ALIBABA CLOUD

Alibaba Cloud

Hybrid Backup

Back up NAS

Document Version: 20201019

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.Native backup

1.1. Clientless NAS backup

This topic describes how to use Hybrid Backup Recovery (HBR) to back up files in Apsara File Storage NAS. You can then restore the files at the earliest opportunity if they are lost or damaged.

Prerequisites

An NFS or SMB file system is created.

For more information about how to create an NFS or SMB file system, see Manage file systems.

Background information

Before you use HBR to back up files from Apsara File Storage NAS, note the following items:

- Unless otherwise specified, NAS in this topic refers to Apsara File Storage NAS.
- Clientless NAS backup allows you to back up Network File System (NFS) and Server Message Block (SMB) file shares no matter whether the file system is mounted. HBR uses an efficient backup mechanism that scans files in NAS file systems, instead of creating snapshots for NAS file systems.
- In addition to the native backup service, you can also use a backup client for files to back up files in NAS file systems. For more information, see Overview.

Back up files within a region

> **Note** We recommend that each created NAS backup job contains no more than 50 million files and the total number of files and subfolders in each folder is no more than 8 million.

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. Log on to the HBR console.
2. In the left-side navigation pane, choose **Backup > NAS Backup**.
3. In the upper-right corner, click **Create Backup Plan**.
4. In the **Create Backup Plan** panel, set the parameters and click **OK**.

   > **Note** You can enjoy the free trial of each backup plan for 60 days, starting from the day when the backup plan is created.

i. Set the basic parameters as described in the following table.

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

ii. The following table describes the advanced settings of the backup plan. If you want to specify the advanced settings, click Show Advanced Settings and click **Switch to Paid Plan**.

Condition	Description
Source Paths	The path to the folder that you want to back up, for example, /nas/folder. If you want to back up the root folder, enter a forward slash (/).
Backup Interval	The interval at which the backup is performed. Unit: days or weeks.
Retention Policy	The retention policy for the backup data. You can select **Limited** or **Permanent**. If you select **Limited**, you must set the **Retention Period** parameter.
Retention Period	The retention period of the backup data. Unit: days, weeks, months, and years.
Backup Vault	The backup vault where you want to store the backup data. You can select or create only a backup vault in the current region. If you select **Select Vault**, select a backup vault from the Vault Name drop-down list. If no backup vault is available, select **Create Vault** and specify the Vault Name field. The vault name must be 1 to 64 characters in length. **Note** A backup vault is a repository where HBR stores backup data in the cloud. You can back up files from multiple NAS file systems to the same vault. Backup vaults reside in different regions. You can select or create backup vaults only in the current region.

After the backup plan is created, HBR backs up files in the source NAS file system at the specified intervals, starting from the specified start time. 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 pause a running backup job, find the backup plan and choose **More** > **Suspend Plan** in the Actions column. To resume a paused backup job, find the backup plan and choose **More** > **Resume Plan** in the Actions column.
- To delete the backup plan, find the backup plan and choose **More** > **Delete Plan** in the Actions column. After you delete the backup plan, HBR no longer runs backup jobs for the plan but the backup data is retained.
- To view the backups of a file system that are created in the most recent three months or view all backups, find the backup plan and choose **More** > **Backups** in the Actions column.
- To modify a backup plan, find the backup plan and click **Modify** in the Actions column.

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

Restore files within a region

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 parameters in the **Select Backup** step and click **Next**. The following table describes the parameters.

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 to restore. Select **Recent 3 Months** or **All** to filter backups.

3. In the **Select Backup Files** step, set the **Restore Policy** parameter and click **Next**.The following restore policies are supported:
   - **Include All Files**: HBR restores all objects that are backed up from the source OSS bucket.
   - **Include Files** or **Exclude Files**: In the text box, enter the paths to the folders and files that you want to restore. HBR restores files that are backed up from the source OSS bucket based on the restore policy.

   In the text box, enter one path in each line and start each path with the source folder. For example, if the source path is /test/data and you want to restore the file.txt file and the abc folder, enter the following paths:

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

4. In the **Configure Destination** step, select a file system from the **File System** drop-down list and enter the path to the destination folder in the **Destination Path** field.

   > **Note** For example, you can enter /nas/abc if you want to restore files to the /nas/abc folder. If you want to restore files to the root folder, enter a forward slash (/).

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

Back up files across regions

A backup vault is a repository where 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 in the backup vault to the mirror vault.

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

1. Log on to the HBR console.
2. Click **Overview** in the left-side navigation pane. On the Overview page, select a region, for example, China (Hangzhou), in the **Regions** section. Find the backup vault for which you want to create a mirror vault and click the icon in the upper-right corner of the backup vault.

   add

3. In the **Create Mirror Vault** panel, select the **Region** where the mirror vault resides, enter the **Vault Name**, 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. HBR starts to synchronize historical data in a source backup vault to the mirror vault 90 minutes after the mirror vault is created.
   > - A mirror vault contains all the backup data that is stored in the source backup vault when the mirror vault is created.

You can view the data synchronization progress after you create a mirror vault. When the progress reaches 100%, it indicates that all data in the source backup vault is synchronized to the mirror vault.

progress

Restore files across regions

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

1. On the **NAS Backup** page, select the region where the mirror vault resides.
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 as prompted.

> **Note** Select the mirror vault from the **Source Vault** drop-down list. The name of a mirror vault is prefixed with [COPY]. For information about how to set other parameters, see Restore files within a region.

Optional operations

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 about 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 automatically creates a mount target for the file system. You cannot delete the mount target in the NAS console. 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, backup jobs of the file system fail. Before you delete the mount target, ensure that no backup or restore jobs of the file system are running.

2.Use file backup

2.1. Back up NFS NAS using ECS file backup

2.1.1. 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:

- Preparations
- Back up NAS files
- Restore NAS files

2.1.2. Preparations

You can use HBR to back up NFS NAS files and restore them when necessary. This topic describes the preparations that you need to make before backing up data.

Step 1: Create and assign RAM roles to HBR

Before using HBR to back up files from ECS, you must create and assign the AliyunHBRDefaultRole and AliyunECSAccessingHBRRole roles to HBR. To create and assign the two roles, perform the following steps:

1. Log on to the HBR console.
2. In the left-side navigation pane, choose **Backup > ECS File Backup**. Two authorization dialog boxes appear one after one.
3. In each dialog box, click Authorize. On the page that appears, create and assign the role to HBR as prompted.

Install Cloud Assistant

An ECS backup client must work with Cloud Assistant. By default, Cloud Assistant clients are installed on ECS instances that are created after December 1, 2017. To back up ECS instances that you bought before December 1, 2017, you must install the Cloud Assistant client.

Add a mount point

In the NAS console, add a VPC-type mount point for the created NFS NAS file system. For more information about how to add a VPC-type mount point, see Create a mount target.

After adding the mount point, click **Manage** next to the file system in the Action column. On the File System Details page that appears, check the mount point path.

Create an ECS instance

Create an ECS instance in the VPC where the mount point for the NAS file system resides. The CentOS operating system is used in this example. For more information, see Create an instance by using the provided wizard.

Mount the NFS NAS file system to the ECS instance

The procedure is as follows:

1. Run the **sudo yum install nfs-utils** command to install the NFS client. The CentOS operating system is used in this example. For more information about how to install the NFS client in another Linux operating system, see Step 1: Install an NFS client.
2. After installing the NFS client, mount the NFS file system. For more information, see Mount an NFS file system.

2.1.3. 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.

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.

Parameter	Description
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.

2.1.4. Restore NAS files

You can restore backup Apsara File Storage Network Attached Storage (NAS) files to the original Elastic Compute Service (ECS) instance or another ECS instance that uses the same backup vault. When necessary, you can also restore NAS files backed up by a file backup client in a local Internet data center (IDC) to the specified 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 File Backup** page, click the **ECS Instance** tab.
4. On the ECS Instance tab, find the target ECS instance and click **Restore** in the **Actions** column.
5. In the **New Restore Task** pane that appears, set Restore Resource.
   - **From This ECS**

     Select this option if you need to restore backup files from the current ECS instance. Then, follow these steps:

     a. Click **Next**.

     b. Select a snapshot and click **Next**.

c. Set Restore Path, select the files to be restored, and then click **Create**.

- **From Other ECS**

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

  a. Select the ECS instance where the backup files reside and click **Next**.

  b. Select a snapshot and click **Next**.

  c. Set Restore Path, select the files to be restored, and then click **Create**.

- **From Local Client**

  Select this option if you need to restore files backed up by a file backup client in a local IDC to the current ECS instance. Then, follow these steps:

  a. Select the client that is used to back up the files to be restored and click **Next**.

  b. Select a snapshot and click **Next**.

  c. Set Restore Path, select the files to be restored, and then click **Create**.

> **Note** On the **ECS File Backup** page, you can click the **Restore Jobs** tab to view the progress of the created restore job.

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

2.2.1. 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

2.2.2. 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 1: Create and assign RAM roles to HBR

Before using HBR to back up files from ECS, you must create and assign the AliyunHBRDefaultRole and AliyunECSAccessingHBRRole roles to HBR. To create and assign the two roles, perform the following steps:

1. Log on to the HBR console.
2. In the left-side navigation pane, choose **Backup > ECS File Backup**. Two authorization dialog

boxes appear one after one.

3. In each dialog box, click Authorize. On the page that appears, create and assign the role to HBR as prompted.

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.

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 provided 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.

2.2.3. 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.
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.

2.2.4. Restore NAS files

You can restore backup Apsara File Storage Network Attached Storage (NAS) files to the original Elastic Compute Service (ECS) instance or another ECS instance that uses the same backup vault. When necessary, you can also restore NAS files backed up by a file backup client in a local Internet data center (IDC) to the specified 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 File Backup** page, click the **ECS Instance** tab.
4. On the ECS Instance tab, find the target ECS instance and click **Restore** in the **Actions** column.
5. In the **New Restore Task** pane that appears, set Restore Resource.
   - **From This ECS**

     Select this option if you need to restore backup files from the current ECS instance. Then, follow these steps:

     a. Click **Next**.
     b. Select a snapshot and click **Next**.
     c. Set Restore Path, select the files to be restored, and then click **Create**.
   - **From Other ECS**

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

     a. Select the ECS instance where the backup files reside and click **Next**.
     b. Select a snapshot and click **Next**.
     c. Set Restore Path, select the files to be restored, and then click **Create**.
   - **From Local Client**

     Select this option if you need to restore files backed up by a file backup client in a local IDC to the current ECS instance. Then, follow these steps:

     a. Select the client that is used to back up the files to be restored and click **Next**.
     b. Select a snapshot and click **Next**.
     c. Set Restore Path, select the files to be restored, and then click **Create**.

> **Note** On the **ECS File Backup** page, you can click the **Restore Jobs** tab to view the progress of the created restore job.

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

2.3.1. 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

2.3.2. 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.

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 Step 1: Install an NFS client.
2. Mount the NFS file system. For more information, see Step 2: Mount an NFS file system.

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

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.
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
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 Create an AccessKey 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?

2.3.3. 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.

2.3.4. Restore NAS files

You can restore backup NAS files to their original server or virtual machine. When necessary, you can also restore files backed up by another client in the same vault to the specified server or virtual machine.

Restore files from the current client

To restore NAS files from the current client, perform the following operations:

1. Log on to the HBR file backup client.
2. In the left-side navigation pane, click **Restore** to go to the **Restore Backup / Backups** page.
3. On the Backups tab of the Restore Backup / Backups page, locate the file to be restored, and then click **Restore**.

4. In the **Restore Backup** dialog box that appears, set the parameters as instructed in the following table, select the files to be restored, and then click **Submit**.

Parameter	Description
Target Folder	The folder to which the files are restored.
File Options	○ Include Files: If you select this option, only the selected directories and files are restored to the target folder. ○ Exclude Files: If you select this option, all directories and files except those selected are restored to the target folder.

Restore files from another client

To restore NAS files from another client, perform the following operations:

1. Log on to the HBR file backup client.
2. In the left-side navigation pane, click **Restore** to go to the **Restore Backup / Backups** page.
3. On the Restore Backup / Backups page, click **Restore From Other Client** in the upper-right corner.
4. In the **Restore Backup** dialog box that appears, select the client where the files to be restored reside and click **Next**.
5. Select the snapshot of the backup to be restored and click **Next**.
6. Set the parameters as instructed in the following table, select the files to be restored, and then click **Submit**.

Parameter	Description
Target Folder	The folder to which the files are restored.
File Options	○ Include Files: If you select this option, only the selected directories and files are restored to the target folder. ○ Exclude Files: If you select this option, all directories and files except those selected are restored to the target folder.

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

2.4.1. 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

2.4.2. 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.

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.

> **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 Create an AccessKey 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?

2.4.3. 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.
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.

2.4.4. Restore NAS files

You can restore backup NAS files to their original server or virtual machine. When necessary, you can also restore files backed up by another client in the same vault to the specified server or virtual machine.

Restore files from the current client

To restore NAS files from the current client, perform the following operations:

1. Log on to the HBR file backup client.
2. In the left-side navigation pane, click **Restore** to go to the **Restore Backup / Backups** page.
3. On the Backups tab of the Restore Backup / Backups page, locate the file to be restored, and then click **Restore**.
4. In the **Restore Backup** dialog box that appears, set the parameters as instructed in the following table, select the files to be restored, and then click **Submit**.

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

Parameter	Description
File Options	○ Include Files: If you select this option, only the selected directories and files are restored to the target folder. ○ Exclude Files: If you select this option, all directories and files except those selected are restored to the target folder.

Restore files from another client

To restore NAS files from another client, perform the following operations:

1. Log on to the HBR file backup client.
2. In the left-side navigation pane, click **Restore** to go to the **Restore Backup / Backups** page.
3. On the Restore Backup / Backups page, click **Restore From Other Client** in the upper-right corner.
4. In the **Restore Backup** dialog box that appears, select the client where the files to be restored reside and click **Next**.
5. Select the snapshot of the backup to be restored and click **Next**.
6. Set the parameters as instructed in the following table, select the files to be restored, and then click **Submit**.

Parameter	Description
Target Folder	The folder to which the files are restored.
File Options	○ Include Files: If you select this option, only the selected directories and files are restored to the target folder. ○ Exclude Files: If you select this option, all directories and files except those selected are restored to the target folder.