

# Alibaba Cloud Hybrid Backup

Back up NAS

Issue: 20190912

## 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 due to product version upgrades, adjustments, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and the updated versions of this document will be occasionally released through Alibaba Cloud-authorized channels. You shall 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 the document in the context that Alibaba Cloud products and services are provided on an "as is", "with all faults" and "as available" basis. 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 bear any liability for any errors or financial losses incurred by any organizations, companies, or individuals arising from their download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, bear responsibility for any indirect, consequential, exemplary, incidental, 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 content of the Alibaba Cloud website, including but not limited to works, products, images, archives, information, materials, website architecture, website graphic layout, and webpage design, 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 the Alibaba Cloud website, product programs, or content 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 contact Alibaba Cloud directly if you discover any errors in this document.



## Generic conventions

Table -1: Style conventions

Style	Description	Example
	This warning information indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	 <b>Danger:</b> Resetting will result in the loss of user configuration data.
	This warning information indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	 <b>Warning:</b> Restarting will cause business interruption. About 10 minutes are required to restore business.
	This indicates warning information, supplementary instructions, and other content that the user must understand.	 <b>Notice:</b> Take the necessary precautions to save exported data containing sensitive information.
	This indicates supplemental instructions, best practices, tips, and other content that is good to know for the user.	 <b>Note:</b> You can use Ctrl + A to select all files.
>	Multi-level menu cascade.	Settings > Network > Set network type
<b>Bold</b>	It is used for buttons, menus, page names, and other UI elements.	Click OK.
Courier font	It is used for commands.	Run the <code>cd / d C :/ windows</code> command to enter the Windows system folder.
<i>Italics</i>	It is used for parameters and variables.	<code>bae log list --instanceid Instance_ID</code>
[ ] or [a b]	It indicates that it is an optional value, and only one item can be selected.	<code>ipconfig [-all -t]</code>

Style	Description	Example
<code>{}</code> or <code>{a b}</code>	It indicates that it is a required value, and only one item can be selected.	<code>swich {stand   slave}</code>



# Contents

---

Legal disclaimer.....	I
Generic conventions.....	I
1 Use agentless backup.....	1
1.1 Agentless NAS backup.....	1
2 Use file backup.....	8
2.1 Back up NFS NAS using ECS file backup.....	8
2.1.1 Overview.....	8
2.1.2 Preparations.....	8
2.1.3 Back up NAS files.....	10
2.1.4 Restore NAS files.....	12
2.2 Back up SMB NAS using ECS file backup.....	13
2.2.1 Overview.....	13
2.2.2 Preparations.....	13
2.2.3 Back up NAS files.....	14
2.2.4 Restore NAS files.....	16
2.3 Back up NFS NAS using local file backup.....	17
2.3.1 Overview.....	18
2.3.2 Preparations.....	18
2.3.3 Back up NAS files.....	24
2.3.4 Restore NAS files.....	27
2.4 Back up SMB NAS using local file backup.....	28
2.4.1 Overview.....	29
2.4.2 Preparations.....	29
2.4.3 Back up NAS files.....	34
2.4.4 Restore NAS files.....	37



# 1 Use agentless backup

---

## 1.1 Agentless NAS backup

You can use Hybrid Backup Recovery (HBR) to protect data in Alibaba Cloud Network Attached Storage (NAS) and restore data in a timely manner if data is lost or damaged.



**Note:**

Alibaba Cloud NAS is referred to as NAS in this topic.

### Preparations

Before using HBR to back up and restore data in NAS, you must create a NAS file system for backup.



**Notice:**

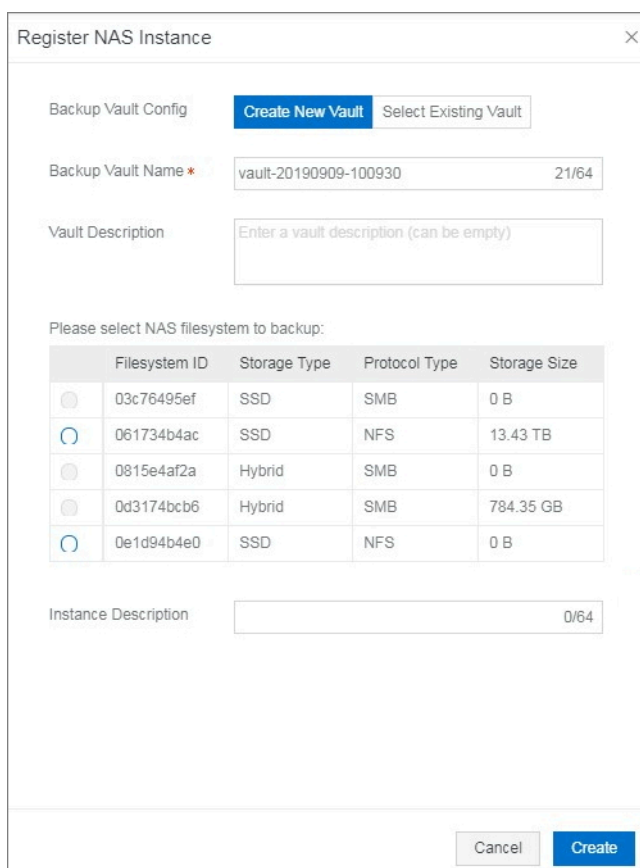
Currently, HBR only allows you to back up data in a NAS file system mounted in compliance with the Network File System (NFS) protocol.

### Step 1: Register a NAS instance

To register a NAS instance, perform the following operations:

1. Log on to the [HBR console](#).
2. In the left-side navigation pane, click NAS Backup.
3. On the NAS Instance tab, click Register NAS Instance in the upper-right corner.

#### 4. In the Register NAS Instance dialog box, specify relevant parameters.



The dialog box titled "Register NAS Instance" contains the following fields and controls:

- Backup Vault Config:** Two buttons, "Create New Vault" (highlighted in blue) and "Select Existing Vault".
- Backup Vault Name:** A text input field containing "vault-20190909-100930" with a character count of "21/64".
- Vault Description:** A text input field with the placeholder text "Enter a vault description (can be empty)".
- Please select NAS filesystem to backup:** A table with the following data:

	Filesystem ID	Storage Type	Protocol Type	Storage Size
<input type="radio"/>	03c76495ef	SSD	SMB	0 B
<input checked="" type="radio"/>	061734b4ac	SSD	NFS	13.43 TB
<input type="radio"/>	0815e4af2a	Hybrid	SMB	0 B
<input type="radio"/>	0d3174bcb6	Hybrid	SMB	784.35 GB
<input checked="" type="radio"/>	0e1d94b4e0	SSD	NFS	0 B

Below the table is an **Instance Description** text input field with a character count of "0/64". At the bottom right are "Cancel" and "Create" buttons.

- **Backup Vault Config :** You can click **Select Existing Vault**. If you have not created a backup vault before, click **Create New Vault** and enter the vault name and description to create a vault. The vault name can be up to 64 characters in length.



#### Note:

Backup vaults are HBR cloud storage repositories that you can use to store backups. You can back up data from multiple ECS instances to the same vault. Backup vaults are located in different regions. You can only select or create backup vaults in the current region.

- **Please select NAS filesystem to backup :** Select the NAS file system you want to back up.

#### 5. Click Create.

You can create a NAS backup plan after the status of the NAS instance changes from **Attaching** to **Attached**.

## Step 2: Create a backup plan



### Note:

We recommend that each created NAS backup job contain no more than 50 million files, and the total number of files and subdirectories in each directory be no more than 8 million.

To create a NAS backup plan, perform the following operations:

1. Log on to the [HBR console](#).
2. In the left-side navigation pane, click NAS Backup.
3. On the NAS Instance tab, click Backup in the Actions column for the registered NAS instance.

NAS Backup

Current Vault

cy-1.10.0

Register NAS Instance

Refresh

NAS Instance

Backup Plan

Backup Jobs

Restore Jobs

①You can also backup Alibaba NAS using file backup service. [View Details](#)

Filesystem ID/Name	Storage Type	Protocol Type	Storage Size	Zone	Mount Point Count	Status	Actions
<a href="#">0541c49921</a> 0541c49921	Hybrid	NFS	2.01 TB	Zone G	3	Attached	<div>BackupRestore</div>

4. In the Create Plan dialog box that appears, specify relevant parameters, as described in the following table, and click OK.

Create Plan

Plan Name \* plan-20190909-101120 20/64

Source File Path ? \* /your-backup-folder (/ means NAS root folder)

Start Time 2019-09-09 10:11:20

Plan Interval 1 Day

Retention 2 Year

Cancel Ok

Parameter	Description
Plan Name	Specify the name of the backup plan. If you do not specify this parameter, a random name is specified by default.
Source File Path	Specify the storage path of the files to be backed up.
Start Time	Specify the start time of the backup plan. The time is accurate to seconds.
Plan Interval	Specify the frequency of incremental backups. Valid units: day and week.

Parameter	Description
Retention	Specify the retention period of the backup. Valid units: day, week, month, and year.

After the backup plan is created, HBR backs up files on the NAS instance at the specified start time and at the specified intervals. On the Backup Plan tab, you can also perform the following operations:

- **Start a backup job:** Find the target backup plan and click **Execute Now** in the **Actions** column.
- **Pause a backup job:** Find the target backup plan and choose **⋮ > Disable Plan** in the **Actions** column. To resume a paused backup job, choose **⋮ > Enable Plan** in the **Actions** column.
- **Delete a backup job:** Find the target backup plan and choose **⋮ > Delete Plan** in the **Actions** column. After you delete a backup plan, HBR no longer runs the plan but retains data that is backed up by using the plan.
- **Modify a backup plan:** Find the target backup plan and click **Edit** in the **Actions** column.

**Note:**

You can view the progress of backup jobs on the Backup Jobs tab. After the specified backup job is completed, you can restore the backup data of the specified source NAS instance to the current or another specified NAS file system.

**Step 3: Create a restoration job**

To create a restoration job, perform the following operations:

1. On the NAS Instance tab, click **Restore** in the **Actions** column for the registered NAS instance.
2. On the Select Source Instance tab of the New Restore Task dialog box, set **Restore Resource** to **From Current NAS** or **From Other NAS**, and click **Next**.
3. On the Select Snapshot tab, set **Backup Time Frame** to **Last 3 Months** or **All Snapshots**, select a backup source, and then click **Next**.

#### 4. On the Config Restore Rules tab, set Restore Path and Restore Rule.

New Restore Task

Select Source Instance > Select Snapshot > **Config Restore Rules**

Restore Path \*

Restore Rule

Input File List ⓘ \*

Input one path per row, e.g.:

0/5000

**Each line of file list should start with basename of backup source path.**

**e.g.:**

**Windows**  
 Source is C:\Windows\ABC. To restore 'folder' and 'file.txt' in 'ABC' folder , please enter:

**Linux**  
 Source is /opt/abc. To restore 'folder' and 'file.txt' in 'abc' folder , please enter:

- If you set Restore Rule to Include All Files, HBR restores all files on the selected source NAS instance.
- If you set Restore Rule to Include Files or Exclude Files, you need to enter the directories of files in the Input File List field. HBR restores files on the selected source NAS instance based on this restoration rule.

In the Input File List field, enter one directory in each line. Ensure that each directory starts with the lowest-level folder in the source directory. For example, if the source directory is /test/data and you want to restore the file.txt and abc files in the data folder, enter the directories as follows:

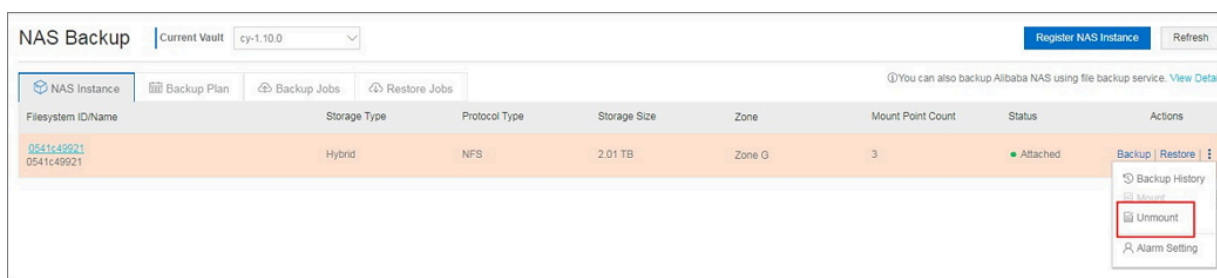
```
/ data / file . txt
/ data / abc
```

#### 5. Click Create.

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

### (Optional) Uninstall a NAS instance

When a NAS instance is registered, HBR automatically creates a mount point in the NAS file system. You cannot directly delete this mount point because it is created by the internal service of Alibaba Cloud. If you need to unmount the NAS file system, uninstall the NAS instance on the NAS Instance tab in the HBR console, as shown in the following figure.



#### Notice:

If you uninstall a NAS instance, relevant backup and restoration jobs may fail. Ensure that no backup or restoration job is in progress before you uninstall the NAS instance.

## 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:

- [#unique\\_8](#)
- [#unique\\_9](#)
- [#unique\\_10](#)

#### 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.

##### Authorize roles

When using Hybrid Backup Recovery (HBR) to back up files from ECS instances, you must authorize two roles: AliyunHBRDefaultRole and AliyunECSAccessingHBRRole. After the authorization, HBR and ECS are accessible by each other. Proceed as follows:

1. Log on to the [HBR console](#).
2. Choose ECS Backup > ECS File Backup.
3. Authorization pages appear one by one, which require you to confirm the authorization of these roles.

##### 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 [#unique\\_13/unique\\_13\\_Connect\\_42\\_section\\_6xi\\_a3u\\_zkq](#).

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.

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-bp1q36pv96rzriqt1lflg	vsw-bp128c92xrqucxo3m4z0		<b>V3 Mount:</b> sudo mount -t nfs -o vers=3,nolock,proto=tcp,noresvport 00d9b4b3fa-dto58.cn-hangzhou.nas.aliyuncs.com:/ /mnt <b>V4 Mount:</b> sudo mount -t nfs -o vers=4,minorversion=0,noresvport 00d9b4b3fa-dto58.cn-hangzhou.nas.aliyuncs.com:/ /mnt	VPC default permission group (...)	Available	Modify Permission Group Activate   Disable   Delete

## 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 [#unique\\_14](#).

Instance ID/Name	Tag	Monitoring	Zone	IP Address	Status	Network Type	Specifications	Billing Method	Actions
i- lj-windows-20190...	6cz		Qingdao Zone C	(Public) (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   More

## 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 [#unique\\_15/unique\\_15\\_Connect\\_42\\_section\\_kvj\\_d02\\_szj](#).
2. After installing the NFS client, mount the NFS file system. For more information, see [#unique\\_16](#).

### 2.1.3 Back up NAS files

**You can use HBR to back up NAS files in an ECS instance and restore the files when they are lost or damaged. This topic describes how to back up NAS files in an ECS instance.**

## Prerequisites

You have completed **preparations**.

## Step 1: Create an ECS file backup client

**The procedure is as follows:**

1. At the top of the page, select the region of the ECS instance from which you need to back up data.
2. On the ECS File Backup page, click Add ECS Instance.
3. In the Add ECS Instance dialog box that appears, select an existing backup vault or click Create Vault to create one. Then, select the ECS instance that you created in [preparations](#).
4. Click Create. Wait for several minutes, and check that the status of the created ECS instance on the ECS Instance tab is Activated.

ECS Name/ID	IP Address	Vault Name/ID	Client Type	Backup Jobs	Status	Actions
 1012 <a href="#">3orjcsxo494u</a>	 42(Public)  13.3(Private)	cy-zs_1.9.1 v-00009g75wbcma7wmtz01	Virtual Private Cloud (VPC) Ver. 1.9.1 c-00009g75wbcma7wmtz01	 Running: 0  Completed: 1  Failed: 0	 Activated (Backup Plan: 1)	<a href="#">Backup</a>   <a href="#">Restore</a>

## Step 2: Create a backup plan

**After creating the ECS file backup client, perform the following operations to create a backup plan:**


1. Click Backup next to the created ECS instance in the Actions column.

ECS Name/ID	IP Address	Vault Name/ID	Client Type	Backup Jobs	Status	Actions
cy-zs-sq2012 <a href="#">hbo1aigp9p9vscs0494u</a>	47.96.109.42(Public) 10.0.13.3(Private)	cy-zs_1_9.1 v-00009j75wbcma7wmtz01	Virtual Private Cloud (VPC) Ver. 1.9.1 c-00009j3qjgs2ghhlgr1i	<div><div>Running: 0</div><div>Completed: 1</div><div>Failed: 0</div></div>	Activated (Backup Plan: 1)	<div><div>Backup</div><div>Restore</div></div>

2. In the **Create Backup Plan** dialog box that appears, set the parameters, and then click **Create**.

The following table describes the parameters.

Parameter	Description
Plan Name	The name of the backup plan. If you leave this field blank, a random name is specified by default.

Parameter	Description
Source 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 the second.
Plan Interval	The frequency of incremental backups. Valid units: hour, day, and week.
Retention	The retention period of the backup. Valid units: day, week, month, and year.
Using Flow Control	<p>You can enable throttling to set bandwidth limits for backing up data from a directory during peak hours. This ensures business continuity.</p> <div>  <b>Note:</b>            If you select Use, select a throttling period and enter the maximum bandwidth that can be used for backup in the throttling period based on business requirements, and then click Add.         </div>

### Step 3: Run the backup job

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

Plan Name/ID	ECS Name/ID	Source Path	Backup Speed	Schedule	Status	Actions
plan-20190626-112827 j-0006nfaewsc81s7w8y5	ecs-20190626-112827-2 i-0006nfaewsc81s7w8y5	C:\	55.38 MB/s	Start: 06/26/2019, 11:30:00 Interval: 1 Day	Partial Complete 100%	View   <b>Execute Now</b>   Cancel Task
plan-20190612-141336 j-0006pibo0hmc0a0a02	ecs-20190612-141336-4 i-0006pibo0hmc0a0a02	/data	131.84 MB/s	Start: 06/12/2019, 14:15:00 Interval: 1 Hour	Waiting 100%	Enable   Pause   Edit   Delete
plan-20190531-172031 j-0006nfaewsc81s7w8y5	ecs-20190531-172031-2 i-0006nfaewsc81s7w8y5	C:\	34.64 MB/s	Start: 05/31/2019, 15:30:00 Interval: 2 Hour	Partial Complete 100%	View   <b>Execute Now</b>   Cancel Task
plan-20190531-161753 j-0006nfaewsc81s7w8y5	ecs-20190531-161753-4 i-0006nfaewsc81s7w8y5	/	317.71 MB/s	Start: 06/06/2019, 15:20:30 Interval: 3 Hour	Waiting 100%	Enable   Pause   Edit   Delete

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

Plan Name/ID	ECS Name/ID	Source Path	Backup Speed	Schedule	Status	Actions
plan-20190626-112827 j-0006nfaewsc81s7w8y5	ecs-20190626-112827-2 i-0006nfaewsc81s7w8y5	C:\	86.25 MB/s	Start: 06/26/2019, 11:30:00 Interval: 1 Day	Running 26.45%	View   <b>Execute Now</b>   Cancel Task

## 2.1.4 Restore NAS files

You can restore backup NAS files to their original ECS instance or another ECS instance in the same vault. When necessary, you can also restore NAS files backed up by a file backup client in a local IDC to the specified ECS instance.

### Procedure

1. Log on to the [HBR console](#).
2. In the left-side navigation pane, choose Cloud Backup > ECS File Backup.
3. On the ECS File Backup page, click the ECS Instance tab.
4. Locate the target ECS instance and click Restore in the Actions column.
5. In the New Restore Task dialog box that appears, set `Restore Resource` .

- From This ECS

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

- a. Select the local client 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.



Note:

On the ECS File Backup page, click the Restore Jobs tab to view the progress of the restoration job.

## 2.2 Back up SMB NAS using ECS file backup

### 2.2.1 Overview

You can use an ECS backup client of HBR to back up SMB 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 SMB NAS files, see the following topics:

- [#unique\\_21](#)
- [#unique\\_22](#)
- [#unique\\_10](#)

### 2.2.2 Preparations

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

#### Authorize roles

When using Hybrid Backup Recovery (HBR) to back up files from ECS instances, you must authorize two roles: AliyunHBRDefaultRole and AliyunECSAccessingHBRRole. After the authorization, HBR and ECS are accessible by each other. Proceed as follows:

1. Log on to the [HBR console](#).
2. Choose ECS Backup > ECS File Backup.
3. Authorization pages appear one by one, which require you to confirm the authorization of these roles.

#### 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 SMB NAS file system. For more information about how to add a VPC-type mount point, see [#unique\\_13/unique\\_13\\_Connect\\_42\\_section\\_6xi\\_a3u\\_zkq](#).

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.

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-bp1q36pv96rzriqt1lflg	vsw-bp128c92xrqucxzo3m4z0		<b>V3 Mount:</b> sudo mount -t nfs -o vers=3,nolock,proto=tcp,noresvport 00d9b4b3fa-dto58.cn-hangzhou.nas.aliyuncs.com:/ /mnt <b>V4 Mount:</b> sudo mount -t nfs -o vers=4,minorversion=0,noresvport 00d9b4b3fa-dto58.cn-hangzhou.nas.aliyuncs.com:/ /mnt	VPC default permission group (...)	Available	Modify Permission Group Activate Disable Delete

## Create an ECS instance

Create an ECS instance in the VPC where the mount point for the NAS file system resides. For more information, see [#unique\\_14](#).



### Notice:

We recommend that you create an ECS instance in Windows 2012. In Windows 2016, you must run Alibaba Cloud HBR as the administrator due to operating system permission control.

Instance ID/Name	Tag	Monitoring	Zone	IP Address	Status	Network Type	Specifications	Billing Method	Actions
i- lj-windows-20190...	6cz		Qingdao Zone C	Internet (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   More

## 2.2.3 Back up NAS files

You can use HBR to back up NAS files in an ECS instance and restore the files when they are lost or damaged. This topic describes how to back up NAS files in an ECS instance.

### Prerequisites

You have completed [preparations](#).

## Step 1: Create an ECS file backup client

The procedure is as follows:

1. At the top of the page, select the region of the ECS instance from which you need to back up data.
2. On the ECS File Backup page, click Add ECS Instance.
3. In the Add ECS Instance dialog box that appears, select an existing backup vault or click Create Vault to create one. Then, select the ECS instance that you created in [preparations](#).
4. Click Create. Wait for several minutes, and check that the status of the created ECS instance on the ECS Instance tab is Activated.

ECS Name/ID	IP Address	Vault Name/ID	Client Type	Backup Jobs	Status	Actions
 i012 <a href="#">c-00093qjgs2qhhilgrti</a>	47.96.109.42(Public) 10.0.13.3(Private)	cy-zs_1.9.1 v-0000sg75wbcma7wmtz01	Virtual Private Cloud (VPC) Ver. 1.9.1 c-00093qjgs2qhhilgrti	Running: 0 Completed: 1 Failed: 0	Activated (Backup Plan: 1)	<a href="#">Backup</a>   <a href="#">Restore</a>   <a href="#">⋮</a>

## Step 2: Create a backup plan

After creating the ECS file backup client, perform the following operations to create a backup plan:

1. Click Backup next to the created ECS instance in the Actions column.

ECS Name/ID	IP Address	Vault Name/ID	Client Type	Backup Jobs	Status	Actions
 cy-zs-sq2012 <a href="#">c-00093qjgs2qhhilgrti</a>	47.96.109.42(Public) 10.0.13.3(Private)	cy-zs_1.9.1 v-0000sg75wbcma7wmtz01	Virtual Private Cloud (VPC) Ver. 1.9.1 c-00093qjgs2qhhilgrti	Running: 0 Completed: 1 Failed: 0	Activated (Backup Plan: 1)	<a href="#">Backup</a>   <a href="#">Restore</a>   <a href="#">⋮</a>

2. In the Create Backup Plan dialog box that appears, set the parameters, and then click Create.

The following table describes the parameters.




### Notice:

You cannot use Volume Shadow Copy Service (VSS) to back up NAS files.

Parameter	Description
Plan Name	The name of the backup plan. If you leave this field blank, a random name is specified by default.
Source 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 the second.



Parameter	Description
Plan Interval	The frequency of incremental backups. Valid units: hour, day, and week.
Retention	The retention period of the backup. Valid units: day, week, month, and year.
Using Flow Control	<p>You can enable throttling to set bandwidth limits for backing up data from a directory during peak hours. This ensures business continuity.</p> <div>  <b>Note:</b>            If you select Use, select a throttling period and enter the maximum bandwidth that can be used for backup in the throttling period based on business requirements, and then click Add.         </div>

### Step 3: Run the backup job

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

Plan Name/ID	ECS Name/ID	Source Path	Backup Speed	Schedule	Status	Actions
plan-20190626-112827 j-0006nfaewsc81s7w8y5	ecs-20190626-112827-2 j-0006nfaewsc81s7w8y5	C:\	55.38 MB/s	Start: 06/26/2019, 11:30:00 Interval: 1 Day	Partial Complete 100%	View   <b>Execute Now</b> Cancel Task Enable Pause Edit Delete
plan-20190612-141336 j-0006nfaewsc81s7w8y5	ecs-20190612-141336-4 j-0006nfaewsc81s7w8y5	/data	131.84 MB/s	Start: 06/12/2019, 14:15:00 Interval: 1 Hour	Waiting 100%	
plan-20190531-172031 j-0006nfaewsc81s7w8y5	ecs-20190531-172031-2019 j-0006nfaewsc81s7w8y5	C:\	34.64 MB/s	Start: 05/31/2019, 15:30:00 Interval: 2 Hour	Partial Complete 100%	
plan-20190531-161753 j-0006nfaewsc81s7w8y5	ecs-20190531-161753-4 j-0006nfaewsc81s7w8y5	/	317.71 MB/s	Start: 06/05/2019, 15:20:30 Interval: 3 Hour	Waiting 100%	

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

Plan Name/ID	ECS Name/ID	Source Path	Backup Speed	Schedule	Status	Actions
plan-20190626-112827 j-0006nfaewsc81s7w8y5	ecs-20190626-112827-2 j-0006nfaewsc81s7w8y5	C:\	86.25 MB/s	Start: 06/26/2019, 11:30:00 Interval: 1 Day	Running 26.45%	View

## 2.2.4 Restore NAS files

You can restore backup NAS files to their original ECS instance or another ECS instance in the same vault. When necessary, you can also restore NAS files backed up by a file backup client in a local IDC to the specified ECS instance.

### Procedure



1. Log on to the [HBR console](#).
2. In the left-side navigation pane, choose Cloud Backup > ECS File Backup.
3. On the ECS File Backup page, click the ECS Instance tab.
4. Locate the target ECS instance and click Restore in the Actions column.
5. In the New Restore Task dialog box that appears, set **Restore Resource** .

- **From This ECS**

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

- a. Select the local client 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.



**Note:**

On the ECS File Backup page, click the Restore Jobs tab to view the progress of the restoration job.

## 2.3 Back up NFS NAS using local file backup

## 2.3.1 Overview

You can use a local file backup client to back up NFS NAS files in a local IDC and restore the files when they are lost or damaged.



Note:

This backup mode is only applicable to regions that do not support ECS backup. For regions that support ECS backup, we recommend that you [use an ECS file backup client to back up NFS NAS files](#).

For more information about how to back up NFS NAS files in a local IDC, see the following topics:

- [#unique\\_28](#)
- [#unique\\_29](#)
- [#unique\\_30](#)

## 2.3.2 Preparations

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



Note:

- For more information about how to back up NFS NAS files in an ECS instance, see [#unique\\_9](#).
- To achieve the optimal backup speed, we recommend that you run an HBR backup client on a host that uses a 64-bit CPU with at least two cores and has more than 8 GB memory available.
- The size of data that can be backed up varies depending on available memory resources. For example, with 4 GB memory available, you can back up a maximum number of one million files with a total size of 8 TB.

### RAM user and AccessKey

Resource Access Management (RAM) is an Alibaba Cloud service that helps you manage user identities and access to your cloud resources. You can create and manage multiple RAM users within a single Alibaba Cloud account. You can grant different permissions to each RAM user, so that RAM users have different access permissions on Alibaba Cloud resources.

An AccessKey is required when you activate a backup client. As any leak of an Alibaba Cloud account's AccessKey will expose cloud resources to security risks, we recommend that you use the AccessKey of a RAM user to perform the activation. Before performing a backup job, ensure that you have [Created a RAM user](#) and [Created an access key for a RAM user](#).

### Add a mount point

In the [NAS console](#), add a mount point for the created NFS NAS file system. For more information, see [#unique\\_13/unique\\_13\\_Connect\\_42\\_section\\_6xi\\_a3u\\_zkq](#).

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.

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-bp1q36pv96rzriqt1lflg	vsw-bp128c92xrqucxzo3m4z0		<b>V3 Mount:</b> <code>sudo mount -t nfs -o vers=3,nolock,proto=tcp,noresvport 00d9b4b3fa-dto58.cn-hangzhou.nas.aliyuncs.com:/ /mnt</code> <b>V4 Mount:</b> <code>sudo mount -t nfs -o vers=4,minorversion=0,noresvport 00d9b4b3fa-dto58.cn-hangzhou.nas.aliyuncs.com:/ /mnt</code>	VPC default permission group (...)	Available	<a href="#">Modify Permission Group</a> <a href="#">Activate</a>   <a href="#">Disable</a>   <a href="#">Delete</a>

### Mount an NFS NAS file system

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 [#unique\\_15/unique\\_15\\_Connect\\_42\\_section\\_kvj\\_d02\\_szj](#).
2. After installing the NFS client, mount the NFS file system. For more information, see [#unique\\_16](#).

### Add a client



#### Notice:

- The host that runs the client must have access to the Internet. For ECS instances, you can use the EIP or NAT to access the Internet.
- Only a small number of control commands are sent during the Internet access, which incurs few traffic fees.

You can use a file client to back up and restore data. Before that, you need to download the file client to a local IDC. You can download the file client in the HBR console. The procedure is as follows:

1. Log on to the [HBR console](#).



**Note:**

If the server or virtual machine runs on a Linux operating system without a GUI installed, you need to use an intermediate host with a GUI as an agent to log on to the HBR console.

2. At the top of the HBR console, select the region where you want to store backup data.



**Note:**

- If you use a VPC, the selected region must be the same as the region of the VPC where the data to be backed up resides to ensure a fast backup.
- Select a nearby region for better backup performance.
- Select a remote region for disaster recovery.

3. In the left-side navigation pane, choose On-Premises Backup > File Client.
4. On the File Client page, click Create Client in the upper-right corner.

5. In the Create Client dialog box that appears, set the parameters.

The following table describes the parameters.

Parameter		Description
Backup Vault Name		<p>Specify the backup vault. A backup vault is a repository used by HBR to store backup data on the cloud. You can back up data from multiple clients to the same vault.</p> <ul style="list-style-type: none"> <li>If you have created backup vaults: Click Select Vault and select a vault from the drop-down list.</li> <li>If you have not created any backup vaults: Click Create Vault, and then set Backup Vault Name and Vault Description. The vault name must not exceed 64 bytes in length.</li> </ul>
Client Name		The name of the client. The client name must not exceed 64 bytes in length.

Parameter	Description
Software Platform	The operating system of the host where the data to be backed up resides. Valid values: <ul style="list-style-type: none"><li>• Linux 32-bit</li><li>• Linux 64-bit</li></ul>
Network Type	<ul style="list-style-type: none"><li>• <b>Public Network:</b> Select this option when VPCs are inapplicable.</li><li>• <b>Virtual Private Cloud (VPC):</b> Select this option when the host resides in a VPC and is in the same region as the backup vault.</li></ul>

6. Click Create and then Download Client.



**Note:**

After installing the client by using the client installation package, you can use the client to connect to HBR. You can also go to the File Client page and choose **More > Download Client** in the Actions column to download the client installation package at any time.

**Install and activate the client**

After the client installation package is downloaded, install and activate the client. The procedure is as follows:


1. Run the `tar -xzf hbr-install-xxx-linux-amd64.tar.gz` command to decompress the downloaded client installation package to a specific directory. Then, run the `./setup` command to enable HBR.



**Note:**

Make sure that the disk where the installation directory resides has available space because running logs and execution files are stored in this directory.

2. After the client is installed, activate it. Log on to the HBR console. In the Create Client dialog box, click Next and then set the parameters as instructed in the following table.

Parameter	Description
Client IP Address	<p>The IP address of the file client that your current host can access. It can be a private or public IP address. For example, you can enter 127.0.0.1 (default), 12.34.56.78:8011, or http://87.65.43.21:8443.</p> <div>  <b>Note:</b>  The IP address must be reachable from your current browser. </div>
AccessKey Id	The AccessKey ID of the RAM user. Obtain the AccessKey ID and AccessKey Secret of the RAM user for which HBR is activated.
AccessKey Secret	The AccessKey Secret of the RAM user. Obtain the AccessKey ID and AccessKey Secret of the RAM user for which HBR is activated. .
Create Client Password	The logon password of the client. The password must be at least six characters in length.
Confirm Password	The confirm password, which must be the same as the password entered above.

3. Click **Activate Client**. The file client operation page automatically appears in the browser. Then, you can use the file client to back up data.



**Note:**

If the file client fails to be activated, you can [reactivate the client](#).

### 2.3.3 Back up NAS files

You can use an HBR file backup client to back up NFS NAS files in a local IDC. The HBR file backup client supports instant file backup and scheduled file backup. You can back up files in either mode based on your business requirements.

#### Instant backup

If you do not have any backup schedules and only need to back up full data, perform the following operations:

1. Log on to the HBR file backup client.
2. In the left-side navigation pane, click **Backup**. On the **Backup Jobs** page, click **Create Backup Job** in the upper-right corner.
3. In the **Create Backup Job** dialog box that appears, click the **Basic Settings** tab and set the following parameters:

- **Source** : Enter the path of the mount point for the NAS file system.
- **Running Plan** : Select **Instant**.



**Notice:**

You cannot use Volume Shadow Copy Service (VSS) to back up NAS files.

4. (Optional) Click the **Bandwidth Throttling** tab. Set **Work Hours** and **Throttling** , and then click **Add** to specify the maximum bandwidth that can be used for backup in the throttling period.



**Note:**

- The throttling period is accurate to the hour. You can add multiple throttling periods as needed.
- To modify a throttling period, click **Delete** next to the period in the **Actions** column, and set the period again.
- The maximum bandwidth cannot be less than 1 Mbit/s.



## 5. Click Submit.



### Note:

After the backup job starts, you can perform the following operations on the Backup Jobs page:

- View the progress of the backup job.
- Cancel or retry the backup job by clicking Cancel or Retry in the Actions column, respectively.
- If some files fail to be backed up in the job, locate the job on the Backup Jobs page. In the Errors column of the job, click the Download icon to download the error report.

## Scheduled backup

If you have a backup schedule, perform the following operations to create a backup policy and customize the first backup time and backup frequency:

1. Open a browser and visit `http://localhost:8011` to log on to the HBR file backup client. On the client logon page, enter the logon password.



### Note:

- If you back up data through an intermediate host, replace `localhost` with the IP address of the server or virtual machine where you want to back up data.
- You can log on to the file backup client over the default port 8011. If port 8011 on the target server or virtual machine is occupied by another application, you can [specify another port number for the file backup client](#).

2. In the left-side navigation pane, click Backup Policies.
3. On the Backup Policies page, click Create Policy.
4. In the Create Policy dialog box that appears, set Name and set the other parameters as needed.

Parameter	Description
Name	The name of the policy.

Parameter	Description
Frequency	<b>Valid units:</b> <ul style="list-style-type: none"> <li>• Hour (1-23)</li> <li>• Day (1-6)</li> <li>• Week (1-4)</li> </ul>
Backup Time	The first backup time. The first backup is a full backup.
Retention	<ul style="list-style-type: none"> <li>• Valid units: day, month, and year.</li> <li>• Maximum retention time: 3,650 days (10 years).</li> </ul>

5. Click Submit.

After creating the scheduled backup policy, perform the following operations to start a scheduled backup job:

1. Log on to the HBR file backup client.
2. In the left-side navigation pane, click Backup.
3. On the Backup Jobs page, click Create Backup Job in the upper-right corner.
4. In the Create Backup Job dialog box that appears, click the Basic Settings tab.

When backing up NFS NAS files in a local IDC, set the following parameters:

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



**Notice:**

You cannot use VSS to back up NAS files.

5. (Optional) Click the Bandwidth Throttling tab. Set Work Hours and Throttling , and then click Add to specify the maximum bandwidth that can be used for backup in the throttling period.



**Note:**

- The throttling period is accurate to the hour. You can add multiple throttling periods as needed.
- To modify a throttling period, click Delete next to the period in the Actions column, and set the period again.

- The maximum bandwidth cannot be less than 1 Mbit/s.

6. Click Submit.



**Note:**

After the backup job starts, you can perform the following operations on the Backup Jobs page:

- View the progress of the backup job.
- Cancel or retry the backup job by clicking Cancel or Retry in the Actions column, respectively.
- Delete the backup job by clicking Delete in the Actions column. After the backup job is deleted, data is no longer backed up based on the configured backup policy. Data that has been backed up is retained and can be restored.
- If some files fail to be backed up in the job, locate the job on the Backup Jobs page. In the Errors column of the job, click the Download icon 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.

Parameter	Description
File Options	<ul style="list-style-type: none"><li>· <b>Include Files:</b> If you select this option , only the selected directories and files are restored to the target folder.</li><li>· <b>Exclude Files:</b> If you select this option, all directories and files except those selected are restored to the target folder.</li></ul>

### 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	<ul style="list-style-type: none"><li>· <b>Include Files:</b> If you select this option , only the selected directories and files are restored to the target folder.</li><li>· <b>Exclude Files:</b> If you select this option, all directories and files except those selected are restored to the target folder.</li></ul>

## 2.4 Back up SMB NAS using local file backup

## 2.4.1 Overview

You can use a local file backup client to back up SMB NAS files in a local IDC and restore the files when they are lost or damaged.



Note:

This backup mode is only applicable to regions that do not support ECS backup. For regions that support ECS backup, we recommend that you [use an ECS file backup client to back up SMB NAS files](#).

For more information about how to back up SMB NAS files in a local IDC, see the following topics:

- [#unique\\_41](#)
- [#unique\\_42](#)
- [#unique\\_30](#)

## 2.4.2 Preparations

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



Note:

- For more information about how to back up SMB NAS files in an ECS instance, see [#unique\\_22](#).
- To achieve the optimal backup speed, we recommend that you run an HBR backup client on a host that uses a 64-bit CPU with at least two cores and has more than 8 GB memory available.
- The size of data that can be backed up varies depending on available memory resources. For example, with 4 GB memory available, you can back up a maximum number of one million files with a total size of 8 TB.

### RAM user and AccessKey

Resource Access Management (RAM) is an Alibaba Cloud service that helps you manage user identities and access to your cloud resources. You can create and manage multiple RAM users within a single Alibaba Cloud account. You can grant different permissions to each RAM user, so that RAM users have different access permissions on Alibaba Cloud resources.

You need to use an AccessKey to activate the backup client. We strongly recommend that you use the AccessKey of a RAM user to prevent the leakage of your Alibaba Cloud account AccessKey from compromising the security of all your resources. Make sure that you have [Created a RAM user](#) and [Created an access key for a RAM user](#) before backing up data.

### Add a mount point

In the [NAS console](#), add a mount point for the created SMB NAS file system. For more information, see [#unique\\_13/unique\\_13\\_Connect\\_42\\_section\\_6xi\\_a3u\\_zkq](#).

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.

Mount Point							
Mount Point Type	VPC	VSwitch	Mount Address	Mount Command	Permission Group	Status	Action
VPC	vpc-bp1q36pv96rzriqt1lflg	vsw-bp128c92xrqucxzo3m4z0		<b>V3 Mount:</b> sudo mount -t nfs -o vers=3,nolock,proto=tcp,noresvport 00d9b4b3fa-dto58.cn-hangzhou.nas.aliyuncs.com:/ /mnt <b>V4 Mount:</b> sudo mount -t nfs -o vers=4,minorversion=0,noresvport 00d9b4b3fa-dto58.cn-hangzhou.nas.aliyuncs.com:/ /mnt	VPC default permission group (...)	Available	<a href="#">Modify Permission Group</a> <a href="#">Activate</a>   <a href="#">Disable</a>   <a href="#">Delete</a>

### Add a client

You can use a file client to back up and restore data. Before that, you need to download the file client to a local IDC. You can download the file client in the HBR console. The procedure is as follows:

1. Log on to the [HBR console](#).



#### Note:

If the server or virtual machine runs on a Linux operating system without a GUI installed, you need to use an intermediate host with a GUI as an agent to log on to the HBR console.

2. At the top of the HBR console, select the region where you want to store backup data.



#### Note:

- If you use a VPC, the selected region must be the same as the region of the VPC where the data to be backed up resides to ensure a fast backup.

- Select a nearby region for better backup performance.
- Select a remote region for disaster recovery.

3. In the left-side navigation pane, choose On-Premises Backup > File Client.
4. On the File Client page, click Create Client in the upper-right corner.
5. In the Create Client dialog box that appears, set the parameters.

The following table describes the parameters.

Parameter	Description
Backup Vault Name	<p>Specify the backup vault. A backup vault is a repository used by HBR to store backup data on the cloud. You can back up data from multiple clients to the same vault.</p> <ul style="list-style-type: none"> <li>• If you have created backup vaults: Click Select Vault and select a vault from the drop-down list.</li> <li>• If you have not created any backup vaults: Click Create Vault, and then set Backup Vault Name and Vault Description. The vault name must not exceed 64 bytes in length.</li> </ul>
Client Name	The name of the client. The client name must not exceed 64 bytes in length.

Parameter	Description
Software Platform	The operating system of the host where the data to be backed up resides. Valid values: <ul style="list-style-type: none"><li>· Windows 32-bit</li><li>· Windows 64-bit</li></ul>
Network Type	<ul style="list-style-type: none"><li>· <b>Public Network:</b> Select this option when VPCs are inapplicable.</li><li>· <b>Virtual Private Cloud (VPC):</b> Select this option when the host resides in a VPC and is in the same region as the backup vault.</li></ul>

6. Click Create and then Download Client.



**Note:**

After installing the client by using the client installation package, you can use the client to connect to HBR. You can also go to the File Client page and choose **More > Download Client** in the Actions column to download the client installation package at any time.

Install and activate the client



**Notice:**

- The host that runs the client must have access to the Internet. For ECS instances, you can use the EIP or NAT to access the Internet.
- Only a small number of control commands are sent during the Internet access, which incurs few traffic fees.

After the client installation package is downloaded, install and activate the client. The procedure is as follows:

1. Run the installation program, select the installation directory, and then complete the installation as prompted.




**Note:**

Make sure that the disk where the installation directory resides has available space because running logs and execution files are stored in this directory.



2. After the client is installed, activate it. Log on to the HBR console. In the Create Client dialog box, click Next and then set the parameters as instructed in the following table.

Parameter	Description
Client IP Address	<p>The IP address of the file client that your current host can access. It can be a private or public IP address. For example, you can enter 127.0.0.1 (default), 12.34.56.78:8011, or http://87.65.43.21:8443.</p> <div>  <b>Note:</b>  The IP address must be reachable from your current browser. </div>
AccessKey Id	The AccessKey ID of the RAM user. Obtain the AccessKey ID and AccessKey Secret of the RAM user for which HBR is activated.
AccessKey Secret	The AccessKey Secret of the RAM user. Obtain the AccessKey ID and AccessKey Secret of the RAM user for which HBR is activated.
Create Client Password	The logon password of the client. The password must be at least six characters in length.
Confirm Password	The confirm password, which must be the same as the password entered above.

3. Click **Activate Client**. The file client operation page automatically appears in the browser. Then, you can use the file client to back up data.



**Note:**

If the file client fails to be activated, you can [reactivate the client](#).

## 2.4.3 Back up NAS files

You can use an HBR file backup client to back up SMB NAS files in a local IDC. The HBR file backup client supports instant file backup and scheduled file backup. You can back up files in either mode based on your business requirements.

### Instant backup

If you do not have any backup schedules and only need to back up full data, perform the following operations:

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



**Notice:**

You cannot use Volume Shadow Copy Service (VSS) to back up NAS files.

4. (Optional) Click the **Bandwidth Throttling** tab. Set **Work Hours** and **Throttling** , and then click **Add** to specify the maximum bandwidth that can be used for backup in the throttling period.



**Note:**

- The throttling period is accurate to the hour. You can add multiple throttling periods as needed.
- To modify a throttling period, click **Delete** next to the period in the **Actions** column, and set the period again.
- The maximum bandwidth cannot be less than 1 Mbit/s.

## 5. Click Submit.



### Note:

After the backup job starts, you can perform the following operations on the Backup Jobs page:

- View the progress of the backup job.
- Cancel or retry the backup job by clicking Cancel or Retry in the Actions column, respectively.
- If some files fail to be backed up in the job, locate the job on the Backup Jobs page. In the Errors column of the job, click the Download icon to download the error report.

## Scheduled backup

If you have a backup schedule, perform the following operations to create a backup policy and customize the first backup time and backup frequency:

1. Open a browser and visit `http://localhost:8011` to log on to the HBR file backup client. On the client logon page, enter the logon password.



### Note:

- If you back up data through an intermediate host, replace `localhost` with the IP address of the server or virtual machine where you want to back up data.
- You can log on to the file backup client over the default port 8011. If port 8011 on the target server or virtual machine is occupied by another application, you can [specify another port number for the file backup client](#).

2. In the left-side navigation pane, click Backup Policies.
3. On the Backup Policies page, click Create Policy.
4. In the Create Policy dialog box that appears, set Name and set the other parameters as needed.

Parameter	Description
Name	The name of the policy.

Parameter	Description
Frequency	<b>Valid units:</b> <ul style="list-style-type: none"> <li>• Hour (1-23)</li> <li>• Day (1-6)</li> <li>• Week (1-4)</li> </ul>
Backup Time	The first backup time. The first backup is a full backup.
Retention	<ul style="list-style-type: none"> <li>• Valid units: day, month, and year.</li> <li>• Maximum retention time: 3,650 days (10 years).</li> </ul>

5. Click Submit.

After creating the scheduled backup policy, perform the following operations to start a scheduled backup job:

1. Log on to the HBR file backup client.
2. In the left-side navigation pane, click Backup.
3. On the Backup Jobs page, click Create Backup Job in the upper-right corner.
4. In the Create Backup Job dialog box that appears, click the Basic Settings tab.

When backing up SMB NAS files in a local IDC, set the following parameters:

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



**Notice:**

You cannot use VSS to back up NAS files.

5. (Optional) Click the Bandwidth Throttling tab. Set Work Hours and Throttling , and then click Add to specify the maximum bandwidth that can be used for backup in the throttling period.



**Note:**

- The throttling period is accurate to the hour. You can add multiple throttling periods as needed.
- To modify a throttling period, click Delete next to the period in the Actions column, and set the period again.

- The maximum bandwidth cannot be less than 1 Mbit/s.

6. Click Submit.



**Note:**

After the backup job starts, you can perform the following operations on the Backup Jobs page:

- View the progress of the backup job.
- Cancel or retry the backup job by clicking Cancel or Retry in the Actions column, respectively.
- Delete the backup job by clicking Delete in the Actions column. After the backup job is deleted, data is no longer backed up based on the configured backup policy. Data that has been backed up is retained and can be restored.
- If some files fail to be backed up in the job, locate the job on the Backup Jobs page. In the Errors column of the job, click the Download icon 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	<ul style="list-style-type: none"><li>· <b>Include Files:</b> If you select this option , only the selected directories and files are restored to the target folder.</li><li>· <b>Exclude Files:</b> If you select this option, all directories and files except those selected are restored to the target folder.</li></ul>

### 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	<ul style="list-style-type: none"><li>· <b>Include Files:</b> If you select this option , only the selected directories and files are restored to the target folder.</li><li>· <b>Exclude Files:</b> If you select this option, all directories and files except those selected are restored to the target folder.</li></ul>