runs the backup client for files must have access to the Internet. If the host is an Elastic Compute Service (ECS) instance, the ECS instance can access the Internet by using an elastic IP address (EIP) or a Network Address Translation (NAT) gateway.
- Only a small number of commands are sent over the Internet, which incurs few traffic fees.

Before you back up and restore files, you must install a backup client for files on the host of the NFS client. To create a backup client for files in the HBR console and download the installation package of the client, perform the following steps:

1. Log on to the HBR console.

   If the host of the NFS client runs a Linux operating system without a graphical user interface (GUI), use an intermediate host with a GUI as an agent to log on to the HBR console.

2. In the left-side navigation pane, choose **Backup > On-Premises Backup > File**.
3. In the top navigation bar, select the region where you want to store backup data.

   Note

   - If you use a virtual private cloud (VPC), select the region of the VPC. This guarantees a high backup speed.
   - If you do not use a VPC and you need to achieve optimal backup performance, select a region that is close to the location of the data that you want to back up.
   - If you do not use a VPC and you need to implement disaster recovery, select a region that is distant from the location of the data that you want to back up.

4. In the upper-right corner of the On-Premises Backup page, click **Add Client**.
5. In the **Add Client** pane, set the parameters.

Parameter	Description
Backup Vault	The backup vault where you want to store the backup data. A backup vault is a repository that HBR uses to store backup data. You can use a single vault to store backup data that is received from multiple backup clients. Backup vaults reside in different regions. You can select or create only a backup vault in the current region. ◦ If you have created backup vaults, click **Select Vault**, and select a backup vault from the **Vault Name** drop-down list. ◦ If you have not created backup vaults, click **Create Vault** and specify the **Vault Name** field. The name must be 1 to 64 characters in length.
Backup Client	The backup client that you want to add. You can select an activated client or create a client.
Client Name	The name of the backup client. The name must be 1 to 64 characters in length.

Parameter	Description
Software Platform	The operating system that is running on the server or VM from which you want to back up data. Valid values: ○ Windows 32-bit ○ Windows 64-bit ○ Linux 32-bit ○ Linux 64-bit
Network Type	○ **Virtual Private Cloud (VPC)**: Select this option if the server or VM from which you want to back up data resides in a VPC and the VPC is in the same region as the backup vault. ○ **Internet**: Select this option if no VPCs are available.
Use HTTPS	Specifies whether to use HTTPS for encrypted data transmission. Note that HTTPS compromises the performance of data transmission. Data that is stored in the backup vault is encrypted, regardless of the setting of this switch. If you modify the setting of this parameter, the modification takes effect on the next restore job.

6. Click **Create**. Then, click **Download Client**.

> **Note** The backup client is used to connect the host of the NFS client to HBR. You can also download the backup client from the client list.

Step 4: Install and activate the backup client

After you download the installation package of a backup client for files, perform the following steps to install and activate the backup client:

1. Run the **tar -xzvf hbr-install-xxx-linux-amd64.tar.gz** command to decompress the installation package to a specified directory. Then, run the **./setup** command to install the backup client.

> **Note** Make sure that enough space is available in the installation directory because both operational logs and an executable file are saved in the installation directory.

2. Activate the backup client. Go to the HBR console. In the **Add Client** pane, click **Next**. In the Activate Client step, set the parameters. The following table describes the parameters.

Parameter	Required	Description

Parameter	Required	Description
Client IP Address	Yes	The IP address of the backup client that your current host can access. You can specify an internal IP address or an Internet IP address. For example, the IP address can be 127.0.0.1 (default), 12.34.56.78:8011, or 87.65.43.21:8443. **Note** The IP address must be reachable from your browser in use.
AccessKey Id	Yes	The AccessKey ID and AccessKey secret of the RAM user that is used to access HBR. For more information, see How can I create an AccessKey pair for a RAM user?.
AccessKey Secret	Yes	
Client Password	Yes	The password that is used to log on to the backup client. The password must be at least six characters in length.
Data Network Proxy	No	The information of the proxy server that is used to transmit backup data. **Note** You can configure a data network proxy only for a backup client whose version is 1.11.11 or later.
Control Network Type	No	The type of the network that is used to call the HBR API.
Control Network Proxy	No	The information of the proxy server that is used to call the HBR API.
Message Network Type	No	The type of the network that is used to send messages from HBR to the backup client.

3. Click **Activate Client**. The page of the backup client for files appears. You can then use the backup client to back up data.

> **Note** If the activation of a backup client fails, you can reactivate the client. For more information, see How can I reactivate a file backup client?

3.3.3. Back up NAS files

You can use an HBR backup client for files to back up files from user-created Network File System (NFS) file systems. HBR provides the two types of backup plans: instant and scheduled. This topic describes how to back up files from user-created NFS file systems.

Create an instant backup plan

If you need only one-time full backup, perform the following steps to create an instant backup plan:

1. Log on to an HBR backup client.
2. In the left-side navigation pane, click Backup. In the upper-right corner of the Backup Jobs page, click **Create Backup Job**.
3. On the **Basic Settings** tab of the **Create Backup Job** dialog box, set the parameters. The following table describes the parameters.
    - Source : Enter the path to the mount target of the NAS file system.
    - Running Plan : Select **Instant**.

    > Notice Volume Shadow Copy Service (VSS) is not supported for NAS backup.

4. Optional. Click the **Bandwidth Throttling** tab. Set **Work Hours**. In the Throttling field, enter the maximum bandwidth that can be used for backup during the specified throttling period. Then, click **Add**.

    > Note
    > - The throttling period is accurate to the hour. You can add multiple throttling periods based on your requirements.
    > - If you need to modify a throttling period, find the throttling period, click **Delete** in the Actions column, and then add a throttling period.
    > - The maximum bandwidth must be at least 1 MB/s.

5. Click **Submit**.

    > Note After a backup job is started, you can perform the following operations on the **Backup Jobs** page:
    > - View the progress of the backup job.
    > - Click **Cancel** or **Retry** in the **Actions** column to cancel or retry the backup job.
    > - If the backup of some files fail, click the **Download** icon in the Errors column to download the error report.

Create a scheduled backup plan

If you need scheduled backup, perform the following steps to create a scheduled backup plan:

1. Open a browser and enter `http://localhost:8011` in the address bar. On the page that appears, enter the password to log on to the HBR backup client for files.

    > Note
    > - If you are using an intermediate host, replace `localhost` with the IP address of the NAS client host.
    > - Port 8011 is the default port that you can use for logon to a backup client for files. If port 8011 on the host of the backup client is occupied by another application, you can specify another port number for the backup client.

2. In the left-side navigation pane, click **Backup Policies**.
3. In the upper-right corner of the **Backup Polices** page, click **Create Policy**.
4. In the **Create Policy** dialog box, set the Name and other parameters.

Parameter	Description
Name	The name of the backup policy.
Frequency	The interval at which backup is performed. Units: ○ Hours. Valid values: 1 to 23. ○ Days. Valid values: 1 to 6. ○ Weeks. Valid values: 1 to 4.
Backup Time	The time to start the first backup. The first backup is a full backup.
Retention	○ The retention period of backup data. Units: days, months, or years. ○ Maximum retention period: 3650 days (10 years).

5. Click **Submit**.

   After the scheduled backup policy is created, perform the following steps to start a scheduled backup job:

   i. Log on to the HBR backup client for files.
   ii. In the left-side navigation pane, click **Backup**.
   iii. In the upper-right corner of the Backup Jobs page, click **Create Backup Job**.
   iv. In the **Create Backup Job** dialog box, click the **Basic Settings** tab. If you are creating a backup job for a user-created NFS file system, set the following parameters:
      - Source : Enter the path to the mount target of the NAS file system.
      - Running Plan : Select **Scheduled**.
      - Backup Policy : Select the created backup policy.

      Notice VSS is not supported for NAS backup.

v. Optional. Click the **Bandwidth Throttling** tab. Set **Work Hours**. In the Throttling field, enter the maximum bandwidth that can be used for backup during the specified throttling period. Then, click **Add**.

> Note
>
> - The throttling period is accurate to the hour. You can add multiple throttling periods based on your requirements.
> - If you need to modify a throttling period, find the throttling period, click **Delete** in the Actions column, and then add a throttling period.
> - The maximum bandwidth must be at least 1 MB/s.

vi. Click **Submit**.

> Note After a backup job is started, you can perform the following operations on the **Backup Jobs** page:
>
> - View the progress of the backup job.
> - Click **Cancel** or **Retry** in the **Actions** column to cancel or retry the backup job.
> - Click **Delete** in the **Actions** column to delete the backup job. After you delete the backup job, HBR no longer runs the backup job based on the specified backup policy. However, HBR retains the backups that are created by the backup job. You can still restore data from these backups.
> - If the backup of some files fail, click the **Download** icon in the Errors column to download the error report.

3.3.4. Restore NAS files

You can restore files to the source server or virtual machine (VM). You can also restore files to a server or VM that is different from the backup source.

Restore files to the source client

To restore files to the source client, perform the following steps:

1. Log on to a Hybrid Backup Recovery (HBR) backup client.
2. In the left-side navigation pane, click **Restore** to open the **Restore Backup / Backups** page.
3. On the **Backups** tab, find the backup, and click **Restore** in the Actions column.
4. In the **Restore Backup** dialog box, set the parameters that are listed in the following table, select the files that you want to restore, and then click **Submit**.

Parameter	Description
Target Folder	The destination folder to which the files are restored.

Parameter	Description
File Options	○ **Include Files**: Only the selected files and folders are restored to the destination folder. ○ **Exclude Files**: Except for the selected files and folders, all other files and folders are restored to the target folder.

Restore files to a client that is different from the backup source

To restore files to a client that is different from the backup source, perform the following steps:

1. Log on to the destination HBR file backup client.
2. In the left-side navigation pane, click **Restore** to open the **Restore Backup / Backups** page.
3. In the upper-right corner of the Backups tab, click **Restore From Other Client**.
4. In the **Restore Backup** dialog box, select the source client and click **Next**.
5. Select the backup that you want to restore, and click **Next**.
6. In the Restore Backup dialog box, set the parameters that are listed in the following table, select the files that you want to restore, and then click **Submit**.

Parameter	Description
Target Folder	The folder to which the files are restored.
File Options	○ **Include Files**: Only the selected files and folders are restored to the destination folder. ○ **Exclude Files**: Except for the selected files and folders, all other files and folders are restored to the target folder.

3.4. Back up SMB file systems by using HBR backup clients for on-premises files

3.4.1. Overview

You can use Hybrid Backup Recovery (HBR) backup clients for on-premises files to back up files from user-created Server Message Block (SMB) file systems. You can then restore the files if they are lost or damaged.

> **Note** This backup method is only applicable to regions where ECS backup is not supported. For regions that support ECS backup, we recommend that you use an HBR backup client for ECS to back up files from SMB file systems.

You can use the following procedure to back up files from an SMB file system:

- Prerequisites

- Back up NAS files
- Restore NAS files

3.4.2. Prerequisites

You can use Hybrid Backup Recovery (HBR) backup clients for on-premises files to back up files from user-created Server Message Block (SMB) file systems. You can then restore the files if they are lost or damaged. This topic describes the preparations that you must make before backup.

Prerequisites

An SMB file system is created.

Background information

Before you use HBR to back up files from an SMB file system, note the following information:

- To achieve the optimal backup performance, we recommend that you run a backup client on a host that has the following configurations: 64-bit processors, two or more CPU cores, and more than 8 GB available memory.
- The volume of data that can be backed up depends on the available memory. If a host has 4 GB available memory, a maximum of one million files or 8 TB data can be backed up.

(Recommended) Prepare an AccessKey pair for a RAM user

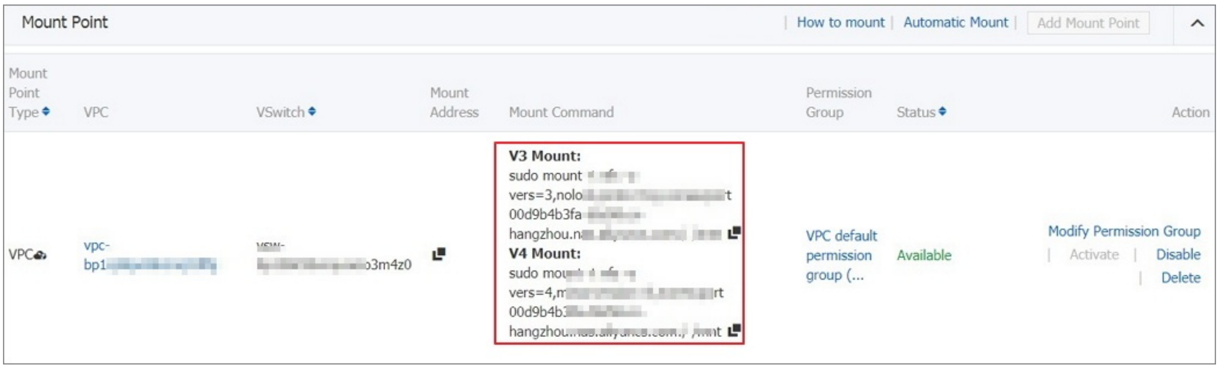
Resource Access Management (RAM) is a service provided by Alibaba Cloud. It allows you to create and manage multiple identities under an Alibaba Cloud account and then grant diverse permissions to a single identity or a group of identities. In this way, you can authorize different identities to access different Alibaba Cloud resources.

An AccessKey pair is required when you activate a backup client. The AccessKey pair is an identity credential. If an AccessKey pair of your Alibaba Cloud account is used, all cloud resources that belong to the account are exposed to risks. Therefore, we recommend that you use an AccessKey pair of a RAM user to activate backup clients. Before you back up data, make sure that a RAM user is created and an AccessKey pair is created for the RAM user. For more information, see Create a RAM user and Create an AccessKey pair for a RAM user.

Step 1: Create a mount target

Log on to the NAS console and create a mount target for the SMB file system that you want to back up. For more information, see Create a mount target.

On the **Mount Target** page of the file system, verify that the mount target is created.



Mount Point | How to mount | Automatic Mount | Add Mount Point

Mount Point Type	VPC	VSwitch	Mount Address	Mount Command	Permission Group	Status	Action
VPC	vpc-bp1[redacted]	vsw-[redacted]o3m4z0		**V3 Mount:** sudo mount [redacted] vers=3,nolo[redacted]t 00d9b4b3fa[redacted] hangzhou.n[redacted] **V4 Mount:** sudo mou[redacted] vers=4,m[redacted]rt 00d9b4b3[redacted] hangzhou[redacted]mnt	VPC default permission group (...	Available	Modify Permission Group Activate | Disable | Delete

Step 2: Create a backup client for files

Before you back up and restore files, you must install a backup client for files on the host of the SMB client. To create a backup client for files in the HBR console and download the installation package of the client, perform the following steps:

1. Log on to the HBR console.

   If the host of the SMB client runs a Linux operating system without a graphical user interface (GUI), use an intermediate host with a GUI as an agent to log on to the HBR console.

2. In the left-side navigation pane, choose **Backup > On-Premises Backup > File**.
3. In the top navigation bar, select the region where you want to store backup data.

   > Note
   >
   > - If you use a virtual private cloud (VPC), select the region of the VPC. This guarantees a high backup speed.
   > - If you do not use a VPC and you need to achieve optimal backup performance, select a region that is close to the location of the data that you want to back up.
   > - If you do not use a VPC and you need to implement disaster recovery, select a region that is distant from the location of the data that you want to back up.

4. In the upper-right corner of the On-Premises Backup page, click **Add Client**.
5. In the **Add Client** pane, set the parameters.

Parameter	Description
Backup Vault	The backup vault where you want to store the backup data. A backup vault is a repository that HBR uses to store backup data. You can use a single vault to store backup data that is received from multiple backup clients. Backup vaults reside in different regions. You can select or create only a backup vault in the current region. - If you have created backup vaults, click **Select Vault**, and select a backup vault from the **Vault Name** drop-down list. - If you have not created backup vaults, click **Create Vault** and specify the **Vault Name** field. The name must be 1 to 64 characters in length.
Backup Client	The backup client that you want to add. You can select an activated client or create a client.
Client Name	The name of the backup client. The name must be 1 to 64 characters in length.

Parameter	Description
Software Platform	The operating system that is running on the server or VM from which you want to back up data. Valid values: ◦ Windows 32-bit ◦ Windows 64-bit ◦ Linux 32-bit ◦ Linux 64-bit
Network Type	◦ **Virtual Private Cloud (VPC)**: Select this option if the server or VM from which you want to back up data resides in a VPC and the VPC is in the same region as the backup vault. ◦ **Internet**: Select this option if no VPCs are available.
Use HTTPS	Specifies whether to use HTTPS for encrypted data transmission. Note that HTTPS compromises the performance of data transmission. Data that is stored in the backup vault is encrypted, regardless of the setting of this switch. If you modify the setting of this parameter, the modification takes effect on the next restore job.

6. Click **Create**. Then, click **Download Client**.

   Note The backup client is used to connect the host of the SMB client to HBR. You can also download the backup client from the client list.

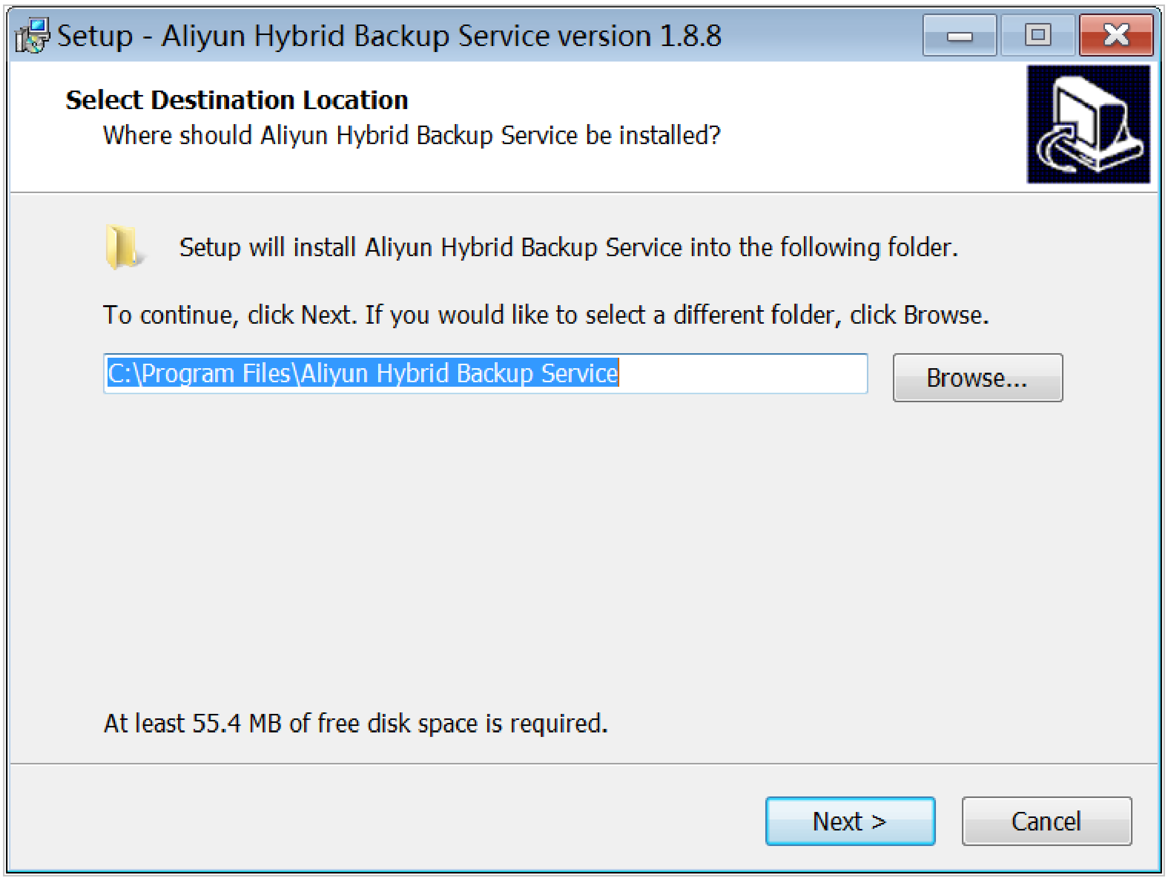
Step 3: Install and activate the backup client

Notice

- The host that runs the backup client for files must have access to the Internet. If the host is an Elastic Compute Service (ECS) instance, the ECS instance can access the Internet by using an elastic IP address (EIP) or a Network Address Translation (NAT) gateway.
- Only a small number of commands are sent over the Internet, which incurs few traffic fees.

After you download the installation package of a backup client for files, perform the following steps to install and activate the backup client:

1. Run the executable file that is decompressed from the installation package, select an installation directory, and then follow the instructions to install the backup client.



Setup - Aliyun Hybrid Backup Service version 1.8.8

Select Destination Location

Where should Aliyun Hybrid Backup Service be installed?

Setup will install Aliyun Hybrid Backup Service into the following folder.

To continue, click Next. If you would like to select a different folder, click Browse.

C:\Program Files\Aliyun Hybrid Backup Service

At least 55.4 MB of free disk space is required.

Note Make sure that enough space is available in the installation directory because both operational logs and an executable file are saved in the installation directory.

2. Activate the backup client. Go to the HBR console. In the **Add Client** pane, click **Next**. In the Activate Client step, set the parameters. The following table describes the parameters.

Parameter	Required	Description
Client IP Address	Yes	The IP address of the backup client that your current host can access. You can specify an internal IP address or an Internet IP address. For example, the IP address can be 127.0.0.1 (default), 12.34.56.78:8011, or 87.65.43.21:8443. **Note** The IP address must be reachable from your browser in use.
AccessKey Id	Yes	The AccessKey ID and AccessKey secret of the RAM user that is used to access HBR. For more information, see How can I create an AccessKey pair for a RAM user?.
AccessKey Secret	Yes	

Parameter	Required	Description
Client Password	Yes	The password that is used to log on to the backup client. The password must be at least six characters in length.
Data Network Proxy	No	The information of the proxy server that is used to transmit backup data. Note You can configure a data network proxy only for a backup client whose version is 1.11.11 or later.
Control Network Type	No	The type of the network that is used to call the HBR API.
Control Network Proxy	No	The information of the proxy server that is used to call the HBR API.
Message Network Type	No	The type of the network that is used to send messages from HBR to the backup client.

3. Click **Activate Client**. The page of the backup client for files appears. You can then use the backup client to back up data.

> **Note** If the activation of a backup client fails, you can reactivate the client. For more information, see How can I reactivate a file backup client?

3.4.3. Back up NAS files

You can use an HBR backup client for files to back up files from user-created Server Message Block (SMB) file systems. HBR provides the two types of backup plans: instant and scheduled. This topic describes how to back up files from user-created SMB file systems.

Create an instant backup plan

If you need only one-time full backup, perform the following steps to create an instant backup plan:

1. Log on to an HBR backup client.
2. In the left-side navigation pane, click Backup. In the upper-right corner of the Backup Jobs page, click **Create Backup Job**.
3. On the **Basic Settings** tab of the **Create Backup Job** dialog box, set the parameters. The following table describes the parameters.
   - Source : Enter the path to the mount target of the NAS file system.
   - Running Plan : Select **Instant**.

> **Notice** Volume Shadow Copy Service (VSS) is not supported for NAS backup.

4. Optional. Click the **Bandwidth Throttling** tab. Set **Work Hours**. In the Throttling field, enter the

maximum bandwidth that can be used for backup during the specified throttling period. Then, click **Add**.

> **Note**
>
> - The throttling period is accurate to the hour. You can add multiple throttling periods based on your requirements.
> - If you need to modify a throttling period, find the throttling period, click **Delete** in the Actions column, and then add a throttling period.
> - The maximum bandwidth must be at least 1 MB/s.

5. Click **Submit**.

> **Note** After a backup job is started, you can perform the following operations on the **Backup Jobs** page:
>
> - View the progress of the backup job.
> - Click **Cancel** or **Retry** in the **Actions** column to cancel or retry the backup job.
> - If the backup of some files fail, click the **Download** icon in the Errors column to download the error report.

Create a scheduled backup plan

If you need scheduled backup, perform the following steps to create a scheduled backup plan:

1. Open a browser and enter `http://localhost:8011` in the address bar. On the page that appears, enter the password to log on to the HBR backup client for files.

> **Note**
>
> - If you are using an intermediate host, replace `localhost` with the IP address of the NAS client host.
> - Port 8011 is the default port that you can use for logon to a backup client for files. If port 8011 on the host of the backup client is occupied by another application, you can specify another port number for the backup client.

2. In the left-side navigation pane, click **Backup Policies**.
3. In the upper-right corner of the **Backup Polices** page, click **Create Policy**.
4. In the **Create Policy** dialog box, set the Name and other parameters.

Parameter	Description
Name	The name of the backup policy.
Frequency	The interval at which backup is performed. Units: ○ Hours. Valid values: 1 to 23. ○ Days. Valid values: 1 to 6. ○ Weeks. Valid values: 1 to 4.

Parameter	Description
Backup Time	The time to start the first backup. The first backup is a full backup.
Retention	○ The retention period of backup data. Units: days, months, or years. ○ Maximum retention period: 3650 days (10 years).

5. Click **Submit**.

   After the scheduled backup policy is created, perform the following steps to start a scheduled backup job:

   i. Log on to the HBR backup client for files.

   ii. In the left-side navigation pane, click **Backup**.

   iii. In the upper-right corner of the Backup Jobs page, click **Create Backup Job**.

   iv. In the **Create Backup Job** dialog box, click the **Basic Settings** tab. If you are creating a backup job for a user-created NFS file system, set the following parameters:

   - Source : Enter the path to the mount target of the NAS file system.
   - Running Plan : Select **Scheduled**.
   - Backup Policy : Select the created backup policy.

   > Notice VSS is not supported for NAS backup.

   v. Optional. Click the **Bandwidth Throttling** tab. Set **Work Hours**. In the Throttling field, enter the maximum bandwidth that can be used for backup during the specified throttling period. Then, click **Add**.

   > Note
   >
   > - The throttling period is accurate to the hour. You can add multiple throttling periods based on your requirements.
   > - If you need to modify a throttling period, find the throttling period, click **Delete** in the Actions column, and then add a throttling period.
   > - The maximum bandwidth must be at least 1 MB/s.

vi. Click **Submit**.

> **Note** After a backup job is started, you can perform the following operations on the **Backup Jobs** page:
>
> - View the progress of the backup job.
> - Click **Cancel** or **Retry** in the **Actions** column to cancel or retry the backup job.
> - Click **Delete** in the **Actions** column to delete the backup job. After you delete the backup job, HBR no longer runs the backup job based on the specified backup policy. However, HBR retains the backups that are created by the backup job. You can still restore data from these backups.
> - If the backup of some files fail, click the **Download** icon in the Errors column to download the error report.

3.4.4. Restore NAS files

You can restore files to the source server or virtual machine (VM). You can also restore files to a server or VM that is different from the backup source.

Restore files to the source client

To restore files to the source client, perform the following steps:

1. Log on to a Hybrid Backup Recovery (HBR) backup client.
2. In the left-side navigation pane, click **Restore** to open the **Restore Backup / Backups** page.
3. On the **Backups** tab, find the backup, and click **Restore** in the Actions column.
4. In the **Restore Backup** dialog box, set the parameters that are listed in the following table, select the files that you want to restore, and then click **Submit**.

Parameter	Description
Target Folder	The destination folder to which the files are restored.
File Options	○ **Include Files**: Only the selected files and folders are restored to the destination folder. ○ **Exclude Files**: Except for the selected files and folders, all other files and folders are restored to the target folder.

Restore files to a client that is different from the backup source

To restore files to a client that is different from the backup source, perform the following steps:

1. Log on to the destination HBR file backup client.
2. In the left-side navigation pane, click **Restore** to open the **Restore Backup / Backups** page.
3. In the upper-right corner of the Backups tab, click **Restore From Other Client**.
4. In the **Restore Backup** dialog box, select the source client and click **Next**.

5. Select the backup that you want to restore, and click **Next**.
6. In the Restore Backup dialog box, set the parameters that are listed in the following table, select the files that you want to restore, and then click **Submit**.

Parameter	Description
Target Folder	The folder to which the files are restored.
File Options	○ **Include Files**: Only the selected files and folders are restored to the destination folder. ○ **Exclude Files**: Except for the selected files and folders, all other files and folders are restored to the target folder.