ALIBABA CLOUD

Alibaba Cloud

Apsara File Storage NAS

FAQ

Document Version: 20200918

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.FAQs

1.1. Why do I need RAM permissions to create a mount point in a classic network

Unlike Virtual Private Cloud (VPC) environments, classic network environments are not isolated at the network layer. To ensure data security of your NAS file system, NAS must be authorized through RAM to list your ECS instances. This makes sure that only your own ECS instances can mount or access the NAS file system. Note that the NAS file system and the ECS instance must be under the same Alibaba Cloud account.

> Note
>
> - NAS is only granted permission to call your DescribeInstances interface and has no permission to call any other instances. ECS instances acquired by NAS through the DescribeInstances interface are only used for permission verification, and are not recorded in any form.
> - Do not delete or edit AliyunNASDefaultRole in RAM as it may cause an operation exception error or failure when mounting the file system.

1.2. Is there a NAS terminology

Alibaba Cloud NAS (Network Attached Storage) provides an infinitely scalable file system to store data for ECS servers, and primarily involves the following concepts:

- File system: The file system is a NAS instance. You can mount the file system on an ECS server, E-HPC, or Container Service, and then use it like a local file system.
- Mount point: A mount point is the entry through which a computing node accesses NAS. It defines what type of network computing node can access NAS, and what permissions are required to access NAS.
- Permission group: A permission group defines NAS access permissions, including authorized IP addresses, read/write permissions, and user permissions.

1.3. How many file systems can an account create

Each Alibaba Cloud account can create up to 10 file systems. The maximum storage capacity of each file system is 1 PB (performance type) or 10 PB (capacity type).

1.4. What protocols does NAS support

NAS supports the following protocols:

1. NFS V3.0 and NFS v4.0.
2. SMB 2.1 and later versions, with corresponding support for Windows 7, Windows Server 2008 R2 and all later versions of Windows, but does not support Windows Vista, Windows Server 2008 and earlier versions.

1.5. What is a mount point and where can I use it

A mount point is the interface for computing nodes (such as ECS instance, E-HPC, or Container Service) to access a NAS file system.

Mount points define the network type of the computing nodes and the permissions required to access NAS.

One mount point can be simultaneously mounted by multiple computing nodes, enabling shared access.

1.6. What is a permission group and where can I use it

A permission group defines NAS access permissions, including authorized IP addresses, read/write permissions, and user permissions.

1.7. Does NAS support inotify

While inotifywait is commonly used in combination with rsync to backup/synchronize data on a quasi-real-time basis, it may not work properly on NAS file systems due to the implementation of inotify.

How inotify works

inotify is a sub-module of the Linux kernel, and inotifywait is the user-mode interface of inotify. inotify is realized at the VFS layer. When file operations reach the VFS layer, the inotify module sends the operation type (creation/deletion/attribute change, and so on) and operation object (file name) to the user-mode, and the user-mode inotifywait then outputs the operation information to the user.

Problem

Because inotify is implemented at the VFS layer of the kernel, the local kernel cannot recognize operations made by a remote client on the NFS file system. Therefore, inotify cannot recognize modifications on files made by the remote client.

If you Mount the same NAS file system simultaneously on Client A and Client B, and enable inotifywait at Client A to monitor the mounted directory, the following occurs:

- inotifywait recognizes operations on files in the mounted directory on Client A.
- inotify cannot recognize any operation on files in the mounted directory on Client B.

Solution

An alternative solution is to use FAM.

FAM is a library used for monitoring files or directories, and it is fully implemented in user-mode. You then only need to run a daemon in the background to regularly scan the directory and check for file changes.

However, using FAM has the following issues:

- You must write a program to call the FAM interface implementation function.
- In scenarios with a large number of files, using FAM may have poor performance and consume a lot of resources. Furthermore, it cannot ensure real-time monitoring.

1.8. How can I obtain an AccessKey pair?

You can create an AccessKey pair for an Alibaba Cloud account or Resource Access Management (RAM) user. When you call API operations, an AccessKey pair is required to complete identity verification.

Context

An AccessKey pair includes an AccessKey ID and AccessKey secret.

- An AccessKey ID is used to identify a user.
- An AccessKey secret corresponds to an AccessKey ID. You must keep the AccessKey secret confidential.

> **Notice** We recommend you use a RAM user to perform operations. This prevents against the leakage of the AccessKey pair for an Alibaba Cloud account. The leakage of the AccessKey pair for an Alibaba Cloud account exposes all of the resources under the account to security risks.

Procedure

1. Log on to the Alibaba Cloud console.
2. Move the pointer over your account profile picture in the upper-right corner of the page, and click **AccessKey**.
3. In the **Security Tips** dialog box, select Continue to Manage AccessKey or Get Started with RAM AccessKey.

   > **Notice** We recommend you use a RAM user to perform operations. This prevents against the leakage of the AccessKey pair for an Alibaba Cloud account.

   - Obtain the AccessKey pair of an Alibaba Cloud account.
     a. Click **Continue to Manage AccessKey**.
     b. On the **Security Management** page, click **Create AccessKey**.
     c. On the **Mobile Phone Verification** page, obtain a verification code, complete the verification process, and then click **OK**.
     d. In the **Create User AccessKey** dialog box, view the AccessKey ID and AccessKey secret in the AccessKey Details section.

        You can click **Save AccessKey Information** to download the AccessKey pair.
   - Obtain the AccessKey pair of a RAM user
     a. Click **Get started with RAM AccessKey**.
     b. On the Users page of the RAM console, click **Create User** to create a user.

        If you obtain an AccessKey pair for an existing RAM user, skip this step.

c. In the left-side navigation pane, choose **Identities** > **Users** and find the target user.

d. Click the logon name of the user to go to the User Details page. Select the **Authentication** tab, and click **Create AccessKey** in the **User AccessKeys** section.

> Note
>
> - You can create a maximum of two AccessKey pairs or each RAM user.
> - After you create an AccessKey pair, you cannot view the AccessKey secret of the AccessKey pair by using the console. We recommend that copy the AccessKey pair when creating it and keep the AccessKey secret confidential to prevent against information leakage.

e. On the **Mobile Phone Verification** page, obtain a verification code, complete the verification process, and then click **OK**.

f. In the **Create User AccessKey** dialog box that appears, view the AccessKey ID and AccessKey secret in the AccessKey Details section.

You can also click **Download CSV File** or **Copy** to save the AccessKey pair.

1.9. How can I view a list of clients on which a file system is mounted?

Apsara File Storage NAS allows you to mount a file system on multiple clients. You can view a list of clients on which a General-purpose NAS file system is mounted in the NAS console.

Procedure

1. Log on to the NAS console.
2. Choose **File System** > **File System List**.
3. Find the target file system and click **Management** in the Operations column.
4. In the left-side navigation pane, choose **Mounting Use** > **Mount Target**. On the page that appears, click **Client mounted** in the Operations column to view a list of clients on which the file system is mounted. The IP address of each client is displayed in the list.

> Note In the list, the clients on which you use the file system within the last minute are displayed. Other clients on which you mount the file system may be excluded from the list.

1.10. Can I switch the type of Apsara File Storage NAS file systems?

This topic describes how to switch the type of an Apsara File Storage NAS file system.

You cannot switch the type of the file system after it is created.

You can create a new file system if you no longer want to use the original file system.

- If the file system does not store any data

i. Create a new file system and mount it on an ECS instance. For more information, see Create a file system and Precautions.

ii. Delete the original file system.

- If the file system stores data

i. Create a new file system and mount it on an ECS instance. For more information, see Create a file system and Precautions.

ii. Migrate the data in the original file system to the new system. For more information, see Migrate data between Apsara File Storage NAS file systems.

iii. Delete the original file system.

1.11. Can I switch the type of a mount target?

This topic describes how to switch the type of a mount target.

If you have added a mount target for a file system, you cannot switch the type of the mount target. You can create a new mount target and mount the file system on the instance again.

For example, you have created an Apsara File Storage NAS Capacity file system and have mounted the file system on an instance through a mount target in a classic network. If you want to switch the mount target in a virtual private cloud (VPC), perform the following steps:

> **Note** You can add two mount targets for an Apsara File Storage NAS Capacity file system or an Apsara File Storage NAS Performance file system. However, you can only add one mount target in a VPC for an Apsara File Storage NAS Extreme file system.

1. Add a mount target in a VPC. For more information, see Create a mount target.
2. Unmount the file system which is mounted on the instance through the mount target in a classic network. For more information, see Unmount a file system.
3. Use the mount target in the VPC to mount the file system on the same target path of the instance. For more information, see Mount a file system.
4. Make sure that no client is mounted on the instance in the NAS console.

   You can click the **The client is mounted** button in the mount point section of the file system details page to view the mounted clients.
5. Disable the mount target in the classic network.
6. After you make sure that your business is not adversely affected, delete the mount target in the classic network.

1.12. Which file system protocol can I select to create a file system, NFS or SMB?

Apsara File Storage NAS is compatible with standard file system protocols, including the Network File System (NFS) and Server Message Block (SMB) protocols. This topic describes how to select NFS or SMB file systems based on different operating systems.

We recommend that you select the required file system protocol based on your business requirements.

- If you want to share files between Linux clients, we recommend that you create an NFS file system.
- If you want to share files between Windows clients, we recommend that you create an SMB file system.
- If you want to share files between Linux clients and Windows clients, we recommend that you create an SMB file system.

2.Scale and Performance

2.1. What impacts the I/O performance of Windows service SMB protocol

Symptom

By default, the `large mtu` option is disabled on a Windows SMB client, which affects the increase in I/O performance.

Solution

You can modify the following registry key to enable the `large mtu` option:

HKLM\System\CurrentControlSet\Services\LanmanWorkstation\Parameters

Create a `DWORD` at this location with the key named DisableLargeMtu and value set to `0`. Restart the file system to apply the change.

2.2. How to improve performance when using IIS to access NAS

Problem description

When IIS accesses a file by using a NAS share, the backend of IIS will frequently access NAS. Unlike accessing a local file system, you must interact with networks when accessing NAS. Even if it takes a short time for each interaction, the total amount of time increases with an increasing number of clients.

Solutions

For more information, see SMB2 Client Redirector Caches Explained.

You can increase the values of the following registry keys. For example, you can change the values to 600 or above.

The path of the registry key is *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\LanmanWorkstation\Parameters*.

The registry keys are listed as follows:

- FileInfoCacheLifetime
- FileNotFoundCacheLifetime
- DirectoryCacheLifetime

Note

- When none of the preceding keys exists, troubleshoot the issue as follows:
  i. Ensure that SMB is used rather than NFS.
  ii. Ensure that the current version of Windows supports these registry keys. When the current version of Windows supports these registry keys but they do not exist, you can manually create these registry keys. For more information, see Performance tuning for file servers.
- For web files that are frequently accessed by IIS, such as js and css scripts, we recommend that you move these files to a local PC.

2.3. SMB basic operation FAQ

Why is the disconnected state displayed when I use the net use command to view the status of a mount point?

If no operation is performed on a file system within 15 minutes, the connection is disconnected. The connection is established whenever an operation starts.

What is the maximum capacity and performance of a CIFS or SMB file system?

Currently, when an SMB file system is deployed on a NAS Capacity cluster, the maximum capacity and bandwidth for a single file system are subject to NAS Capacity. Other features, such as supports for a unique namespace, VPCs, and classic networks are the same as those of an NFS file system.

For more information, see Network Attached Storage.

Supported protocols and operating systems for an SMB file system

For more information, see Limits.

For more information about unsupported features for an SMB file system, see Unsupported SMB features.

Restrictions when accessing an SMB file system

Similar to accessing an NFS file system, you cannot access an SMB file system from an ECS instance that is located in another region or from the Internet. You must connect to a VPC by using a dedicated leased line to access the file system.

To access a file system from external networks outside the VPC where the file system is located, see the following sections:

- Access NAS from an on-premises IDC using a VPN network
- Access NAS from an on-premises IDC using NAT
- Mount NAS file systems on ECS instances that are located in multiple VPCs
- Mount NAS file systems on ECS instances that are owned by multiple accounts

2.4. How can I modify the maximum number of concurrent NFS requests?

The maximum number of concurrent requests from a Network File System (NFS) agent is 2 by default. This reduces the performance of NFS file systems. We recommend that you set the maximum number to 128. This topic describes how to modify the maximum number of concurrent NFS requests.

You can use one of the following methods to modify the maximum number of concurrent NFS requests.

> **Note** After you use method 1 to modify the maximum number, you must restart the ECS instance. This may affect business continuity. You can use method 2 to modify the maximum number of concurrent NFS requests without restarting the ECS instance.

Method 1

1. Install an NFS agent. For more information, see Install an NFS agent.
2. Run the following commands to set the maximum number of concurrent NFS requests to 128.

```
echo "options sunrpc tcp_slot_table_entries=128" >> /etc/modprobe.d/sunrpc.conf
echo "options sunrpc tcp_max_slot_table_entries=128" >>  /etc/modprobe.d/sunrpc.conf
```

> **Note** The first time you install an NFS agent, run the preceding commands once with root permissions. You do not need to run the commands again.

3. Use the following command to restart the ECS instance.

```
reboot
```

4. Mount a file system. For more information, see Mount an NFS file system.
5. Use the following command to verify the results.

   If the returned value is 128, the maximum number is modified.

```
cat /proc/sys/sunrpc/tcp_slot_table_entries
```

Method 2

1. Install an NFS client. For more information, see Install an NFS client.
2. Run the following command to set the maximum number of concurrent NFS requests to 128.

```
echo "options sunrpc tcp_slot_table_entries=128" >> /etc/modprobe.d/sunrpc.conf
echo "options sunrpc tcp_max_slot_table_entries=128" >>  /etc/modprobe.d/sunrpc.conf
```

> **Note** The first time you install an NFS agent, run the preceding commands once with root permissions. You do not need to run the commands again.

3. Mount a file system. For more information, see Mount an NFS file system.
4. Run the following command to set the maximum number of concurrent NFS requests to 128.

```
sysctl -w sunrpc.tcp_slot_table_entries=128
```

5. Unmount a file system. For more information, see Unmount a file system from a Linux ECS instance.
6. Mount the file system again. For more information, see Mount an NFS file system.
7. Use the following command to verify the results.

   If the value 128 is returned, it indicates that the maximum number is modified.

```
cat /proc/sys/sunrpc/tcp_slot_table_entries
```

2.5. Why is the speed of access to an NFS file system from a Linux client limited to several Mbit/s?

This topic describes why the speed of access to an NFS file system from an NFS client that runs Linux is limited to several Mbit/s and how you remove the limit.

The maximum number of concurrent NFS requests from an NFS client running Linux is limited to 2 by default, which reduces NFS performance.

After an NFS client is installed, you can modify the maximum number of concurrent NFS requests to improve NFS performance. For more information, see How can I modify the maximum number of concurrent NFS requests?.

2.6. How do I resolve SMB performance issues?

I/O latency

When you use a mount target to access a Server Message Block (SMB) file system, you need to wait for several minutes before the I/O operation is started.

The following sections describe how to reduce the I/O latency of an SMB file system.

Solution

The I/O latency of an SMB file system may be caused by an NFS client or web client on the ECS instance.

- If an NFS client is installed but no longer required, delete the NFS client.
- Find the ProviderOrder key. The path to the ProviderOrder key is `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\NetworkProvider\Order\ProviderOrder`.

For example, if the value of the ProviderOrder key is `LanmanWorkstation,RDPNP,Nfsnp`, delete `,Nfsnp` and restart the ECS instance.

- If a web client is installed, delete it.

> **Note** If a client accesses the SMB file system for the first time and the latency is higher than expected, ping the domain name of the mount target. You can then check whether the domain name is accessible and check the latency.
>
> - If the domain name of the mount target is inaccessible, we recommend that you check the network settings.
> - If the latency is high, ping the IP address of the mount target. If the latency of accessing the IP address is lower than that of accessing the domain name, check the configurations of the Domain Name System (DNS) server.

Procedure

1. Modify the value of the ProviderOrder key. If the latency is high the first time you access the file system, we recommend that you check this value.
2. Use the fio tool to conduct a performance test to check the issue.

```
fio.exe --name=./iotest1 --direct=1 --rwmixread=0 --rw=write --bs=4K --numjobs=1 --thread --iode
pth=128 --runtime=300 --group_reporting --size=5G --verify=md5 --randrepeat=0 --norandommap
--refill_buffers --filename=\\<mount point dns>\myshare\testfio1

fio.exe --name=./iotest1 --direct=1 --rwmixread=0 --rw=write --bs=4K --numjobs=1 --thread --iode
pth=128 --runtime=300 --group_reporting --size=5G --verify=md5 --randrepeat=0 --norandommap
--refill_buffers --filename=\\<mount point dns>\myshare\testfio1
```

3. We recommend that you perform I/O operations based on large data blocks. The smaller the data blocks are, the more network resources are consumed. If the data block size cannot be modified, use BufferedOutputStream.

3.Mount file systems

3.1. How can I mount a subdirectory of an Apsara File Storage NAS file system on a Linux server?

This topic describes how to create and mount a subdirectory of an Apsara File Storage NAS file system on a Linux server.

Prerequisites

An Apsara File Storage NAS file system is mounted on a Linux server. For more information, see Mount an NFS file system.

If you mount the */mnt* directory of the file system on the server, the */mnt* directory serves as the root directory of the file system. You can create subdirectories under the */mnt* directory.

Procedure

1. Create a subdirectory under the root directory of the Apsara File Storage NAS file system on the server (for example, a Linux ECS instance).

   ```
   mkdir /mnt/subdir
   ```

2. Create a local directory for mounting the Apsara File Storage NAS file system.

   ```
   mkdir /tmp/mnt
   ```

   > **Note** You can use a local directory for mounting only one file system. To mount multiple file systems, you must create multiple local directories.

3. Mount the subdirectory of the Apsara File Storage NAS file system.

   ```
   sudo mount -t nfs -o vers=4,minorversion=0,rsize=1048576,wsize=1048576,hard,timeo=600,retrans=2,noresvport file-system-id.region.nas.aliyuncs.com:/subdir /tmp/mnt
   ```

   The parameters in the mount command are described as follows. Replace them as needed.

   - *file-system-id.region.nas.aliyuncs.com*: specifies the endpoint of the mount target. To retrieve the endpoint of the mount target, do as follows: Log on to the NAS console , find the target file system, and then click **Manage**. You can find the endpoint of the mount target on the page that appears.
   - */subdir*: specifies the subdirectory of the Apsara File Storage NAS file system.
   - */tmp/mnt*: specifies the local directory of the server.

4.Access Apsara File Storage NAS from a local IDC

4.1. How can I access Apsara File Storage NAS from a server in my local IDC?

This topic describes how to use a VPN gateway or an NAT gateway to access Apsara File Storage NAS from a local server.

By default, you can mount an Apsara File Storage NAS file system only on an ECS instance that resides in the same VPC as that of the file system. To access an Apsara File Storage NAS file system from a local server, you must use Express Connect, VPN Gateway, or NAT Gateway to connect your local IDC with the VPC where the file system resides.

After the network connection is established, you can mount the Apsara File Storage NAS file system on your local servers. For more information, see Access an Apsara File Storage NAS file system from a local data center by using VPN Gateway or Access an Apsara File Storage NAS file system from a local IDC by using NAT Gateway.