# Alibaba Cloud
# Apsara File Storage NAS

## User Guide

Issue: 20190605

# 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:<br>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:<br>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. |  Notice:<br>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:<br>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 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.

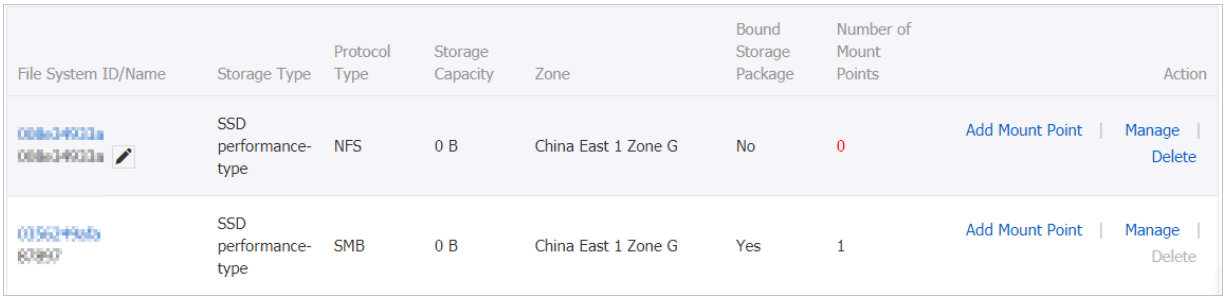
## Prerequisites

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

1. Log on to the *NAS console*.
2. *Create a file system*Create 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.

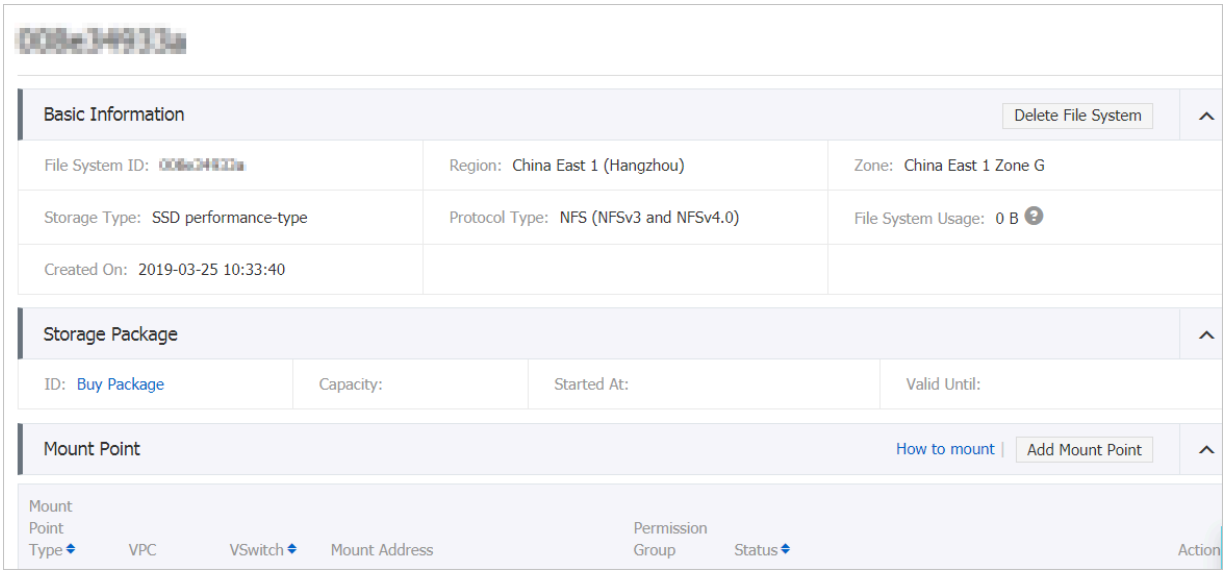


| File System ID/Name | Storage Type | Protocol Type | Storage Capacity | Zone | Bound Storage Package | Number of Mount Points | Action |
|---|---|---|---|---|---|---|---|
| [redacted] | SSD performance-type | NFS | 0 B | China East 1 Zone G | No | 0 | Add Mount Point \| Manage \| Delete |
| [redacted]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

# 2 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.

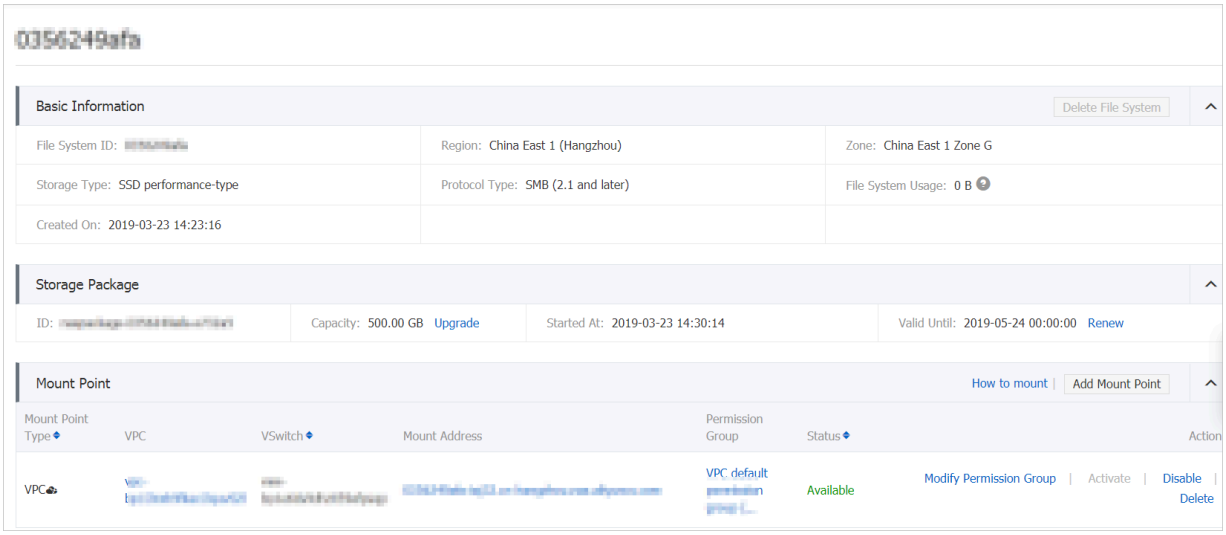
## Prerequisites

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

1. Log on to the *NAS console*.
2. *Create a file system*Create at least one file system.
3. *Add a mount point*Add 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 *Add a mount point*.

### 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.

# 3 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:

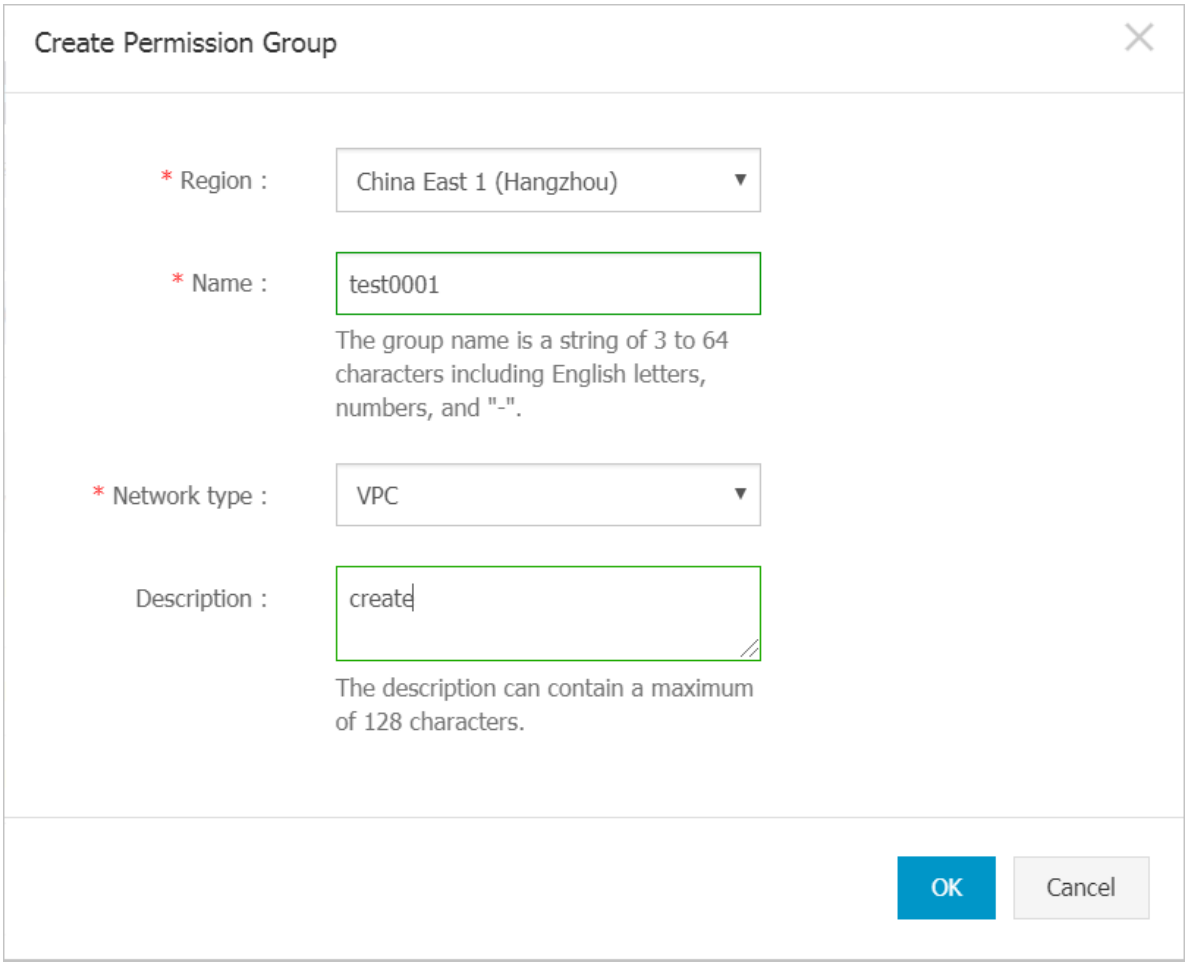
- For a mount point that is located in a classic network, no default permission group is provided. You need to bind a custom permission group to the mount point. In the custom permission group, you can only specify one IP address in each rule, and IP segments are not supported.
- We recommend that you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

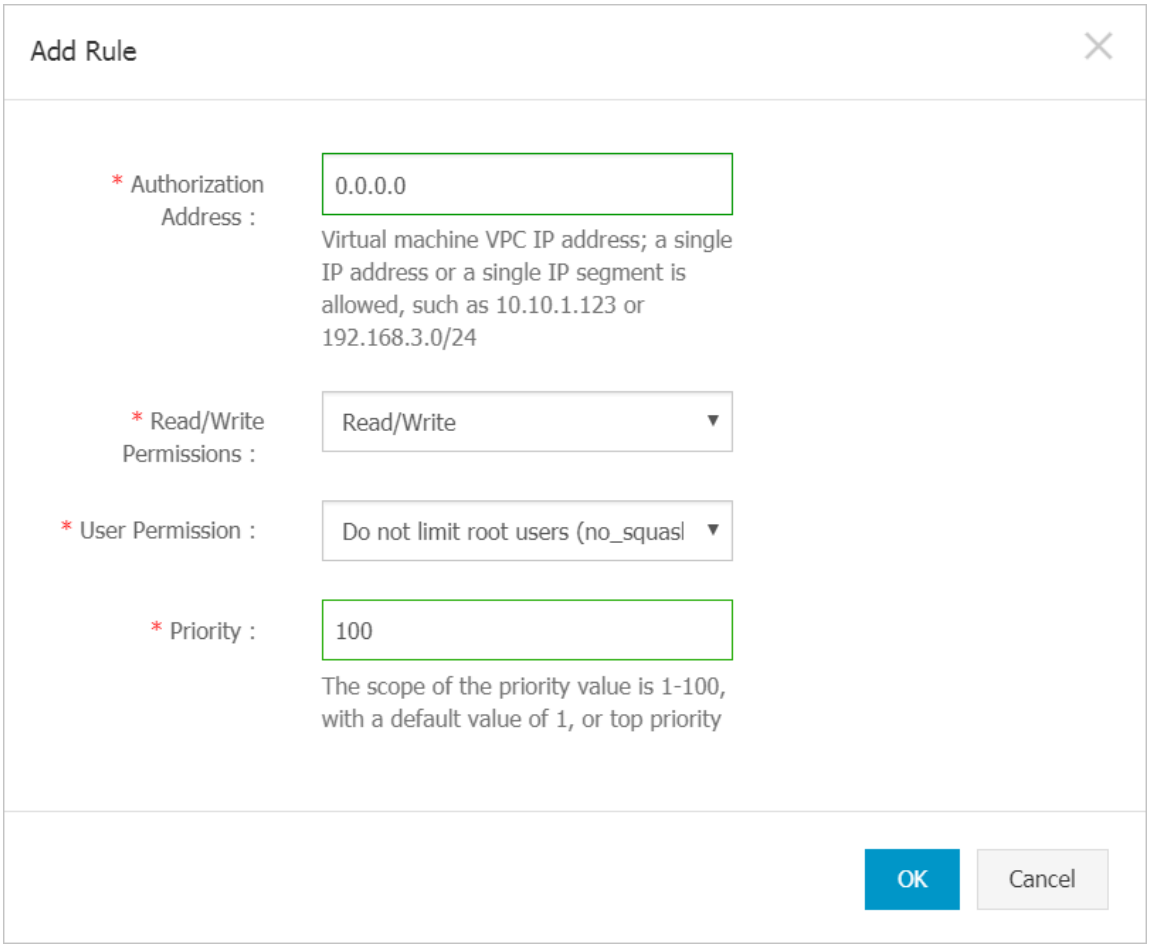
## Manage permission group rules

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.



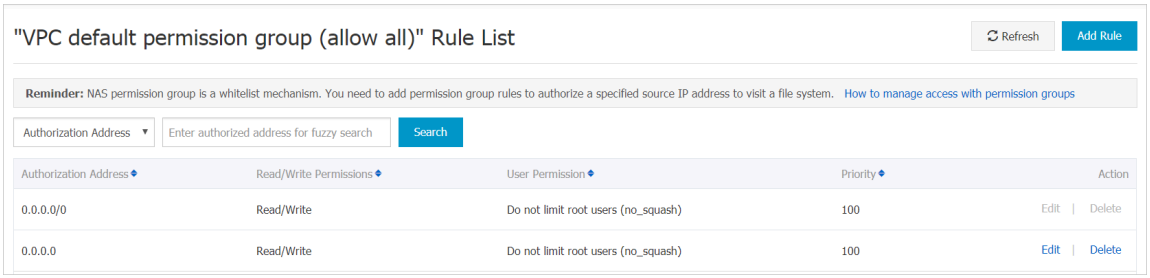

For a rule, you can configure the following options.

| 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.<br>When a Linux user attempts to access the files or directories of a file system, the specified user permission is checked.<br>- Do not limit root users (no_squash): allows access to a file system from root users.<br>- Limit root users (root_squash): denies access to a file system from root users. All root users are treated as nobody users.<br>- 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.



# 4 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.

## NAS operations that you can authorize in RAM

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. |
| 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. |

## NAS resources that you can authorize in RAM

You can only define RAM policies for the following resources:

| Resource | Description |
| --- | --- |
| * | Indicates all NAS resources. |

### Example

The following policy allows read-only access to all NAS resources.

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