Alibaba Cloud
Apsara File Storage NAS

User Guide

Issue: 20190709

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.	Danger: 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.	Warning: Restarting will cause business interruption. About 10 minutes are required to restore business.
	This indicates warning informatio n, supplementary instructions, and other content that the user must understand.	Notice: 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.	Note: You can use Ctrl + A to select all files.
>	Multi-level menu cascade.	Settings > Network > Set network type
Bold	It is used for buttons, menus , page names, and other UI elements.	Click OK.
`Courier font`	It is used for commands.	Run the `cd / d C :/ windows` command to enter the Windows system folder.
Italics	It is used for parameters and variables.	`bae log list -- instanceid` *Instance_ID*
[] or [a|b]	It indicates that it is a optional value, and only one item can be selected.	`ipconfig` *[-all|-t]*

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

Contents

1 Manage permission

1.1 Manage the resource access permissions of a file system

You can grant Resource Access Management (RAM) users the permissions to operate Network Attached Storage (NAS) file systems. We recommend that you log on and operate NAS file systems as a RAM user to follow best practices for security.

操作步骤

1. Log on to the RAM console
2. 在左侧导航栏中，选择权限策略管理，单击新建权限策略，根据页面提示，创建策略。此处以创建查看NAS资源的权限策略（NASReadOnlyAccess）为例。 脚步语法的详细介绍可参见Policy 结构和语法。

```
{
    " Statement ": [
        {
            " Effect ": " Allow ",
            " Action ": " nas : Describe *",
            " Resource ": "*"
        }
    ],
    " Version ": " 1 "
}
```

You can authorize a RAM user one or more of the following permissions to operate NAS file systems.

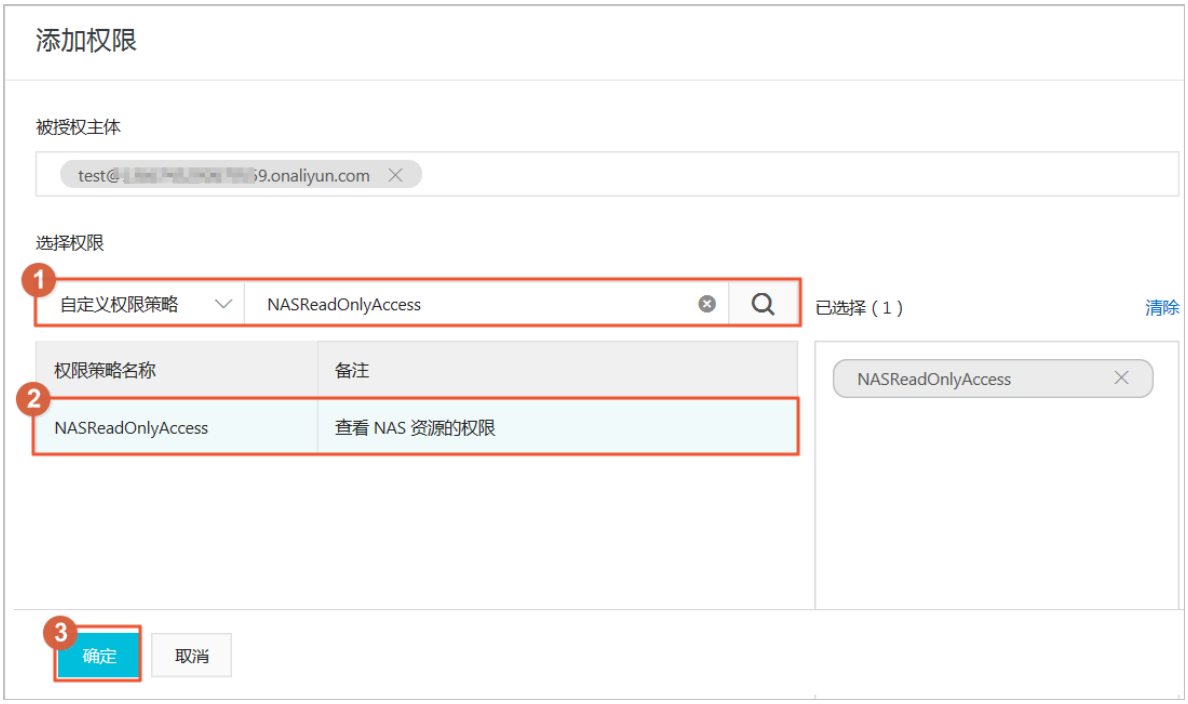
Action	Description
DescribeFileSystems	List all file systems.
DescribeMountTargets	List all mount points.
DescribeAccessGroup	List all permission groups.
DescribeAccessRule	List all permission group rules.
CreateMountTarget	Add a mount point for a file system.
CreateAccessGroup	Create permission groups.
CreateAccessRule	Create permission group rules.
DeleteFileSystem	Delete file systems.
DeleteMountTarget	Delete mount points.

Action	Description
DeleteAccessGroup	Delete permission groups.
DeleteAccessRule	Delete permission group rules.
ModifyMountTargetStatus	Enable or disable mount points.
ModifyMountTargetAccessGroup	Modify the permission group of a mount point.
ModifyAccessGroup	Modify permission groups.
ModifyAccessRule	Modify permission group rules.

You can only define RAM policies for the following resources:

Resource	Description
*	Indicates all NAS resources.

3. 创建成功后，返回用户页面。
4. 选择要授权的子账号，单击添加权限，选择NAS权限，为子账号授权。



1.2 Manage the data access permissions of a file system

You can use permission groups to manage data access permissions of a file system in Network Attached Storage (NAS).

Introduction

A permission group can be a whitelist or a blacklist of a mount point. You can add IP addresses and IP segments to a permission group by adding rules. You can also grant different levels of permissions to the IP addresses and IP segments in the rules.

When NAS is activated, a permission group named VPC default permission group (allow all) is generated. The default permission group allows read/write access to a mount point from all IP addresses in a VPC and no limit is specified for root users.

Note:

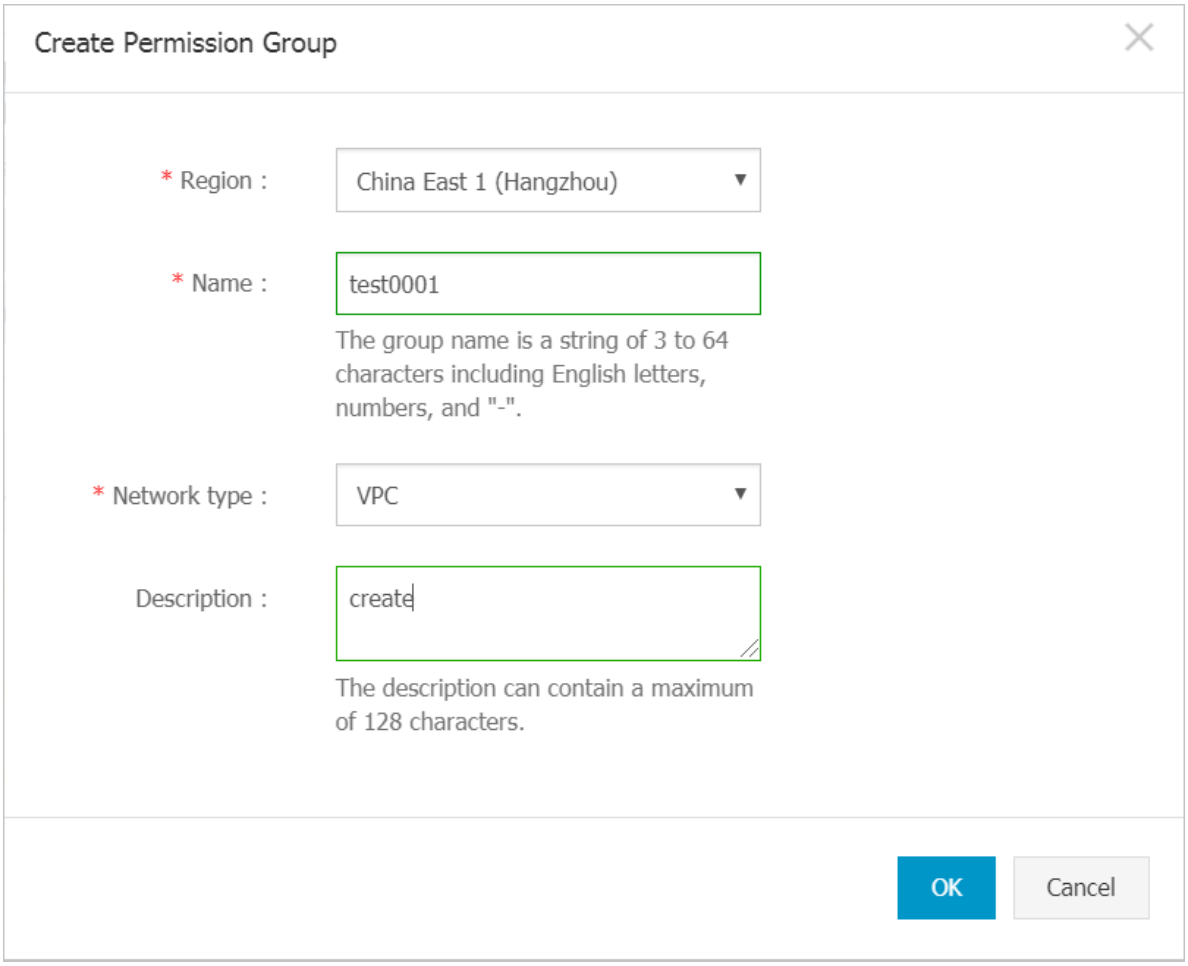
- For a mount point that is located in a classic network, no default permission group is provided. You need to bind a custom permission group to the mount point. In the custom permission group, you can only specify one IP address in each rule, and IP segments are not supported.
- We recommend that you only specify required IP addresses or IP segments when adding rules to a permission group to ensure data security.

Create a permission group

Proceed as follows to create a permission group

1. Log on to the NAS console.
2. In the left-side navigation pane, select Permission Group, and then click Create Permission Group in the upper-right corner.

3. Enter a name to create a new permission group.



Note:

With an Alibaba Cloud account, you can create up to 10 permission groups.

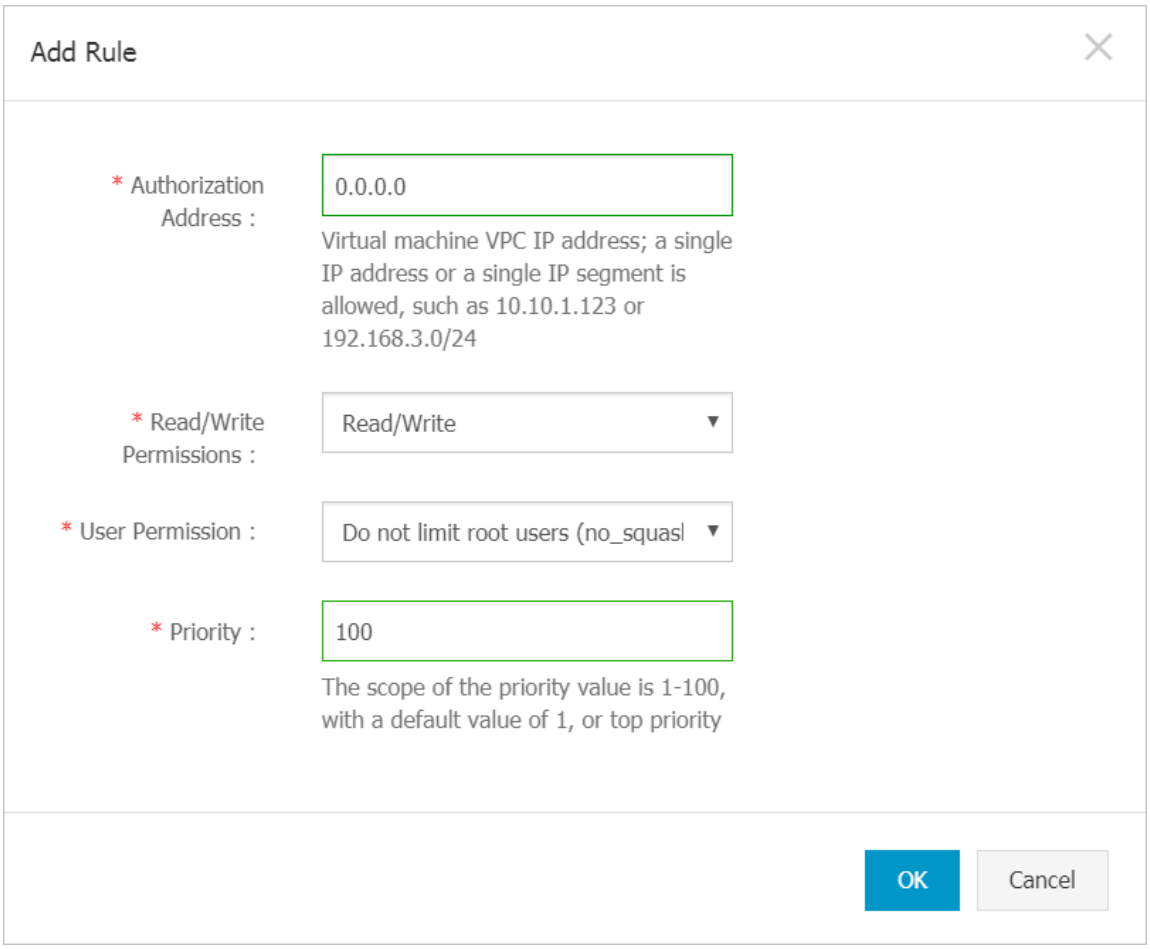
Manage permission group rules

You can add, modify, and delete permission group rules.

1. Log on to the NAS console.
2. In the left-side navigation pane, select Permission Group, and then click Manage next to a permission group.

3. On the Permission Group Rules page,

   - you can click Add Rule in the upper-right corner to add a rule.



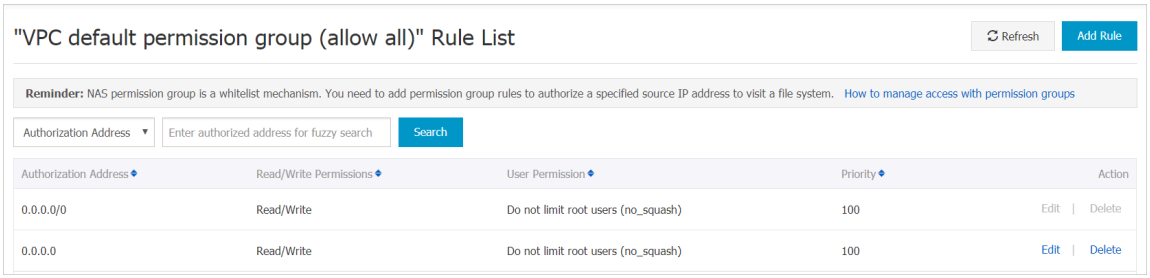
For a rule, you can configure the following options.

Option	Value	Description
Authorization Address	An IP address or IP segment. When you add a rule to a permission group whose network type is classic network, you must specify an IP address.	The authorized object to which this rule applies.
Read/Write Permissions	Read-only and Read/Write	Indicates whether to allow read-only or read/write access to a file system from the authorized object.

Option	Value	Description
User Permission	Do not limit root users (no_squash), Limit root users (root_squash), and Limit all users (all_squash)	Indicates whether to limit a Linux user's access to a file system. When a Linux user attempts to access the files or directories of a file system, the specified user permission is checked. - Do not limit root users (no_squash): allows access to a file system from root users. - Limit root users (root_squash): denies access to a file system from root users. All root users are treated as nobody users. - Limit all users (all_squash): denies access to a file system from all users including root users. All users are treated as nobody users.

Option	Value	Description
Priority	1 to 100, in which 1 is the highest priority	When an authorized object matches multiple rules, the rule with the highest priority takes effect.

- After you create a permission group rule, you can click Edit or Delete next to the rule to modify or delete this rule.



2 Manage file systems

In the NAS console, you can perform a number of operations on file systems. These operations include viewing a list of file systems, viewing the details of a file system, and deleting a file system.

Prerequisites

Before using a file system, you must perform the following actions:

1. Log on to the NAS console.
2. LinuxCreate at least one file system.

View a list of file systems

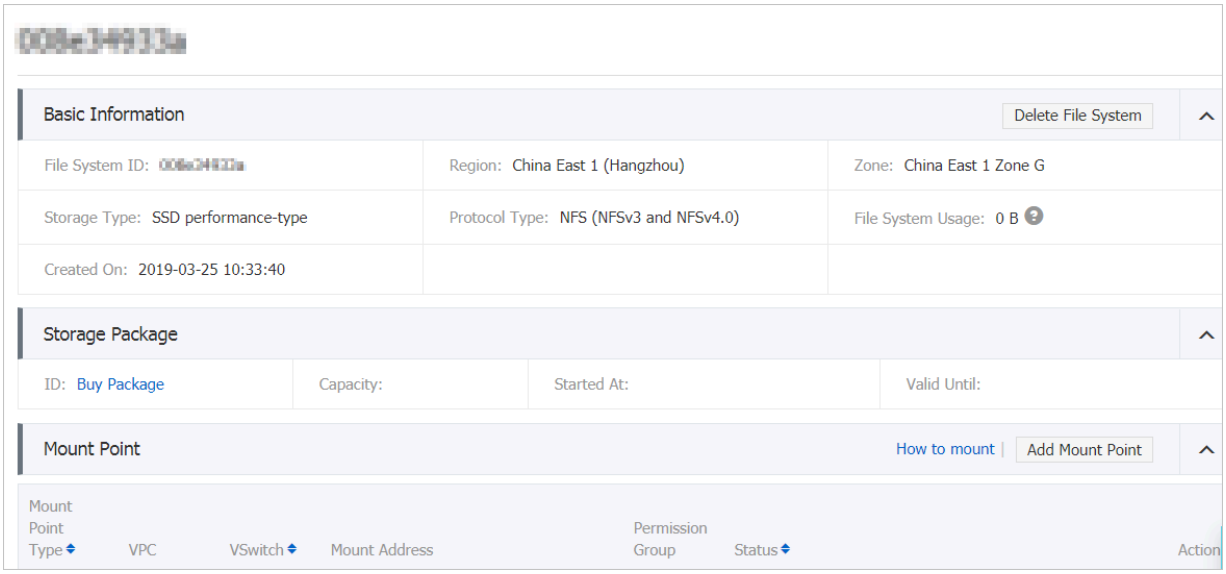
In the left-side navigation pane, select File System List to open the File System List page as shown in the following figure.

File System ID/Name	Storage Type	Protocol Type	Storage Capacity	Zone	Bound Storage Package	Number of Mount Points	Action
[illegible]	SSD performance-type	NFS	0 B	China East 1 Zone G	No	0	Add Mount Point | Manage | Delete
[illegible]	SSD performance-type	SMB	0 B	China East 1 Zone G	Yes	1	Add Mount Point | Manage | Delete

On the File System List page, you can modify the name, add a mount point, and view the details of a file system. You can also delete a file system and perform other operations.

View the details of a file system

On the File System List page, click the ID of a file system or click Manage next to a file system to open the File System Details page as shown in the following figure.



The File System Details page includes two sections:

- Basic Information: displays the file system ID, region, zone, and file system usage.
- Mount Point: displays the mount points for the file system. You can manage these mount points.

Delete a file system

On the File System List page, click Delete next to a file system to delete it.

> **Note:**
>
> - Before deleting a file system, you must remove all mount points of the file system.
> - After a file system is deleted, the data on the file system cannot be restored. We recommend that you ensure that all data is backed up.

3 Manage mount points

In the NAS console, you can perform multiple operations on mount points. These operations include viewing a list of mount points, deleting a mount point, modifying the permission group of a mount point, disabling a mount point, and enabling a mount point.

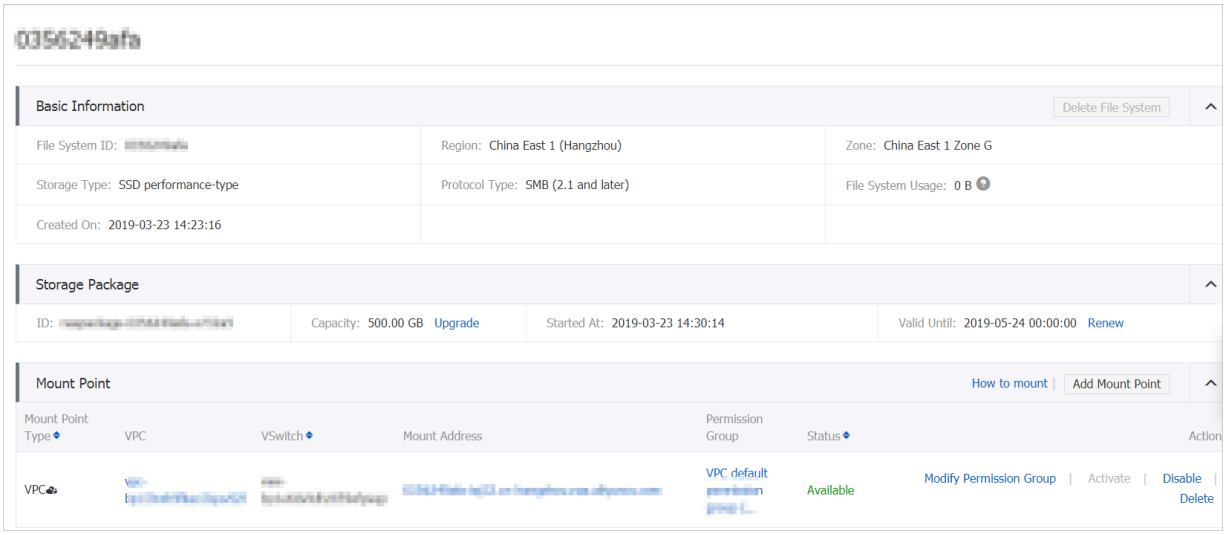
Prerequisites

Before operating a mount point, you must perform the following actions:

1. Log on to the NAS console.
2. LinuxCreate at least one file system.
3. WindowsAdd at least one mount point to a file system.

View a list of mount points

On the File System List page, click the name of a file system to open the File System Details page. On the File System Details page, you can manage mount points in the Mount Point section. You can perform multiple actions, such as adding a mount point, modifying the permission group of a mount point, enabling or disabling a mount point, and deleting a mount point.



Add a mount point

You can add one or more mount points to a file system. For more information, see Windows.

Enable or disable a mount point

You can click Disable next to a mount point to prevent a client from accessing the mount point, or click Activate to enable access.

Delete a mount point

You can click Delete next to a mount point to delete the mount point. You cannot restore a deleted mount point.

> Note:
> Before deleting a VPC, you must remove all mount points located in the VPC.

Modify the permission group of a mount point

You must bind a permission group to each mount point. ECS instances whose IP addresses are added to the permission group of a mount point are allowed to access the mount point. You can click Modify Permission Group next to a mount point to modify the permission group of the mount point.

> Note:
> The process of modifying the permission group requires up to one minute.

4 Mount a file system

4.1 Considerations before mounting a file system

After adding a mount point, you can mount a file system to computing resources through the mount point.

Prerequisites

When mounting a file system to an ECS instance through a mount point, you must note the following limits:

- If the mount point type is VPC, you can mount a file system to an ECS instance only when the instance and the mount point are in the same VPC. In addition, the IP address authorized by a rule of the permission group bound to the mount point must match the VPC IP address of the ECS instance.
- If the mount point type is Classic network, you can mount a file system to an ECS instance only when the instance and the mount point belong to the same account. In addition, the IP address authorized by a rule of the permission group bound to the mount point must match the intranet IP address of the ECS instance.

> Note:
> A NAS file system can be mounted to an ECS instance in another region.Use Cloud Enterprise Network（CEN） to establish a network across regions before you mount the file system.

Mounting methods

- NAS supports NFS and SMB file systems. For the mounting methods of the two file systems, see #unique_12 and #unique_13.

4.2 Mount an NFS file system in Linux

After installing an NFS client in Linux, you can mount an NFS file system to an ECS instance.

When you mount a NAS NFS file system to an ECS instance, you can use the DNS name of the file system or the target to which you want to mount the file system. The DNS

name of the file system is automatically resolved to the IP address of the mount target in the available zone of the mounted ECS instance.

Mounting command

You can run either of the following commands to mount an NFS file system.

- To mount an NFSv4 file system, run the following command:

```
sudo mount -t nfs4 -o vers=4.0,rsize=1048576,
wsize=1048576,hard,timeo=600,retrans=2,noresvport
  file-system-id-xxxx.region.nas.aliyuncs.com:/
mount-point
```

  If you fail to mount the file system, run the following command:

```
sudo mount -t nfs4 rsize=1048576,wsize=1048576,hard
,timeo=600,retrans=2,noresvport file-system-id-
xxxx.region.nas.aliyuncs.com:/ mount-point
```

  Note:
  The value of the *vers* parameter varies with the client version. If an error occurs when you use `vers=4.0` in the command, use `vers=4`.

- To mount an NFSv3 file system, run the following command:

```
sudo mount -t nfs -o vers=3,nolock,proto=tcp,
rsize=1048576,wsize=1048576,hard,timeo=600,retrans
=2,noresvport file-system-id-xxxx.region.nas.
aliyuncs.com:/ mount-point
```

Parameter description

The following table describes the parameters used in the mounting command.

Parameter	Description
Domain name of the mount point	Indicates the domain name of the mount point, which consists of information such as *file-system-id*, *region* and *nas.aliyuncs.com*. This parameter is automatically generated when you #unique_15 and does not need to be set manually.

Parameter	Description
mount-point	Indicates the mount point of the NAS file system, which can be the root directory "/" or any sub-directory in the NAS file system.
vers	Indicates the file system version. Only NFSv3 and NFSv4 are supported.

You can specify multiple options when mounting a NAS file system. The options are separated by commas in the command. The following table describes the options.

Option	Description
rsize	Specifies the size of data blocks. Data is read by blocks between the client and the file system deployed in the cloud. Recommended value: 1048576
wsize	Specifies the size of data blocks. Data is written by blocks between the client and the file system deployed in the cloud. Recommended value: 1048576
hard	Specifies whether the data transmissi on stops and waits for a temporarily unavailable file system to be recovered when you use the local application of a file stored in the file system. We recommended that you enable the hard parameter.
timeo	Specifies the time (in 0.1 second) that the NFS client waits for the response before resending a request to the NAS file system deployed in the cloud. Recommended value: 600
retrans	Specifies the number of times that the NFS client resends requests. Recommended value: 2

Option	Description
noresvport	Specifies that a new TCP port is used for network reconnection to ensure that the connection between the file system and the ECS instance will not be ended during network failure recovery. We recommend that you enable the noresvport parameter.

Note:

You must note the following points when configuring the mounting parameters:

- If you have to modify the values of I/O parameters (rsize and wsize), we recommend that you set the parameters to the maximum value (1048576) to prevent performance degradation.
- If you have to modify the value of the time-out parameter (timeo), we recommend that you set the parameter to a value not less than 150. The unit of the timeo parameter is 0.1 second. Therefore, the value 150 indicates that the actual time-out period is 15 seconds.
- We recommend that you enable the hard option. If you do not enable the hard option, set the timeo parameter to a value not less than 150.
- For other mounting options, use their respective default values. For example, do not modify the read or write buffer size or disable the attribute buffer because these operations result in performance degradation.

View mounting information

After the mounting succeeds, you can run the following command to view the mounted file system:

```
mount -l
```

You can also run the following command to view the capacity information about the mounted file system:

```
df -h
```

4.3 Mount an SMB file system

You can mount an SMB file system on an ECS instance that runs Windows.

Prerequisites

Before mounting an SMB file system on an ECS instance that runs Windows, ensure that the following services are started in Windows:

- Workstation

  Choose All Programs > Accessories > Run, or press `Win + R` and enter `services.msc` to open the Services console. Locate the Workstation service and check the status. The Workstation service is started by default.

- TCP/IP NetBIOS Helper

  Use the following steps to start the TCP/IP NetBIOS Helper service:

  1. Open Network and Sharing Center and click the active network connection.
  2. Click Properties to open the Local Area Network Properties dialog box. Double-click Internet Protocol Version 4 (TCP/IPv4) to open the Internet Protocol Version 4 (TCP/IPv4) Properties dialog box, and then click Advanced.
  3. In the Advanced TCP/IP Settings dialog box, choose WINS > Enable NetBIOS over TCP/IP.

Mount a file system using a command

You can run the following command to mount an SMB file system.

```
net use < the target mount drive > \\< the mount address
  of a mount point >\ myshare
```

- The target mount drive indicates the mount drive of the target Windows instance. In this command, you must add a space before \\ and another space before <the target mount drive>.

  > **Note:**
  > Ensure that the name of the target mount drive is unique on the target instance.

- When you create a mount point for a file system, a mount address is generated. You must enter the mount address to mount the file system.

  For more information, see Add a mount point.

- myshare: indicates the name of an SMB share. However, this name cannot be changed.

> **Note:**
> When a network connection is established between NAS and the Windows instance, you can mount an SMB file system on the instance. For more information, see Precautions before mounting a file system.

Examples

For example, to mount an SMB file system on drive Z, you can run the following command.

```
 net use z : \\ file - system - id - xxxx . region . nas .
aliyuncs . com \ myshare
```

View mount information

After mounting an SMB file system, you can run the following command in Windows command prompt to view the mounted file system.

```
net use
```

4.4 Mount an smb file system with task manager in windows

You can create a mounting script in the Windows operating system and then create a scheduled task, so that a NAS file system can be automatically mounted.

Procedure

1. Create a script named `nas_auto.bat` in Windows and add the following mounting command to it. Then, save the script to the disk where you want to mount the file system.

   ```
   net use Z:\\fid-xxxx.cn-shanghai.nas.aliyuncs.com\myshare
   ```

   Note:

   Change the drive letter (Z:) and the domain name of the mount point (fid-xxxx.cn-shanghai.nas.aliyuncs.com) to actual values.

   For details about the mounting command, see #unique_13 .

2. In the Control Panel of Windows, select Administrative Tools, and then select Schedule tasks.
3. In Task Scheduler, select Action > Create Task.
4. On the General tab, enter the Name of the scheduled task, and then select Run whether user is logged on or not and Run with the highest privileges.
5. On the Triggers tab, click New. Then, select At log on for Begin the task, and select Enabled in Advanced settings. After that, click OK.

6. On the Actions tab, click New. Then, selectStart a program for Actions, and then select the created `nas_auto . bat` script in Program/script. After that, click OK.

7. On the Conditions tab, select Start only if the following network connection is available, and then select Any connection.

8. On the Settings tab, select If the running task does not end when requested, force it to stop, and then select Do not start a new instance for If the task is already running, then the following rule applies.

9. Click OK.
10. Restart the server to check whether the task is successfully created.

    If the system displays the following information, the scheduled task can be normally executed:

4.5 Mount an NFS file system with /etc/fstab in Linux

You can modify either one of the following configuration files on an ECS instance to automatically mount a NAS file system when the instance is restarted.

To enable a file system to be mounted automatically on an ECS instance that runs Linux, you can modify either the `/ etc / fstab` file or the `/ etc / rc . local` file.

Modify the /etc/fstab file (recommended)

After you connect to an ECS instance for the first time, add the following command to the `/ etc / fstab` file.

```
fid - xxxx . cn - hangzhou . nas . aliyuncs . com :/ / mnt    nfs
vers = 4 , minorversi  on = 0 , rsize = 1048576 , wsize = 1048576 ,
hard , timeo = 600 , retrans = 2 , _netdev , noresvport   0   0
```

The parameters used in the command are described as follows:

Parameter	Description
_netdev	Prevents a file system from mounting on an ECS instance before a network connection is established.
0(the first zero after noresvport)	Non-zero values indicate that a file system must be backed up by dump. For a NAS file system, the value of the parameter is 0.
0 (the second zero after noresvport)	This value indicates the order in which fsck checks available file systems when an ECS instance is started. For a NAS file system, the value of the parameter is 0. It indicates that fsck is not allowed to run when an instance is started.

Modify the /etc/rc.local file

After you connect to an ECS instance for the first time, add the following command to the `/etc/rc.local` file.

Take an NFSv4 file system as an example. Add the following command.

```
sudo mount -t nfs -o vers=4.0,rsize=1048576,wsize
=1048576,hard,timeo=600,retrans=2,_netdev,noresvport
fid-xxxx.cn-hangzhou.nas.aliyuncs.com:/ /mnt
```

Note:

- In this command, `fid-xxxx.cn-hangzhou.nas.aliyuncs.com` is the domain name of the mount point. For more information about the mount command, see #unique_12.
- Before you modify the `/etc/rc.local` file, ensure that you have the execute permission to run the `/etc/rc.local` file and the `/etc/rc.d/rc.local` file.

Mount a NAS Extreme file system on an ECS instance

1. Modify the `/etc/systemd/system/sockets.target.wants/rpcbind.socket` file, move IPv6-related `rpcbind` parameters to comments.

Otherwise, the rpcbind service fails to automatically start up. The details are shown in the following figure.

2. After you connect to an ECS instance for the first time, add the following command to the `/ etc / fstab` file.

```
xxxx :/ share  / tmp / benchmark     nfs   vers = 3 , proto = tcp ,
noresvport , _netdev   0   0
```

4.6 Mount NAS file systems on ECS instances that are located in multiple VPCs

This section describes how to mount NAS file systems on ECS instances that are located in multiple VPCs.

Context

By default, when you mount a NAS file system on an ECS instance, ensure that the ECS instance and the NAS file system are located in the same VPC network. However , in most deployments, the VPC of an ECS instance is different from the VPC of a NAS mount point. You can connect VPCs by using Cloud Enterprise Network (CEN).

Configure a connection between VPCs

CEN enables connections between instances that are located in multiple VPCs but in the same region. After the connection is established, the ECS instance in VPC1 can directly communicate with the ECS instance and the NAS mount point in VPC2 by using the ping command.

1. Create a CEN instance

   a. Log on to the CEN console.

   b. On the CEN page, click Create CEN Instance.

   c. Configure the CEN instance as shown in the following figure.

      [DO NOT TRANSLATE]

      The options are described as follows:

Option	Description
Name	Enter the name of the CEN instance. The name can be 2 to 128 characters in length and can contain numbers, letters, Chinese characters, hyphens (-), and underscores (_). It must start with a letter or a Chinese character.
Description	Enter the description of the CEN instance. The description can be 2 to 256 characters in length. It cannot start with `http://` or `https://`.
Attach a network	You can attach networks in your account or another account to a CEN instance. For more information, see Networks.

2. Examples

   a. On the Instances page, locate the newly created instance and click Manage in the Actions column.

   b. On the CEN page, click Attach Network to configure the network as shown in the following figure.

      [DO NOT TRANSLATE]

      The options are described as follows:

Option	Description
Account	Select Your Account.
Network Type	Select the type of network to attach to the instance . You can select one of the following values: VPC , Virtual Border Router (VBR), and CloudConne ctNetwork (CCN). Select VPC.
Region	The region where the network is located. Select China (Qingdao).
Networks	Select a network to attach. Select a VPC network.

      Repeat the preceding procedure to attach two VPC networks to the same CEN instance. At this point, the connection between two VPCs is established.

3. Verify the mounting result

   Log on to the ECS instance to verify the mounting result.

```
[ root @ ~]# sudo   mount  - t   nfs  - o   vers = 4 . 0 , vpc2 <
 the   domain   name   of   the   mount   point >:/ / mnt
[ root @ iZbp18jc3n  wxdiy5e1vk  kaZ  ~]#  df  - h
 Filesystem                                          Size    Used
 Avail   Use %  Mounted   on
/ dev / vda1                                            40G    1 . 8G
     36G     5 % /
 devtmpfs                                            1 . 9G       0
   1 . 9G     0 % / dev
 tmpfs                                               1 . 9G       0
   1 . 9G     0 % / dev / shm
 tmpfs                                               1 . 9G    472K
   1 . 9G     1 % / run
 tmpfs                                               1 . 9G       0
   1 . 9G     0 % / sys / fs / cgroup
 tmpfs                                               379M       0
 379M     0 % / run / user / 0
```

```
082e54b989 - ciq13 . cn - hangzhou . nas . aliyuncs . com :/   1 .
0P       0    1 . 0P     0 % / mnt
```

4.7 Mount NAS file systems on ECS instances that are owned by multiple accounts

This section describes how to mount NAS file systems on ECS instances that are owned by multiple accounts.

Context

By default, you can only mount NAS file systems on ECS instances that are in the same account. If data transit is required between ECS instances that are owned by multiple UID accounts in an enterprise account and a NAS file system, you only need to establish a connection between the VPC that the ECS instance is located and the VPC that the NAS file system is located. You can connect multiple VPCs by using Cloud Enterprise Network (CEN).

Configure a connection between VPCs

CEN enables connections between VPCs that belong to multiple accounts. After connections between VPCs are established, ECS instances that are in one VPC can access NAS file systems in another VPC, even if the VPCs belong to different accounts.

1. Create a CEN instance using account A

   a. Log on to the CEN console.

   b. On the Instances page, click Create CEN Instance.

   c. Configure the CEN instance as shown in the following figure.

      [DO NOT TRANSLATE]

      The options are described as follows:

Option	Description
Name	Enter the name of the CEN instance. The name can be 2 to 128 characters in length and can contain numbers, letters, Chinese characters, hyphens (-), and underscores (_). It must start with a letter or a Chinese character.
Description	Enter the description of the CEN instance. The description can be 2 to 256 characters in length. It cannot start with `http://` or `https://`.
Attach networks	You can attach networks in your account or another account to a CEN instance. For more information, see Networks.

   d. Obtain the ID of the new CEN instance.

      In this example, the CEN instance ID is cbn-xxxxxxxxxx4l7.

2. Account B authorizes account A to attach its network instance

   On the VPC Details page, you can authorize another account to attach networks that are owned by the current account. Proceed as follows:

   1. Log on to the VPC console using account B.

   2. In the left-side navigation pane, select VPCs.

   3. Click the instance ID of the target VPC.

   4. In the CEN cross account authorization information section, click CEN Cross Account Authorization.

   In the Attach to CEN dialog box, enter `Peer Account UID` and `Peer Account CEN ID`, and then click OK.

3. Attach a network by using account A

   After the authorization is complete, you can attach a network as follows.

   a. Log on to the CEN console using account A.
   b. On the Instances page, locate the newly created CEN and click Manage in the Actions column.
   c. On the CEN page, click Attach Network to configure the network.

   The options are described as follows:

Option	Description
Account	Select Different Account.
Owner Account	Enter a peer account ID. Enter the account ID of account B.
Network Type	Select the type of network to attach to the instance . You can select one of the following values: VPC , Virtual Border Router (VBR), and CloudConne ctNetwork (CCN). Select VPC.
Region	The region where the network is located. Select China (Qingdao).
Networks	Select a network to attach. Select a VPC instance.

4. **Verify the mounting result**

   Log on to the ECS instance to verify the mounting result.

```
[ root @ ~]# sudo   mount  - t   nfs  - o   vers = 4 . 0 , vpc2 <
 the   domain   name   of   the   mount   point >:/ / mnt
[ root @ iZbp18jc3n  wxdiy5e1vk  kaZ  ~]#  df  - h
 Filesystem                                          Size    Used
 Avail   Use %  Mounted   on
/ dev / vda1                                            40G    1 . 8G
     36G     5 % /
 devtmpfs                                            1 . 9G       0
   1 . 9G     0 % / dev
 tmpfs                                               1 . 9G       0
   1 . 9G     0 % / dev / shm
 tmpfs                                               1 . 9G    472K
   1 . 9G     1 % / run
 tmpfs                                               1 . 9G       0
   1 . 9G     0 % / sys / fs / cgroup
 tmpfs                                               379M       0
 379M     0 % / run / user / 0
 082e54b989 - ciq13 . cn - hangzhou . nas . aliyuncs . com :/   1 .
 0P       0    1 . 0P     0 % / mnt
```

5 Unmount a file system

5.1 Unmount a file system in Linux

To delete a file system, you must unmount it from all ECS instances that have the file system mounted.

Procedure

1. Run the following command in each of the ECS instances:

```
umount < directory where the file system is mounted >
```

> **Note:**
>
> We recommend that you do not specify any other umount options or modify their default value.

2. Run the df command in the ECS instance to check whether the NAS file system is successfully unmounted.

   The df command is used to query the storage usage of and statistical information about a file system mounted to the current ECS instance. If the information about a NAS file system that you unmount is not displayed in the command output, the file system is successfully unmounted.

   - View the mounting status of a NAS file system

```
$ df - T
 Filesystem Type 1K - blocks Used Available Use
 % Mounted on
/ dev / vda1 ext4 41151808 5658860 33379516 15
 % /
 devtmpfs devtmpfs 8122760 0 8122760 0 % / dev
 tmpfs tmpfs 8133492 0 8133492 0 % / dev / shm
 tmpfs tmpfs 8133492 552 8132940 1 % / run
 tmpfs tmpfs 8133492 0 8133492 0 % / sys / fs /
 cgroup
```

```
fid - xxxx . cn - hangzhou . nas . aliyuncs . com :/
nfs4   1099511627   776   2498679808   1097012947   968   1
% / mnt
```

- Unmount the file system

```
$  umount  / mnt
```

5.2 Unmount a file system from an ECS instance that runs Windows

This section describes how to unmount a NAS file system whose protocol type is SMB from an ECS instance that runs Windows.

Procedure

1. Open the command prompt, enter the `NET USE` command to view all of the available network connections

   Example:

```
Status                    Local         Remote              Network
-----------------------------------------------------------------------------
OK                                   \\ name \ IPC $
Microsoft   Windows   Network
OK                                   \\ name2 \ folder
Microsoft   Windows   Network
```

2. You can use the `net use \\ name / delete` command or the `net use \\ name2 \ folder / delete` command to unmount a specific file system.

   Note:

   - You can use the `net use * / delete` command to manually unmount all of the available file systems in Windows.
   - You can use the `Net use */ delete / y` command to automatically unmount all of the file systems in Windows.

3. Open the command prompt, enter the `NET USE` command to verify that all of the available file systems are unmounted.