Alibaba Cloud NAS

Console User Guide

Issue: 20191112

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, consequent**

ial, 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 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 contact Alibaba Cloud directly if you discover any errors in this document.

Document conventions

Style	Description	Example
	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.
	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.
	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.
	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]`

Style	Description	Example
{} or {a|b}	**This format is used for a required value, where only one item can be selected.**	`switch {active|stand}`

Contents

1 Manage permissions

1.1 Use RAM to manage users' access to resources

You can create RAM user accounts to manage users and their access to Aspara File Storage NAS resources.

Context

You can create and manage multiple RAM user accounts with a single Alibaba Cloud account. You can grant different permissions for each RAM user account. This allows each RAM user account to have different access permissions on Alibaba Cloud resources. With RAM, you do not need to share an AccessKey with another account. You can assign minimal permissions to each user to reduce your data security risks.

Create a RAM user

1. **Log on to the *RAM console* by using an Alibaba Cloud account.**
2. **In the left-side navigation pane, choose Identities > Users, and click Create User.**
3. **Configure the user account information.**
4. **Select Console Password Logon and Programmatic Access under Access Mode.**
5. **Select Custom Logon Password under Console Password, enter a password, and select Required at Next Logon under Password Reset.**
6. **Optional. Select Required to Enable MFA under Multi-factor Authentication and click OK.**
7. **Save the new account, logon password, AccessKey ID, and AccessKey secret.**

> **Note:**
> **We recommend that you save the AccessKey information in a timely manner and keep all details strictly confidential.**

Create a user group

If you attempt to create multiple RAM user accounts, you can group RAM user accounts with identical responsibilities into the same group and authorize the group. This makes it easier to manage users and their permissions.

1. **Log on to the *RAM console* by using an Alibaba Cloud account.**
2. **In the left-side navigation pane, choose Identities > Groups, and click Create Group.**
3. **Enter a group name and display name, and click OK.**

Grant permissions to a RAM user or group

By default, a new RAM user or group does not have any permissions. You need to grant permissions to the RAM user or group to ensure that the user or group can access resources by using the console or API operations. The following steps take a RAM user account as an example to grant permissions.

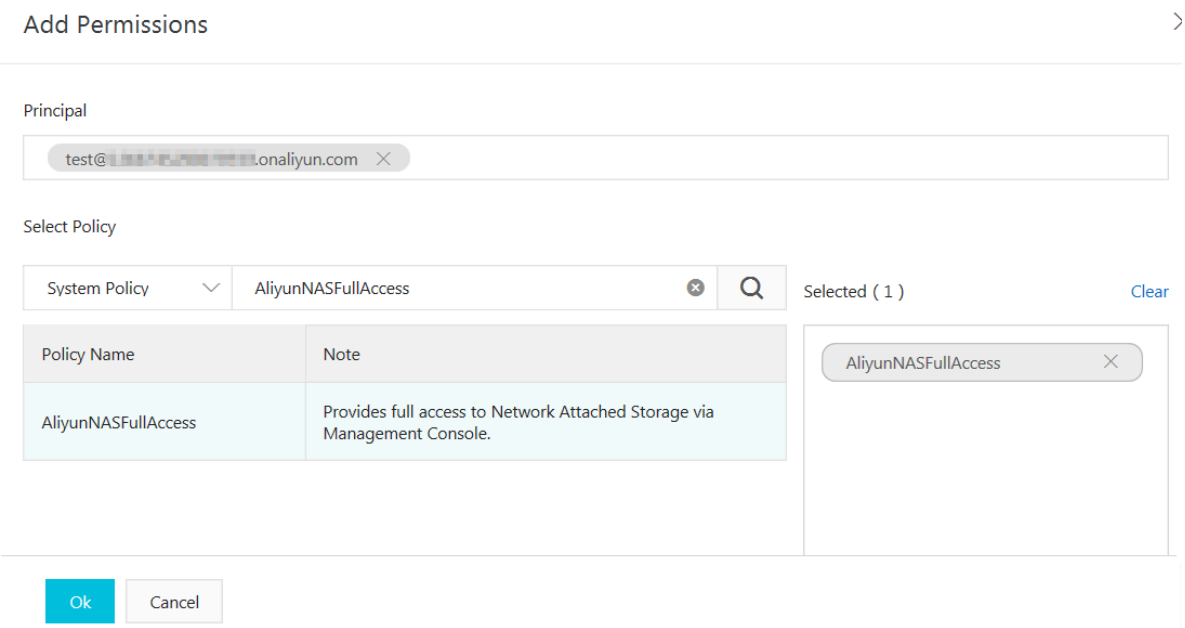
Alibaba Cloud provides two system polices for you to manage access to Aspara File Storage NAS resources. You can grant one of the following policies to a RAM user account as required.

- **AliyunNASFullAccess: This policy grants a RAM user account full access to Aspara File Storage NAS resources.**
- **AliyunNASReadOnlyAccess: This policy grants a RAM user account read-only access to Aspara File Storage NAS resources.**

Note:
If these two system policies cannot meet your business requirements, you can create custom policies. For more information, see *Create a custom policy*.

1. **On the Users page, select a RAM user account to be authorized, and click Add Permissions.**

2. **In the Add Permissions dialog box, select the required NAS permission and grant the permission to the RAM user account.**



1.2 Create a custom policy

This topic describes how to create a custom policy and grant the policy to a RAM user account. Custom policies can better satisfy your specific requirements and help better manage access to your Apsara File Storage NAS resources.

Procedure

1. **Log on to the *RAM console* by using an Alibaba Cloud account.**
2. **In the left-side navigation pane, select Policies, click Create Policy, and follow the instructions to create a policy. The following takes the NASReadOnlyAccess policy as an example. This policy allows read-only access to all Aspara File Storage NAS resources. For more information about the script syntax, see *#unique_6*.**

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

The following table lists the API operations that you can call to manage Apsara File Storage NAS file systems.

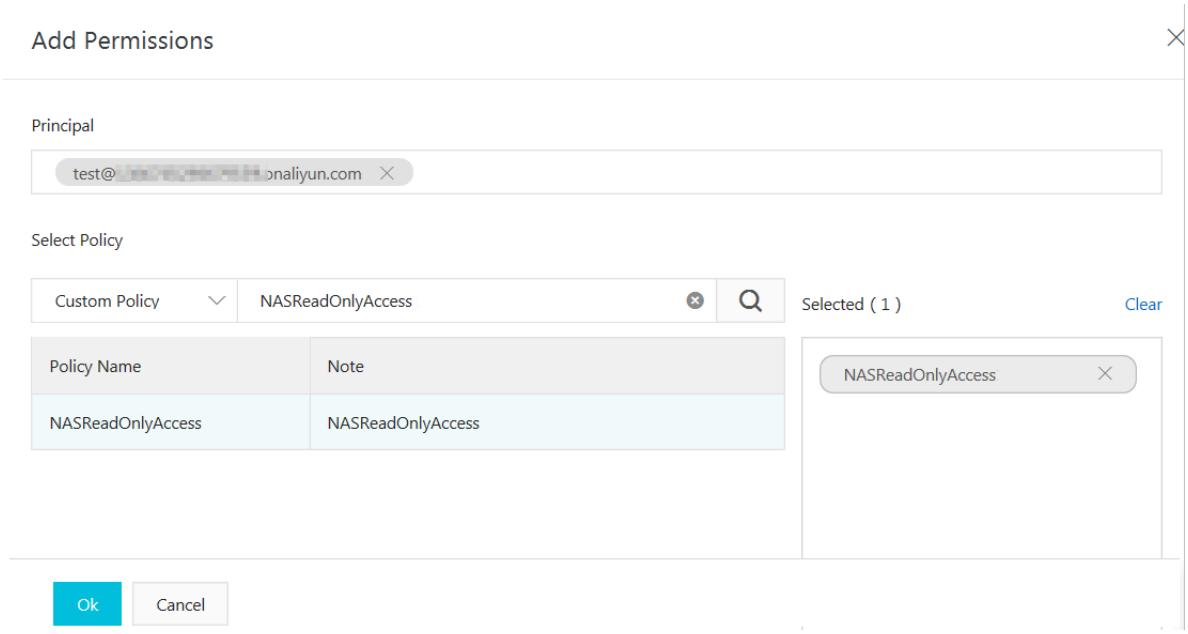
Operation	Description
DescribeFileSystems	Lists all file systems.
DescribeMountTargets	Lists all mount targets of a file system.
DescribeAccessGroup	Lists all permission groups.
DescribeAccessRule	Lists all rules added to a permission group.
CreateMountTarget	Adds a mount target for a file system.
CreateAccessGroup	Creates a permission group.
CreateAccessRule	Adds a rule to a permission group.
DeleteFileSystem	Deletes a file system.
DeleteMountTarget	Deletes a mount target.
DeleteAccessGroup	Deletes a permission group.
DeleteAccessRule	Deletes a rule that is added to a permission group.
ModifyMountTargetStatus	Enables or disables a mount target.
ModifyMountTargetAccessGroup	Modifies the permission group of a mount target.
ModifyAccessGroup	Modifies a permission group.
ModifyAccessRule	Modifies a rule added to a permission group.

The following table shows the accessible Apsara File Storage NAS resources.

Resource	Description
*	All Apsara File Storage NAS resources

3. After the policy is created, go to the Users page.

4. Select a RAM user account to be authorized, click Add Permissions, select the required NAS permission, and grant the permission to the RAM user account.



1.3 Manage permission groups

This topic describes how to manage permission groups in the Apsara File Storage NAS console. The management includes creating and deleting permission groups and rules, viewing a list of permission groups, and viewing the list of rules.

Context

In Apsara File Storage NAS, each permission group represents a whitelist. You can add rules to a permission group, allowing access to a file system from specific IP addresses or IP segments. You can also assign different access permissions to different IP addresses or IP segments.

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

Note:

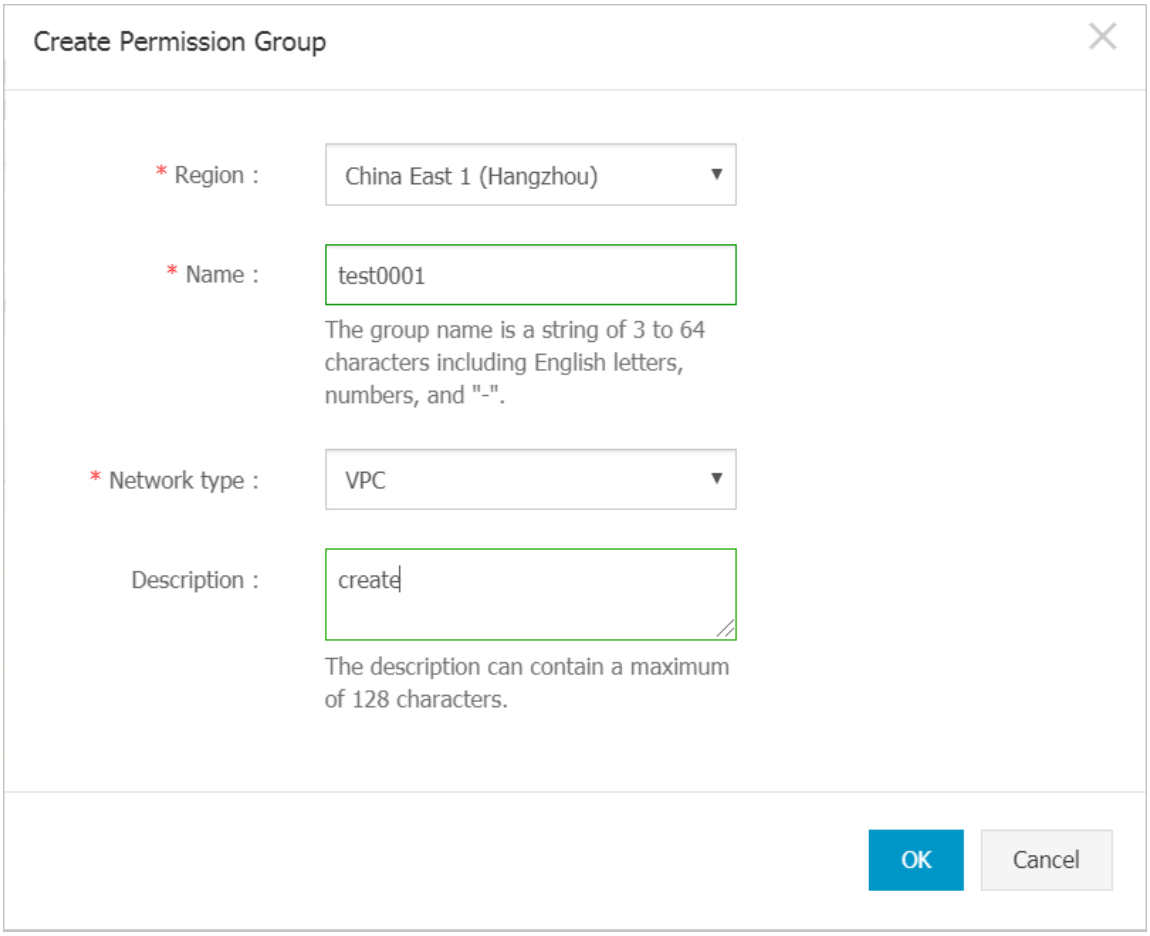
- For a mount target that is located in the classic network, no default permission group is provided. You need to bind a custom permission group to the mount

target. 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 add rules for required IP addresses and IP segments to ensure data security.
- You cannot delete or modify the default permission group and its rules.
- You can create up to 10 permission groups by using an Alibaba Cloud account.

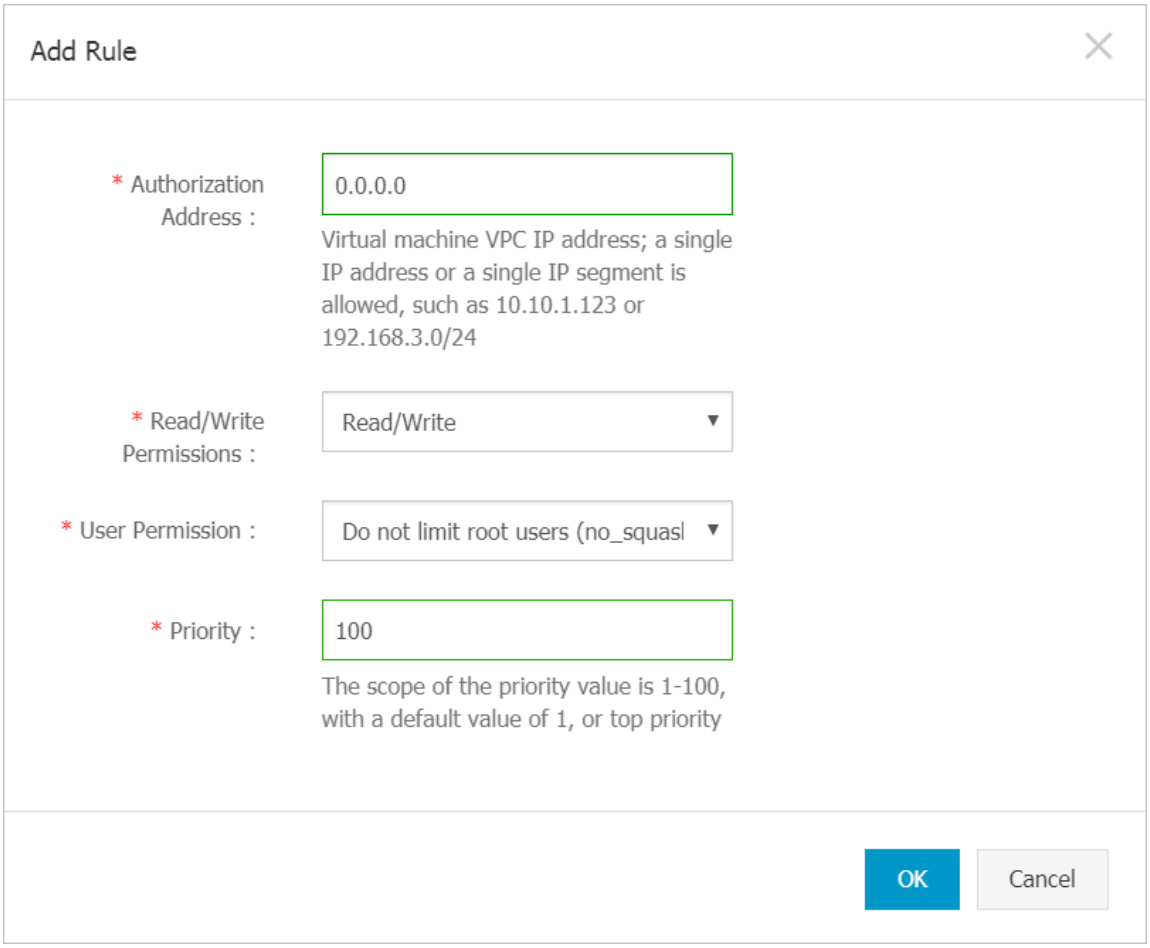
Create a permission group and add rules

1. Log on to the *NAS console*.
2. Create a permission group.
   a) Choose NAS > Permission Group and click Create Permission Group.
   b) In the Create Permission Group dialog box, configure the required settings.



Setting	Description
Region	The region of the permission group.
Name	The name of the permission group.
Network Type	Valid values: VPC and classic network.

3. **Add rules to a permission group.**
   a) **Find the target permission group and click Manage.**
   b) **On the Permission Group Rules page, click Add Rule.**
   c) **Configure the required settings.**



Setting	Description
Authorization Address	The authorized object to which this rule applies.
Read/Write Permissions	Specifies whether to allow read-only or read/write access to the file system from the authorized object. Valid values: Read-only and Read/Write.

Setting	Description
User Permission	Specifies whether to limit a Linux user's access to a file system. · Do not limit root users (no_squash): allows access to a file system for root users. · Limit root users (root_squash): denies access to a file system for root users. All root users are treated as nobody users. · Limit all users (all_squash): denies access to a file system for all users including root users. All users are treated as nobody users. The nobody user is a default user in Linux systems. The nobody user features the least permissions and high-security, which can only access the open-shared content of servers.
Priority	When multiple rules are applied to an authorized object, the rule with the highest priority takes effect. Valid values: 1 to 100, in which 1 is the highest priority.

d) Click OK.

More actions

On the Permission Group page, you can perform the following actions.

Action	Description
View the list of permission groups or the details of a permission group.	View the list of permission groups in a region or view the details of a permission group. The details include the type, number of rules, and number of linked file systems.
Modify a permission group	Find the target permission group and click Edit to edit the description of the permission group.
Delete a permission group	Find the target permission group and click Delete to delete the permission group.
View the list of rules	Find the target permission group and click Manage to view the list of rules in the permission group.
Modify a rule	Click Manage, find the target rule, and click Edit to edit fields including the Authorization Address, Read/Write Permissions, User Permission, and Priority.

Action	Description
Delete a rule	Click Manage, find the target rule, and click Delete to delete the rule.

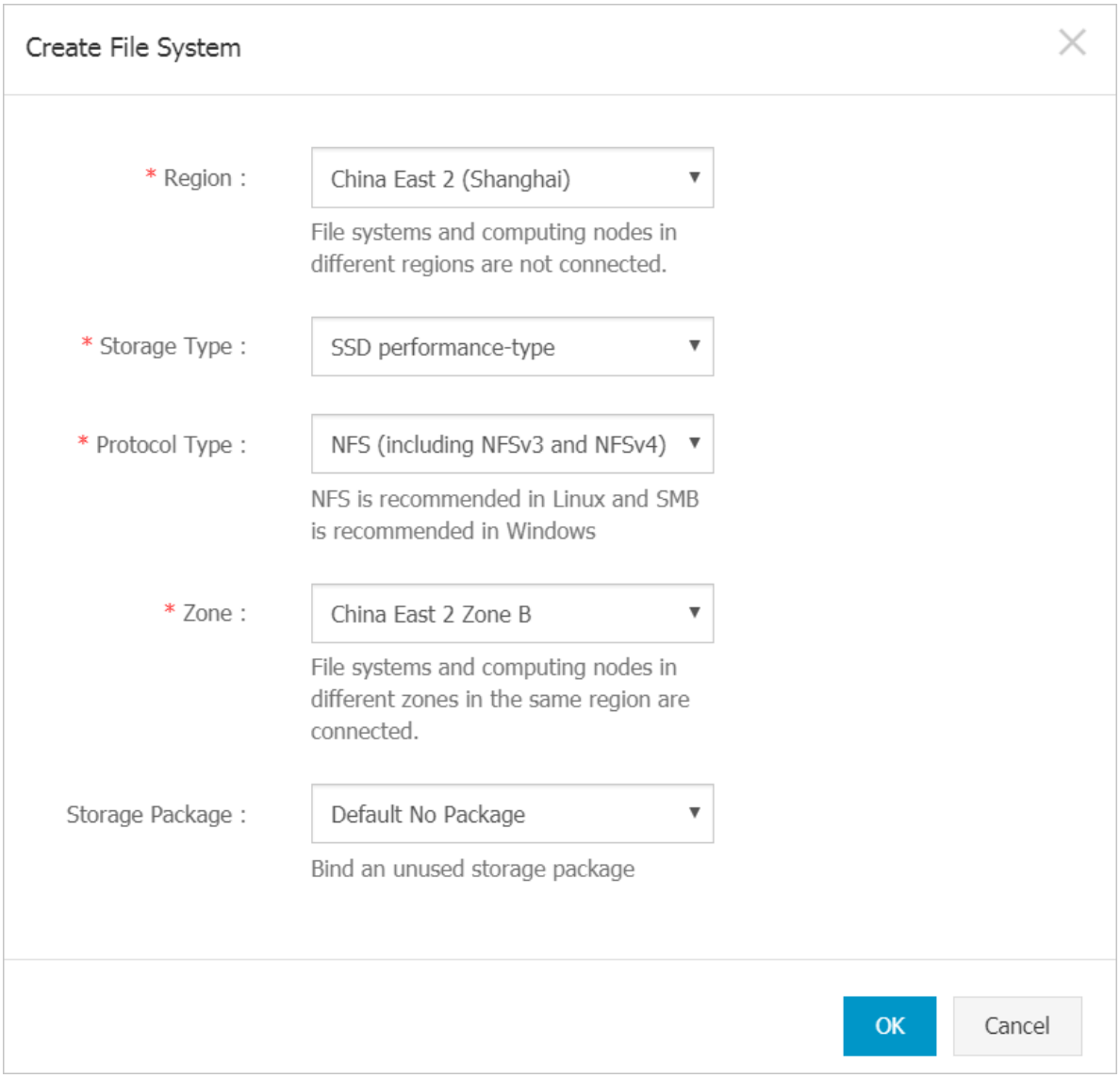
2 Manage file systems

This topic describes how to manage file systems in the NAS console. The management includes how to create and delete file systems. It also includes details about how to view a list of file systems and provides further details of each file system.

Create file systems

1. **Log on to the *NAS console*.**
2. **Choose NAS > File System List and click Create File System.**

3. **In the Create File System dialog box, configure the required settings.**



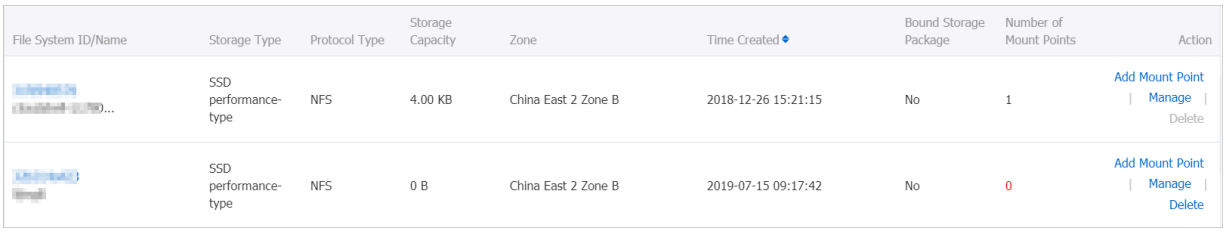
Parameter	Description
Region	Select a region where you want to create a file system. **Note:** · When a file system and an ECS instance are located in different regions, you cannot mount the file system on the ECS instance. · The supported storage types and protocol types of a file system vary depending on the region. For more information, see *Regions and supported storage types and protocols*. · You can create up to 20 file systems in a region by using an Alibaba Cloud account.
Storage Type	Valid values: SSD performance-type and Capacity-type. **Note:** The maximum capacity of an Apsara File Storage NAS Performance file system is 1 PB. The maximum capacity of an Apsara File Storage NAS Capacity file system is 10 PB. You are billed on the pay-as-you-go basis.
Protocol	Valid values: NFS (including NFSv3 and NFSv4) and SMB (2.1 and later). NFS is used to share files stored on an ECS instance that runs Linux. SMB is used to share files stored on an ECS instance that runs Windows.

Parameter	Description
Zone	Each region has multiple isolated locations known as zones. The power supply and network of each zone are independent. Select a zone from the drop-down list. We recommend that you select the zone where the target ECS instance resides. **Note:** When a file system and an ECS instance are located in different zones in the same region, you can mount the file system on the ECS instance.
Storage Package	Storage packages are optional for a file system. If you buy a storage package, you can enjoy an extra discount over the fee charged by using the pay-as-you-go billing method. If you do not purchase a storage package, you are billed on the pay-as-you-go basis by default. For more information, see *Pricing*.

4. Click OK to create the new file system.

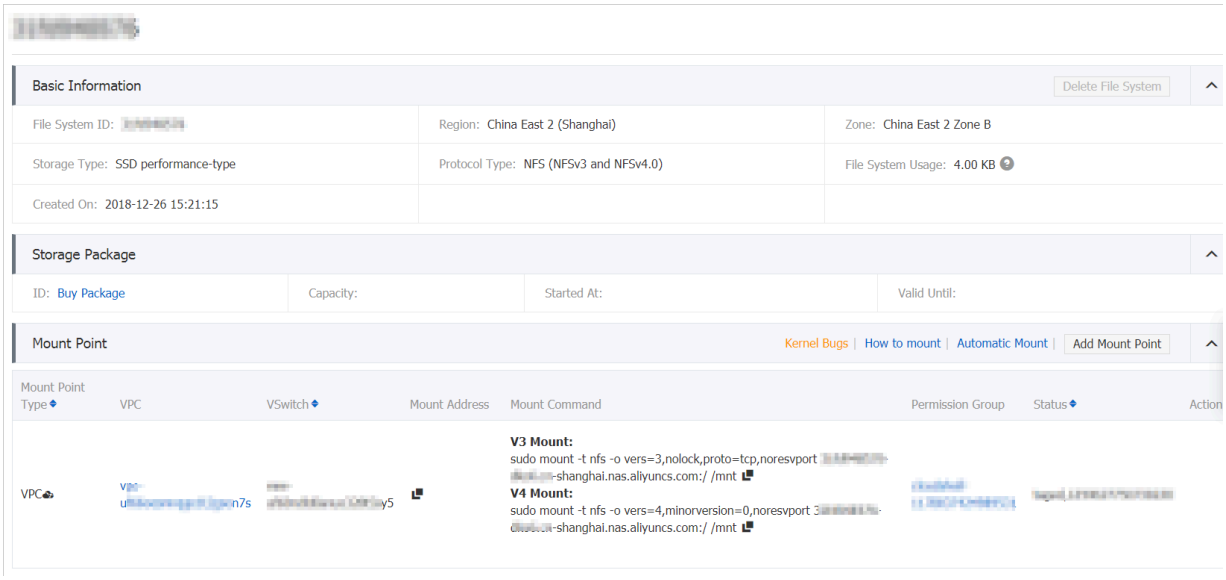
View the list of file systems

On the File System List page, you can view the list of all file systems in a region. On the File System List page, find the target file system and modify the name of the file system.



View the details of a file system

Find the target file system, and click the file system ID or Manage to open the File System Details page. You can view basic information, storage packages, and mount targets of the file system.



Delete a file system

Find the target file system, click Delete to delete the file system.

Note:

- **You must remove all mount targets of a file system before deleting the file system.**
- **Use caution: You cannot restore the data on a file system after it is deleted.**

3 Manage mount targets

This topic describes how to manage mount targets in the NAS console. The management includes how to create, delete, enable, and disable mount targets. It also includes details about how to view mount targets, and modify the permission group of a mount target.

Add a mount target

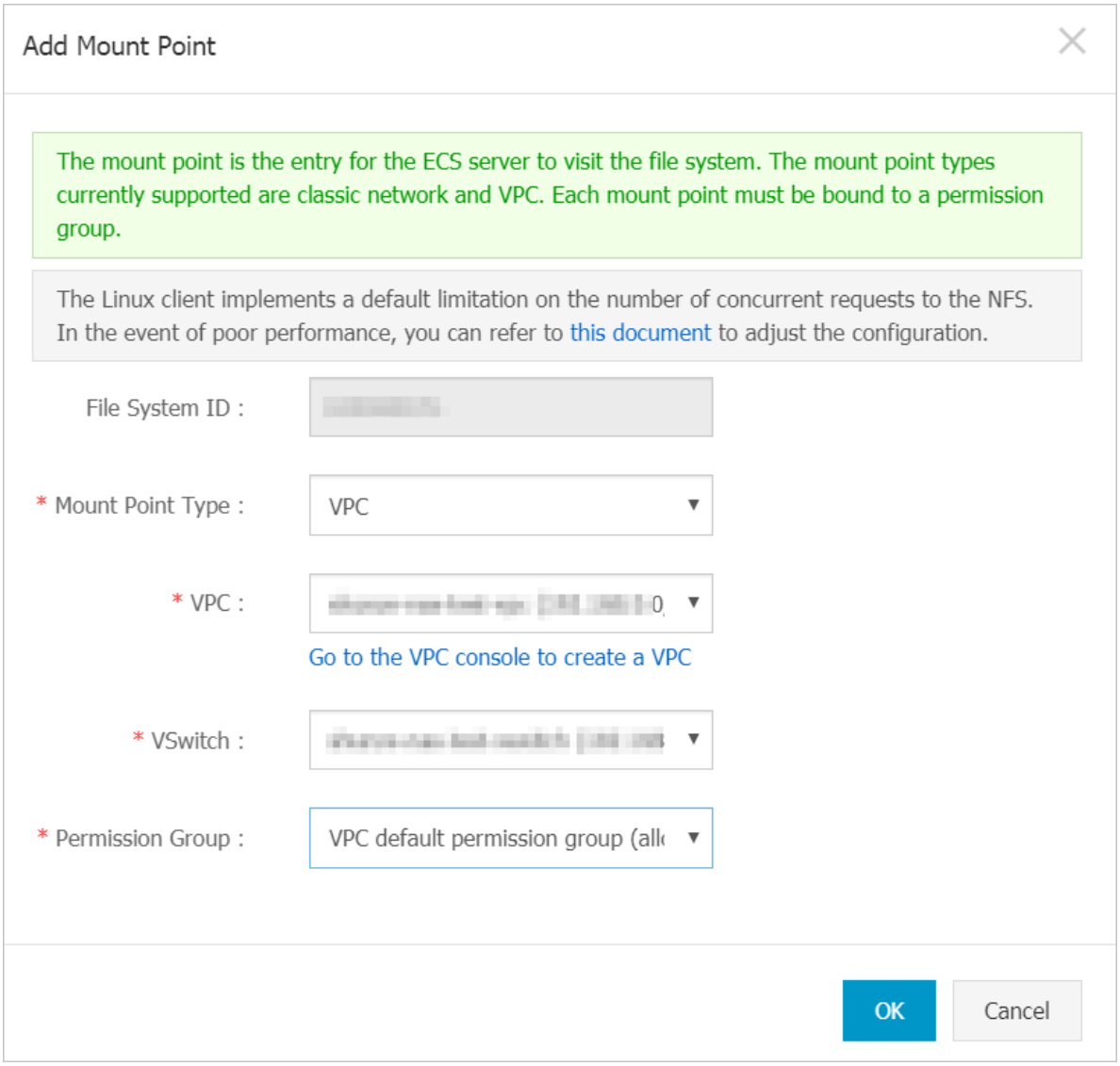
You must use a mount target to mount a file system on an ECS instance. You can perform the following steps to add a mount target in the NAS console.

Note:

You can add two mount targets for an Apsara File Storage NAS Capacity file system or Apsara File Storage NAS Performance file system either in a classic network or a virtual private cloud (VPC).

1. **Log on to the *NAS console*.**
2. **Choose NAS > File System List.**
3. **Find the target file system and click Add Mount Point.**

4. In the Add Mount Point dialog box, configure the required settings.



Mount Point Type includes VPC and classic network.

- **If you want to create a mount target in a VPC, configure the required settings.**

Parameter	Description
VPC	Select a VPC. If no VPC is available, create a VPC in the *Virtual Private Cloud console*. **Note:** **The VPC and VSwitch you select must be the same as those of the ECS instance on which you mount a file system.**

Parameter	Description
VSwitch	Select a VSwitch that is created in the VPC.

Parameter	Description
Permission Group	Select VPC default permission group (allow all) or an existing permission group. **Note:** This VPC default permission group is generated for each Alibaba Cloud account, which allows access to the file system through the mount target from all IP addresses of the VPC. For more information about how to create a permission group, see *Manage permission groups*.

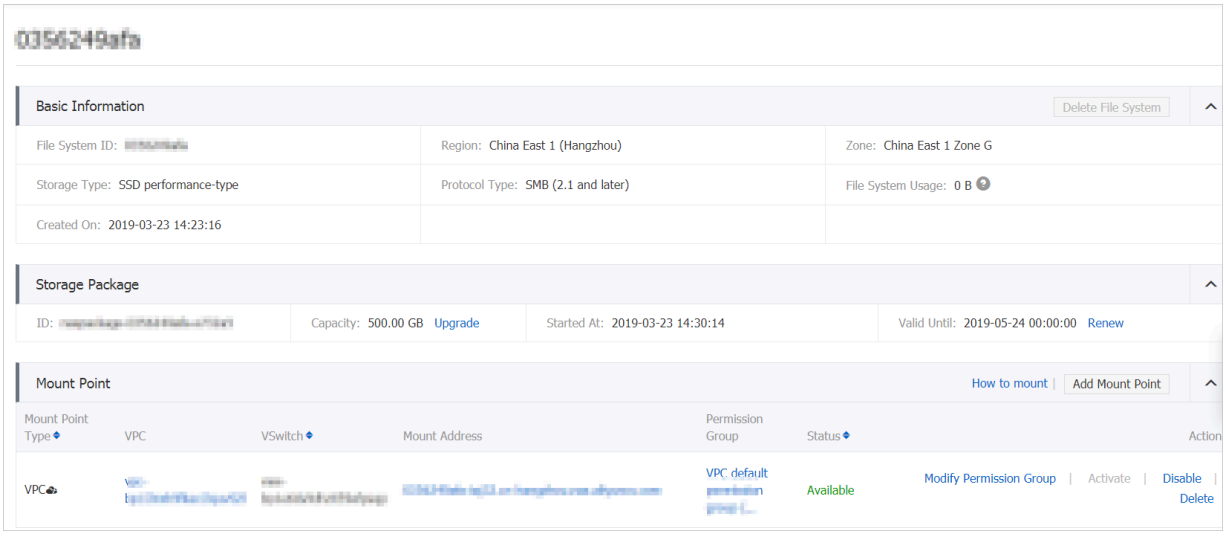
- If you want to create a mount target in a classic network, configure the required settings.

Parameter	Description
Permission group	Select a permission group. If no available permission group exists, create a permission group in the *NAS console*.  **Note:** - You can create a mount target in a classic network only in a region located in mainland China. - You can attach a mount target in a classic network only to an ECS instance. - For data security, no default permission group is available for a mount target in a classic network. You need to create a permission group for the mount target in the classic network and add required rules to the permission group. For more information about how to manage permission groups, see *Manage permission groups*. - When creating a mount target in a classic network for the first time, you are required to use RAM to authorize the NAS service to access ECS instances hosted by the logon Alibaba Cloud account. We recommend that you follow the instructions to complete the authorization before creating a mount target in a classic network. For more information, see *#unique_12*.

5. After you complete the configuration, click OK.

View mount targets

On the File System List page, find the target file system, and click Manage to open the File System Details page. In the Mount Point section, view the information of mount targets.



Enable or disable a mount target

You can perform the following actions to manage access from clients to a file system through a mount target.

- **Click Disable to disable access from clients to a file system through a mount target.**
- **Click Enable to enable access from clients to a file system through a mount target.**

Delete a mount target

Click Delete to delete a mount target.

Note:
Use caution: You cannot restore a mount target after it is deleted.

Modify the permission group of a mount target

Click Modify Permission Group to modify the permission group of a mount target. For more information about permission groups, see *Manage permission groups*.

Note:
After you modify the permission group, the modification process requires about one minute to complete.

4 Mount a file system

4.1 Precautions

Before you mount a file system, we recommend that you familiarize yourself with the following precautions.

Note:

You can only create mount points of the VPC type and mount NFS file systems in NAS Extreme.

- **If the type of a mount point is VPC, you can only mount a linked file system on an ECS instance in the VPC where the mount point resides. The specified authorization address of a rule included in the permission group that is linked to the mount point must match the IP range of the VPC that hosts the ECS instance.**
- **If the type of a mount point is classic network, you can only mount a file system on an ECS instance owned by the same account as that of the mount point. The specified authorization address of a rule included in the permission group that is linked to the mount point must match the IP range of the private network that hosts the ECS instance.**
- **You can manually mount a file system or enable an automatic mount at startup.**
  - **For more information about how to manually mount a file system on an ECS instance running Linux, see** *Mount an NFS file system*.
  - **For more information about how to manually mount a file system on an ECS instance running Linux, see** *Mount an SMB file system*.
  - **For more information about how to enable an automatic mount on an ECS instance running Linux, see** *Enable an automatic mount at startup for an NFS file system* .
  - **For more information about how to enable an automatic mount on an ECS instance running Windows, see** *Enable an automatic mount at startup for an SMB file system*.
- **For more information about how to use Cloud Enterprise Network (CEN) to enable a cross-region mount, see** *Enable a cross-VPC mount for a file system*.
- **For more information about how to use Cloud Enterprise Network (CEN) to enable a cross-account mount, see** *Enable a cross-account mount for a file system*.

- If you need to mount an on-premises file system, use one of the following methods.
  - For more information about how to use a virtual private network (VPN) to mount an on-premises file system, see *#unique_21*.
  - For more information about how to use a network address translation (NAT) gateway to mount an on-premises file system, see *#unique_22*.

4.2 Mount an NFS file system

This topic describes how to install an NFS client in Linux and use the mount command to mount an NFS file system.

Prerequisites

1. You have created a file system. For more information, see *Create file systems*.
2. You have created a mount point. For more information, see *Add a mount target*.

Step 1: Install an NFS client

In Linux, you must install an NFS client before mounting an NFS file system on an ECS instance.

1. Log on to the *ECS console*.
2. Use the following command to install an NFS client.
   - If CentOS, RHEL, or Aliyun Linux is running on the ECS instance, run the following command.

     ```
     sudo yum install nfs-utils
     ```

   - If Ubuntu or Debian is running on the ECS instance, run the following commands.

     ```
     sudo apt-get update
     ```

     ```
     sudo apt-get install nfs-common
     ```

3. Modify the maximum number of concurrent NFS requests. For more information, see *#unique_23*.

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

Step 2: Mount an NFS file system

You can use the domain name of the file system or the domain name of the mount target to mount the NFS file system on an ECS instance. The domain name of the file system is resolved to the IP address of the mount target in a zone where the ECS instance is located.

1. **Log on to the *ECS console*.**
2. **Mount the NFS file system.**
   - **If you need to mount an NFSv4-compliant file system, use the following command.**

     ```
     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:/ /mnt
     ```

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

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

   - **If you need to mount an NFSv3-compliant 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.region.
     nas.aliyuncs.com:/ /mnt
     ```

   The parameters used in the command are described in the following table.

Parameter	Description
Mount point	

Parameter	Description
vers	The version of the file system. Only NFSv3 and NFSv4 are applicable.

When you mount a file system, multiple parameters are available. Separate these parameters with commas (,). We recommend the following values for mount parameters.

Parameter	Description
rsize	You can set the maximum number of bytes of data that the NFS client can receive for each network read request. Recommended value: 1048576
wsize	You can set the maximum number of bytes of data that the NFS client can send for each network write request. Recommended value: 1048576
hard	Indicates that applications stop access to a file system when the file system is unavailable, and wait until the file system is available. We recommended that you use the hard parameter.
timeo	You can set the timeout value that the NFS client uses to wait for a response before it retries an NFS request. Unit: deciseconds. Recommended value: 600 .
retrans	You can set the number of times the NFS client retries a request. Recommended value: 2
noresvport	Indicates that the NFS client uses a new TCP source port when a network connection is re-established to ensure data integrity. We recommend that you use the noresvport parameter.

Note:
If you do not use the preceding values, you must consider the following issues:

- We recommend that you specify a maximum value of 1048576 for both the rsize parameter and the wsize parameter to avoid diminished performance.
- If you must modify the timeo parameter, we recommend that you specify a minimum of 150 for the parameter. The unit of the timeo parameter is decisecond, which is 0.1 second. For example, a value of 150 indicates 15 seconds.
- We recommend that you do not use the soft parameter to avoid data inconsistencies. You must use the soft parameter with careful consideration.
- We recommend that you use the default setting for other mount parameters. For example, changing read or write buffer sizes or disabling attribute caching can result in reduced performance.

3. Use the `mount -l` command to view the mount results.

   An example of a successful mount is shown in the following figure.

   After a file system is mounted, you can use the `df -h` command to view the capacity of the file system.

4.3 Mount an SMB file system

This topic describes how to mount an SMB file system in Windows.

Prerequisites

1. You have created a file system. For more information, see *Create file systems*.
2. You have created a mount point. For more information, see *Add a mount target*.

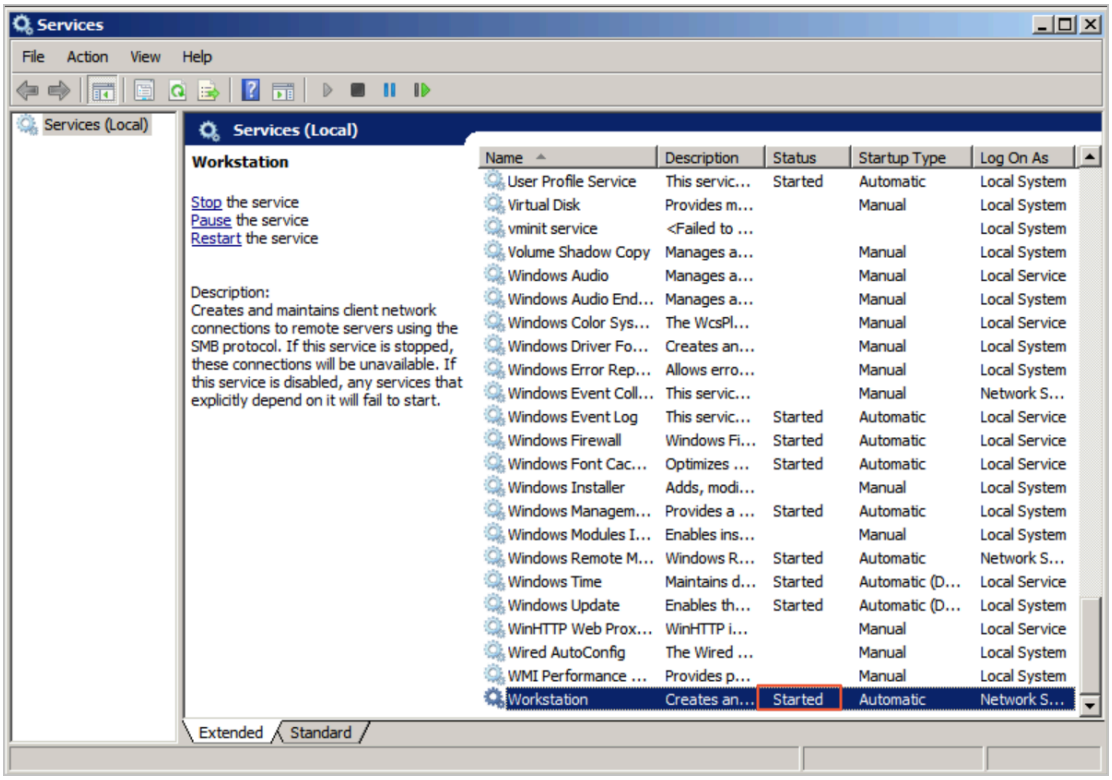
3. Ensure that the following Windows services are started:

   - Workstation

     a. Choose All Programs > Accessories > Run, or press `Win+R` and enter `services.msc` to open the Services console.

     b. Locate the Workstation service and ensure that the status of the service is Started.

     The Workstation service is started by default.



   - TCP/IP NetBIOS Helper

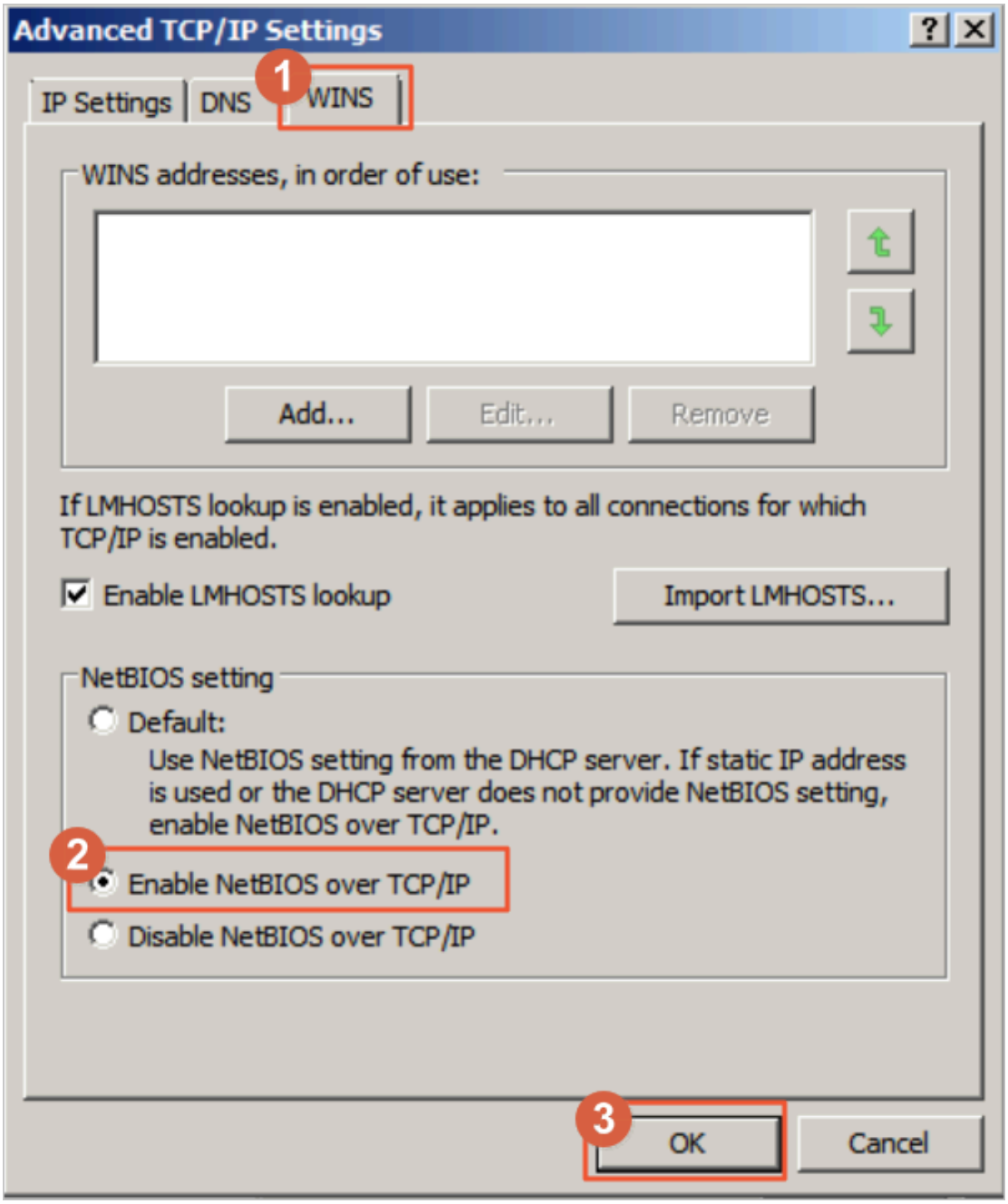
     Perform the following steps to start the TCP/IP NetBIOS Helper service:

     a. Open Network and Sharing Center and click the active network connection.

     b. 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.

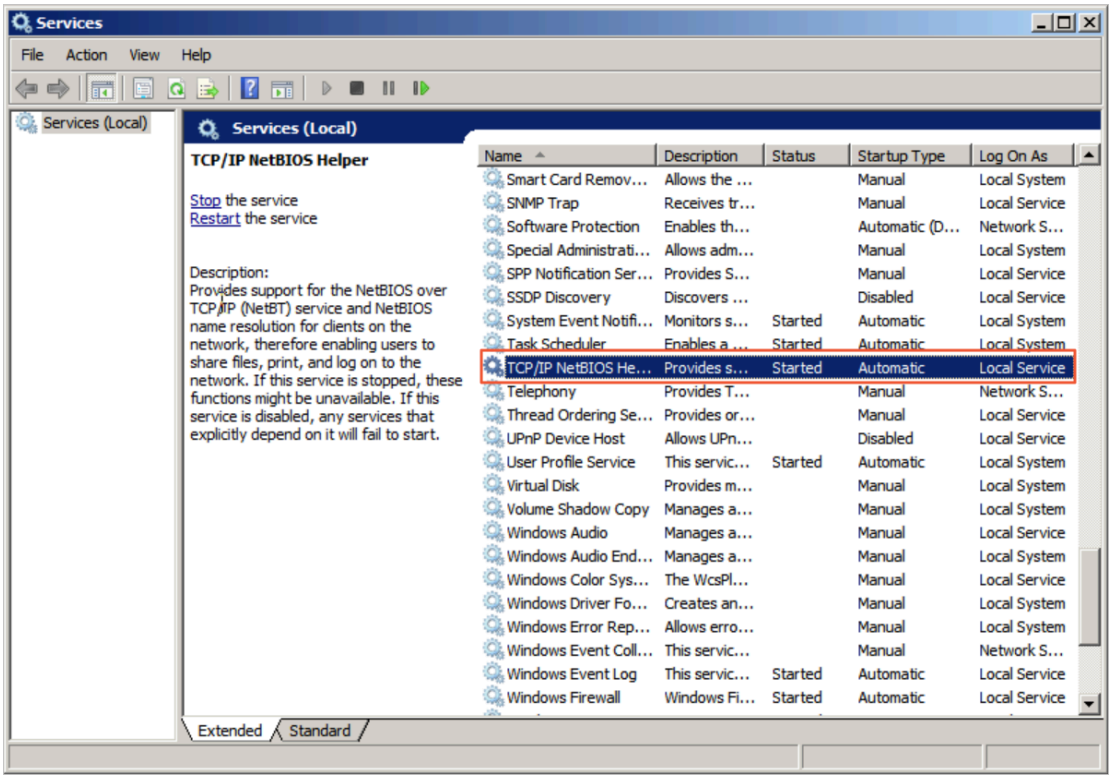
c. **In the Advanced TCP/IP Settings dialog box, choose WINS > Enable NetBIOS over TCP/IP.**



d. **Choose All Programs > Accessories > Run, or press `Win+R` and enter `services.msc` to open the Services console.**

e. **Locate the TCP/IP NetBIOS Helper service and ensure that the status of the service is Started.**

The TCP/IP NetBIOS Helper service is started by default.



Procedure

Perform the following steps to mount an SMB file system.

1. **Open the command prompt and run the following command to mount the file system.**

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

   The format of the command used to mount the file system is `net use <the drive of the mount target> \\<the domain name of a mount point>\myshare`**.**

   - **The drive of the mount target: the target drive on which you need to mount a file system.**
   - **The domain name of a mount point: the domain name generated when you create the mount point for a file system. For more information, see** *Create a mount point***.**
   - **myshare: indicates the name of an SMB share. You cannot change the name.**

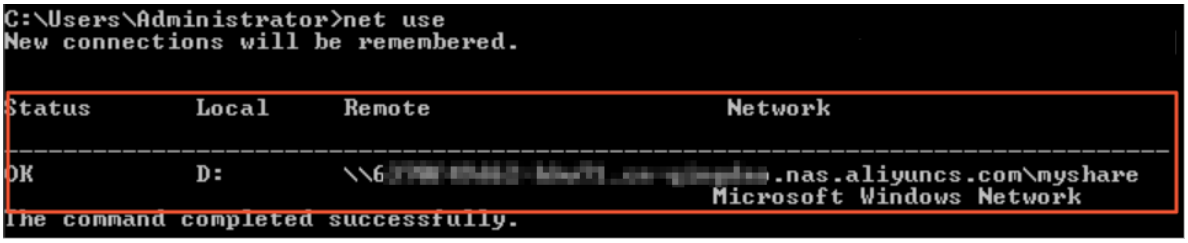
   Note:

   Ensure that the name of the target mount drive is unique on the target ECS instance.

For more information about how to troubleshoot the errors that occur while the mount command is running, see *#unique_25*.

2. **Use the** `net use` **command to view the results.**

   An example of a successful mount is shown in the following figure.



4.4 Enable an automatic mount at startup for an NFS file system

This topic describes how to modify Linux configuration files to allow an NFS file system to be automatically mounted at startup.

Prerequisites

1. **You have created a file system. For more information, see** *Create file systems*.
2. **You have created a mount point. For more information, see** *Add a mount target*.
3. **You have installed an NFS client. For more information, see** *Install an NFS client*.

Prerequisites

We recommend that you configure the `/etc/fstab` **file to enable an NFS file system to be automatically mounted at startup. You can also configure the** `/etc/rc.local` **file to set an automatic mount.**

1. **Configure an automatic mount.**
   - **(Recommended) Open the** `/etc/fstab` **file and add the following command.**

     Note:

If you configure an automatic mount on CentOS 6.x, use the `chkconfig netfs on` command to enable the netfs service to run at startup.

- **If you need to mount an NFSv4-compliant file system, add the following command.**

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

- **If you need to mount an NFSv3-compliant file system, add the following command.**

```
file-system-id.region.nas.aliyuncs.com:/ /mnt nfs vers=3,nolock
,proto=tcp,rsize=1048576,wsize=1048576,hard,timeo=600,retrans=2
,_netdev,noresvport 0 0
```

- **Open the *`/etc/rc.local`* configuration file and add the mount command.**

Note:

Before configuring the *`/etc/rc.local`* file, ensure that you have execute permissions on the *`/etc/rc.local`* and *`/etc/rc.d/rc.local`* files. For example, on CentOS 7.x, no execute permission is granted to a user by default. You must assign the execute permission to a user before configuring the *`/etc/rc.local`* file.

- **If you need to mount an NFSv4-compliant file system, add the following command.**

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

- **If you need to mount an NFSv3-compliant file system, add the following command.**

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

The parameters used in the command are described in the following table.

Parameter	Description
Mount Point	

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 using 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 at startup. For a NAS file system, the value of the parameter is 0. It indicates that fsck is not allowed to run at startup.

2. Run the `reboot` command to restart the ECS instance.

4.5 Enable an automatic mount at startup for an SMB file system

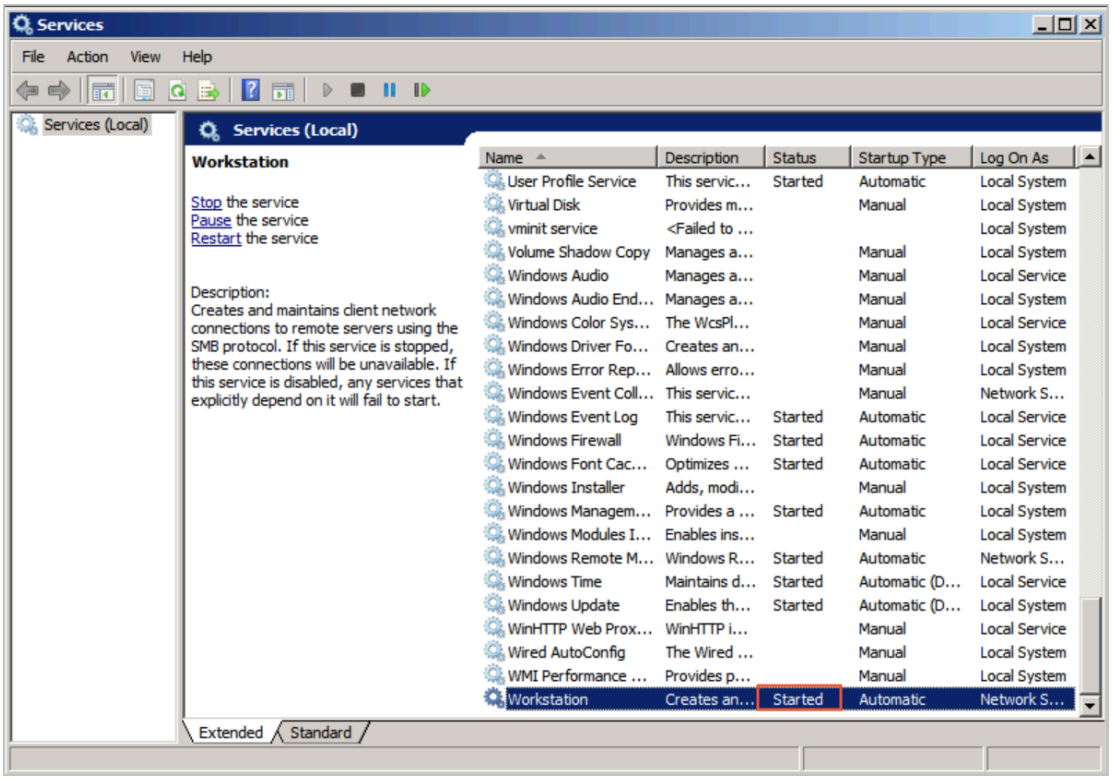
This topic describes how to create a mount script and a scheduled task to enable an automatic mount at startup for an SMB file system.

Prerequisites

1. You have created a file system. For more information, see *Create file systems*.
2. You have created a mount target. For more information, see *Add a mount target*.

3. You must make sure that the following Windows services are started:
   - Workstation
     a. Choose All Programs > Accessories > Run, or press `Win+R` and enter `services.msc` to open the Services console.
     b. Find the Workstation service and ensure that the service is Running and the startup type is Automatic.

        The Workstation service is running by default.



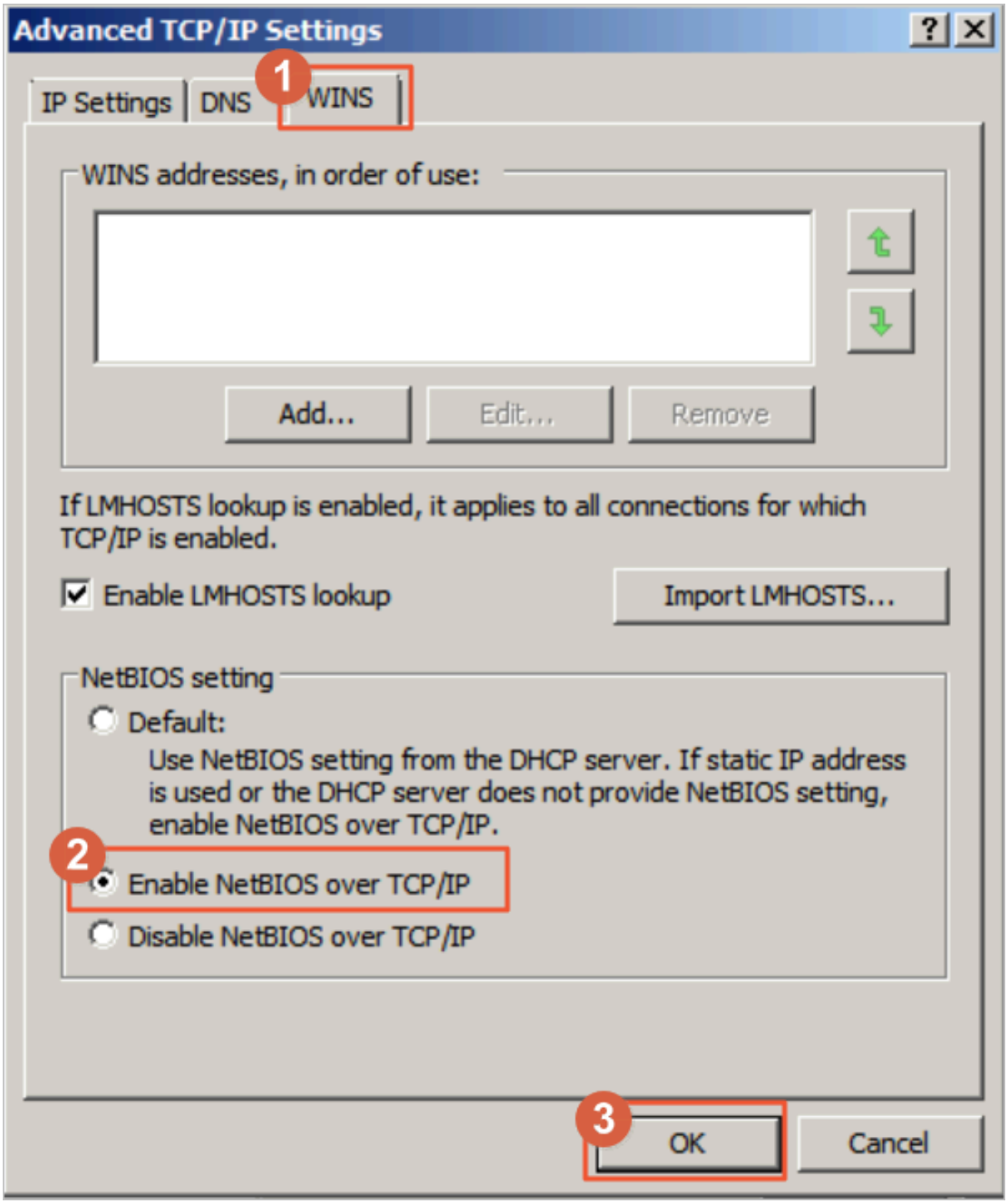
   - TCP/IP NetBIOS Helper

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

     a. Open Network and Sharing Center and click the active network connection.
     b. Click Properties to open the Local Area Network Properties dialog box. Double-click Internet Protocol Version 4 (TCP/IPv4). In the Internet

Protocol Version 4 (TCP/IPv4) Properties dialog box that appears, click Advanced.

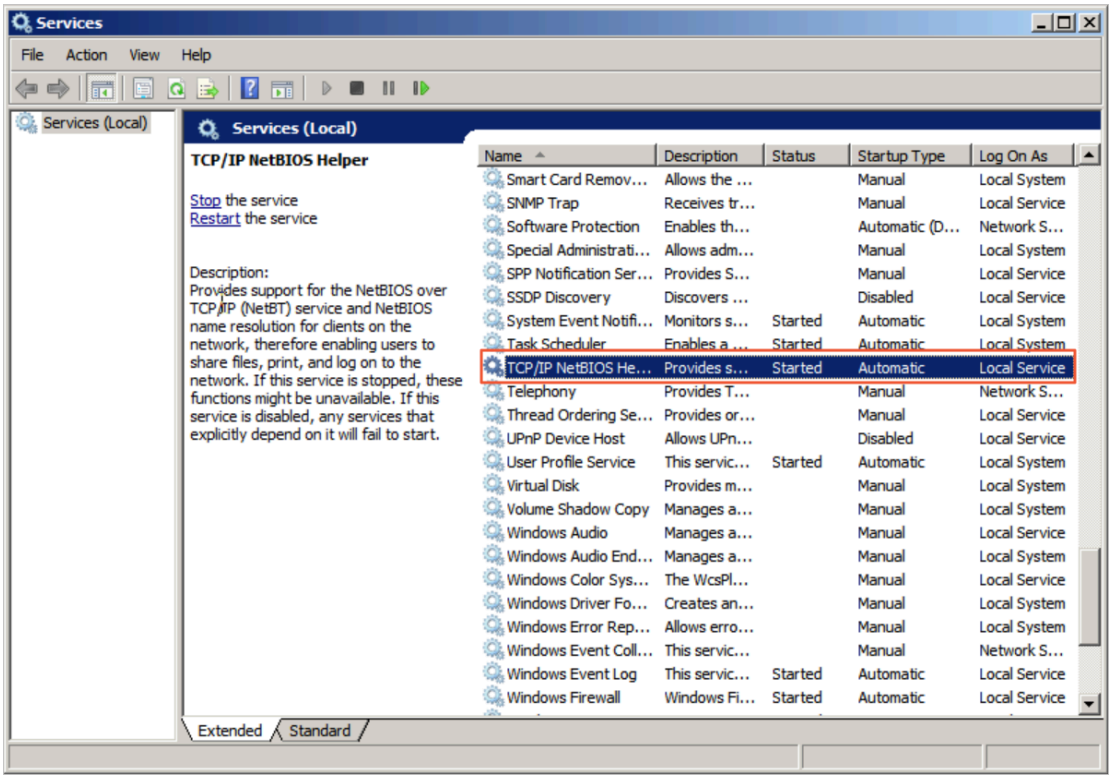
c. In the Advanced TCP/IP Settings dialog box, choose WINS > Enable NetBIOS over TCP/IP.



d. Choose All Programs > Accessories > Run, or press `Win+R` and enter `services.msc` to open the Services console.

e. Find the TCP/IP NetBIOS Helper service and ensure that the service is Running and the startup type is Automatic.

The TCP/IP NetBIOS Helper service is running by default.



Procedure

1. **Create a script file named *nas_auto.bat* and add the following command to the file.**

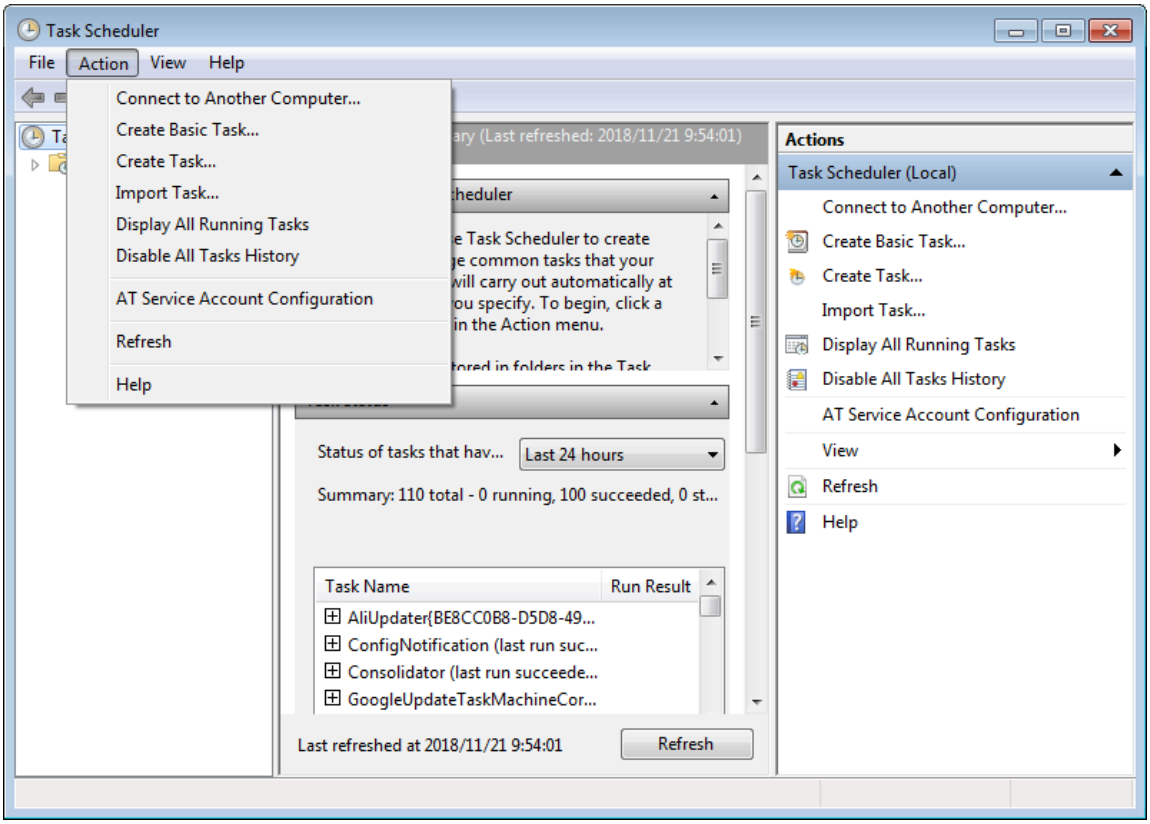
```
net use D: \\file-system-id.region.nas.aliyuncs.com\myshare
```

Note:

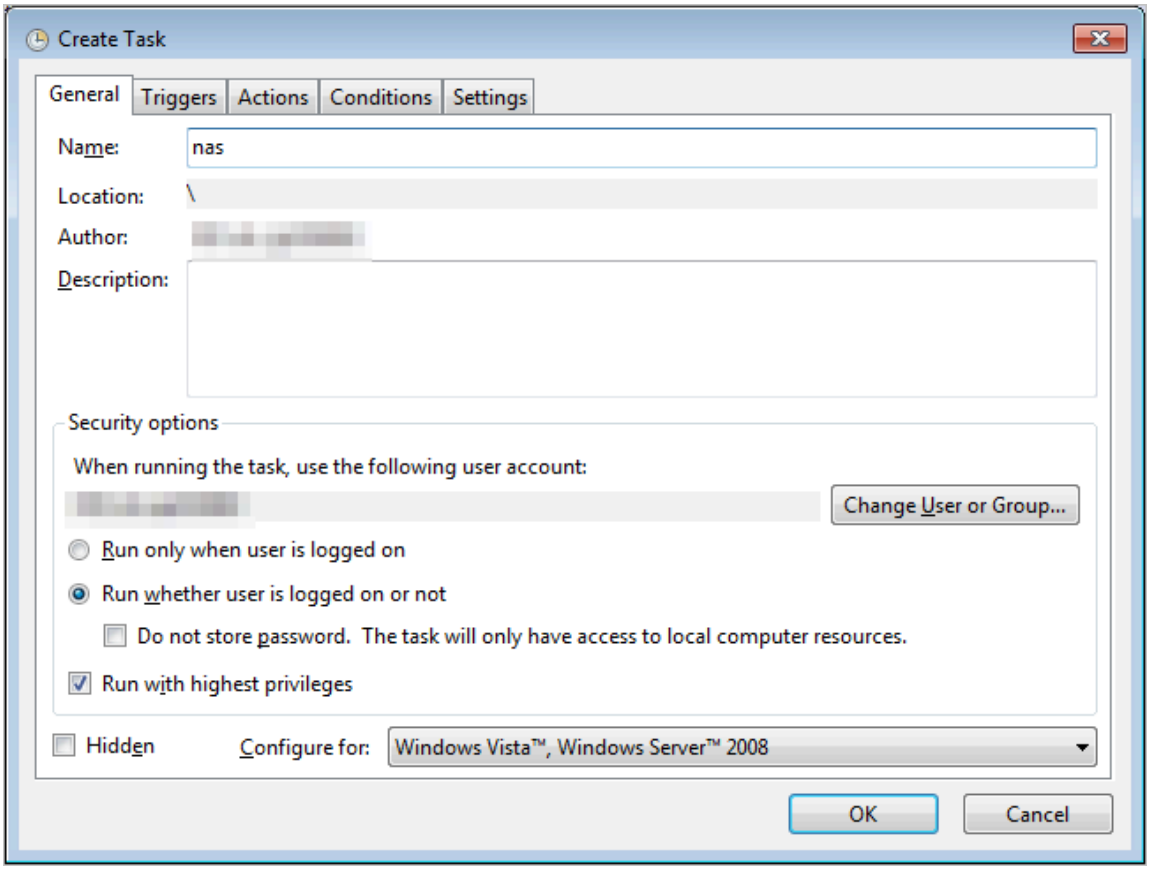
2. **Create a scheduled task.**

   a. **Open the Control Panel and choose Administrative Tools > Task Scheduler.**

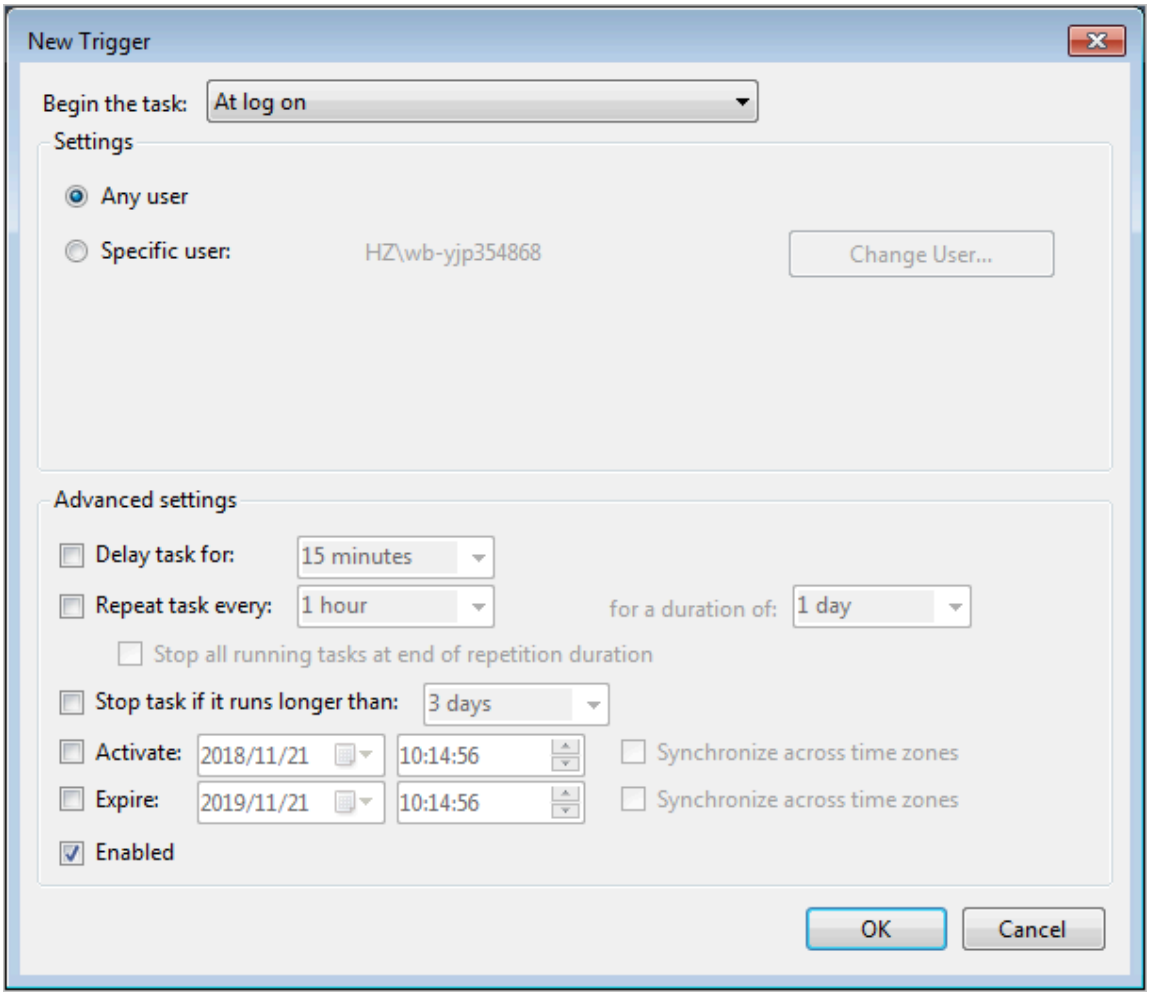
   b. **In the Task Scheduler window, choose Actions > Create Task.**



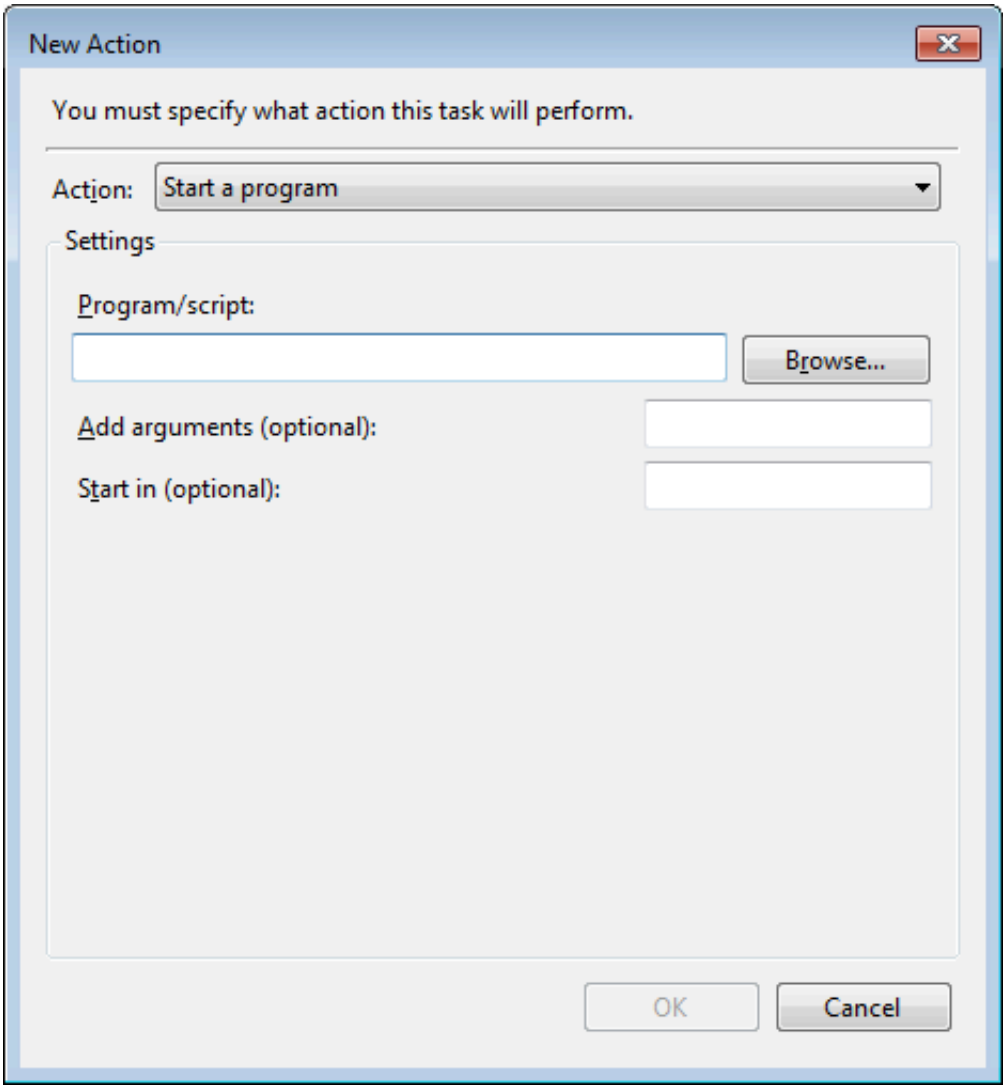
   c. **Select the General tab, enter the Name of the task, and select Run whether user is logged on or not and Run with highest privileges.**



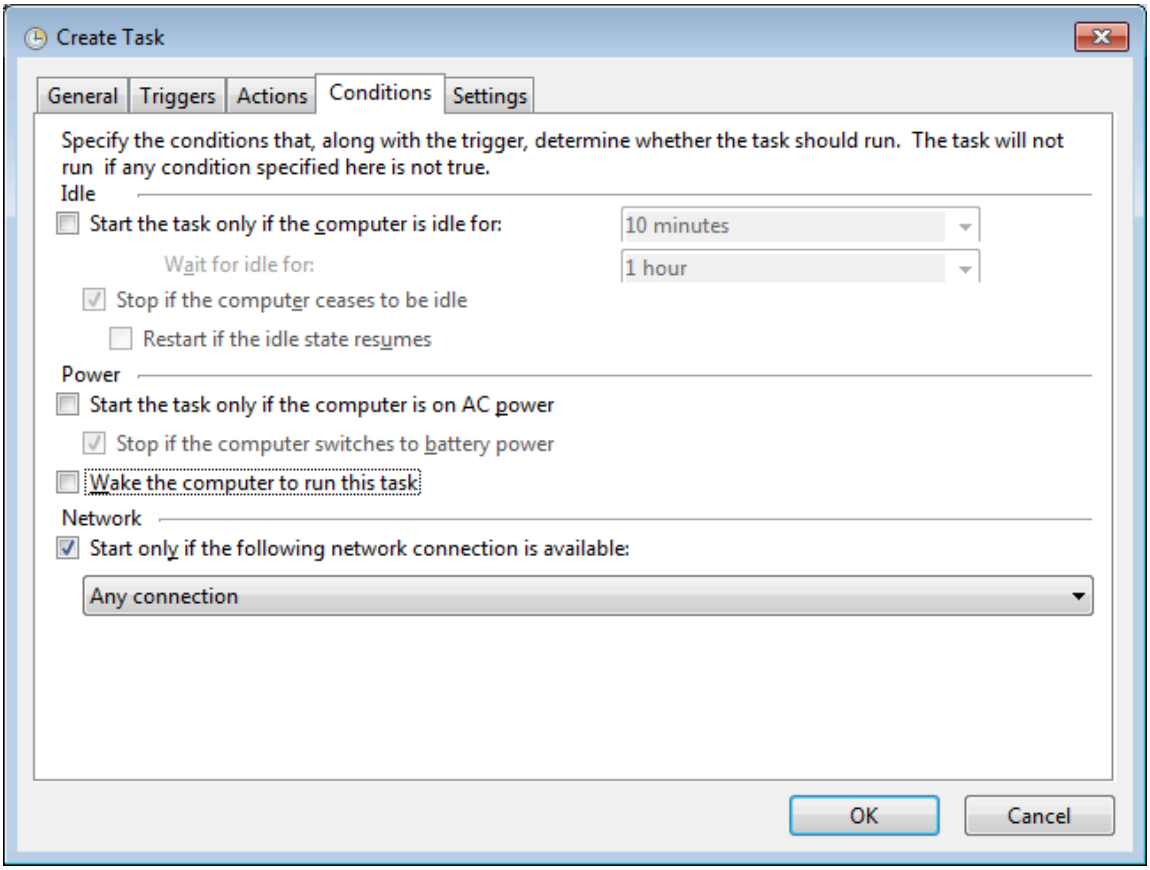
d. Select the Triggers tab, click New, select Logon in the Begin the task field, select Enabled in the Advanced Settings section, and click OK.



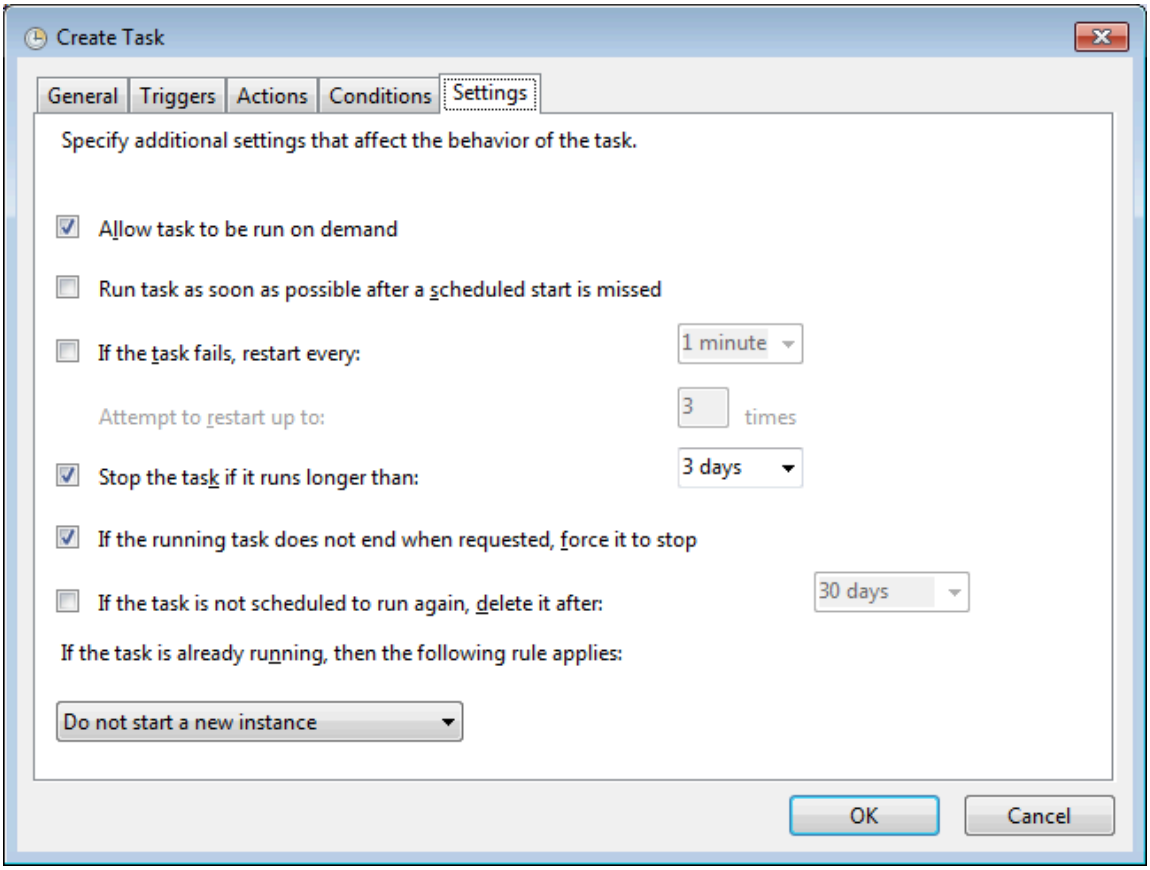
e. **Select the Actions tab, click New, select Start a program in the Action field, select the `nas_auto.bat` file in the Program/script field, and click OK.**



f. Select the Conditions tab, and select Start only if the following network connection is available. Select Any connection in the Network section.



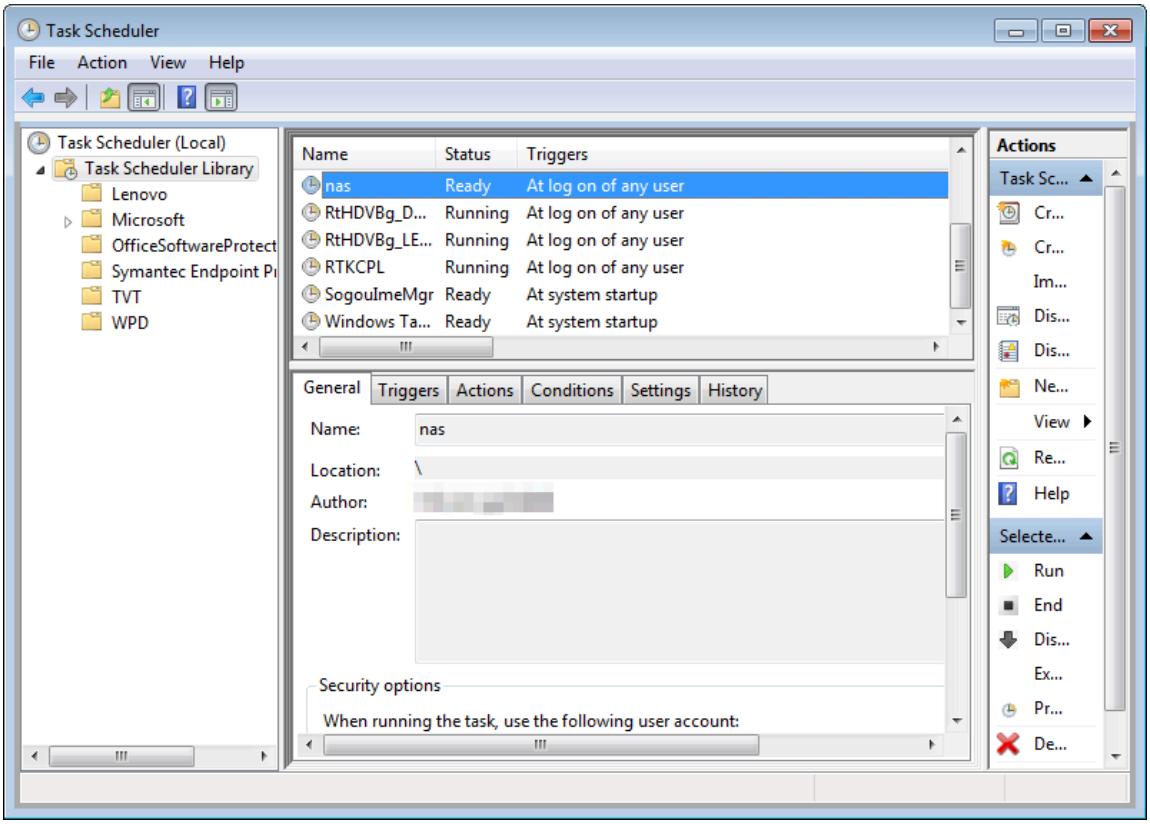
g. **Select the Settings tab, select If the running task does not end when requested, force it to stop, and select Do not start a new instance in the If the task is already running, then the following rule applies field.**



h. Click OK.

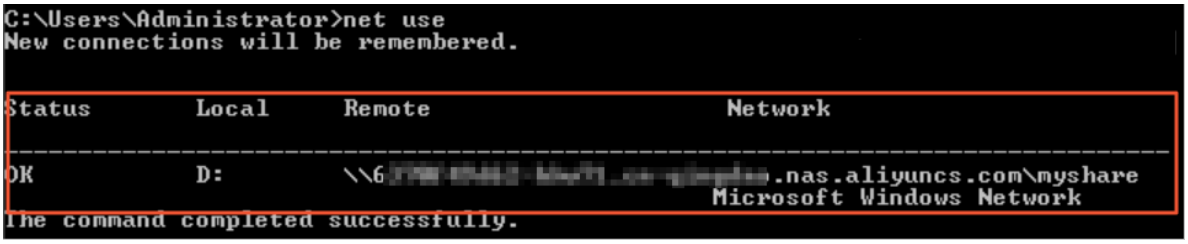
i. Restart the ECS instance to verify if the scheduled task is created.

An example of a successfully created task is shown in the following figure.



3. **Open the command prompt and run the `net use` command to verify the mount results.**

   An example of a successful mount is shown in the following figure.



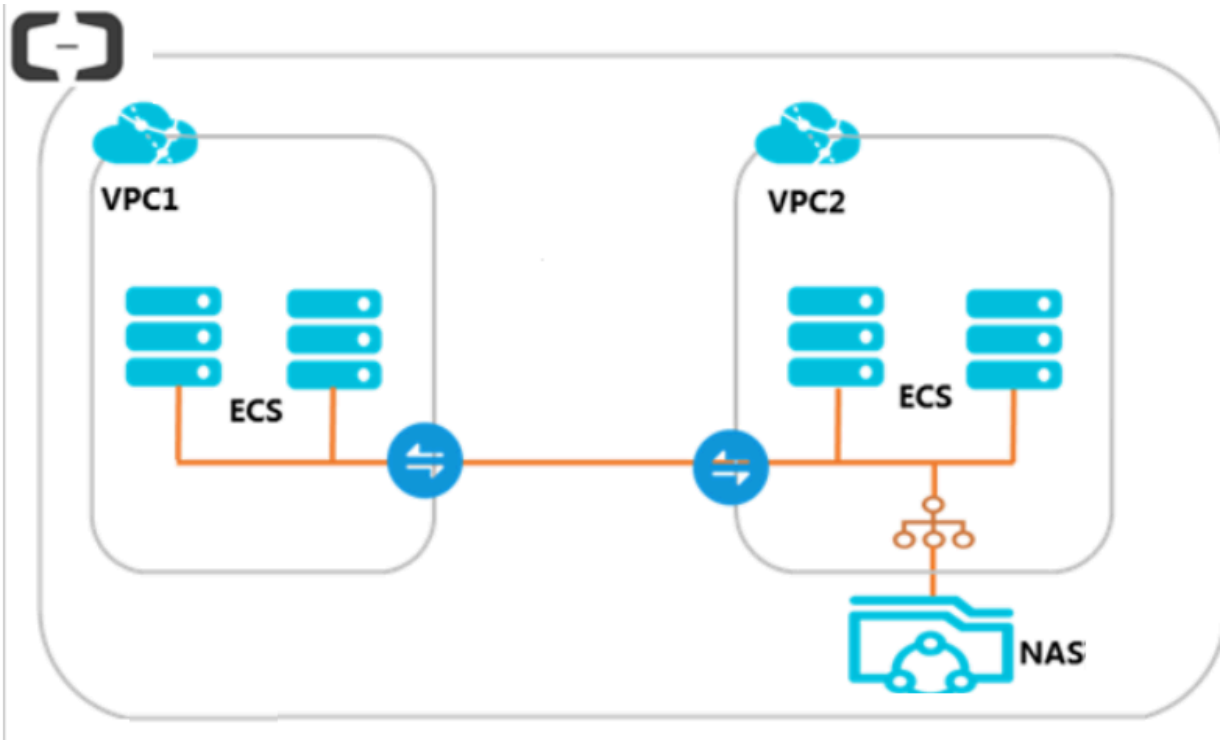
4.6 Enable a cross-VPC mount for a file system

This topic describes how to enable a cross-VPC mount for a file system.

Context

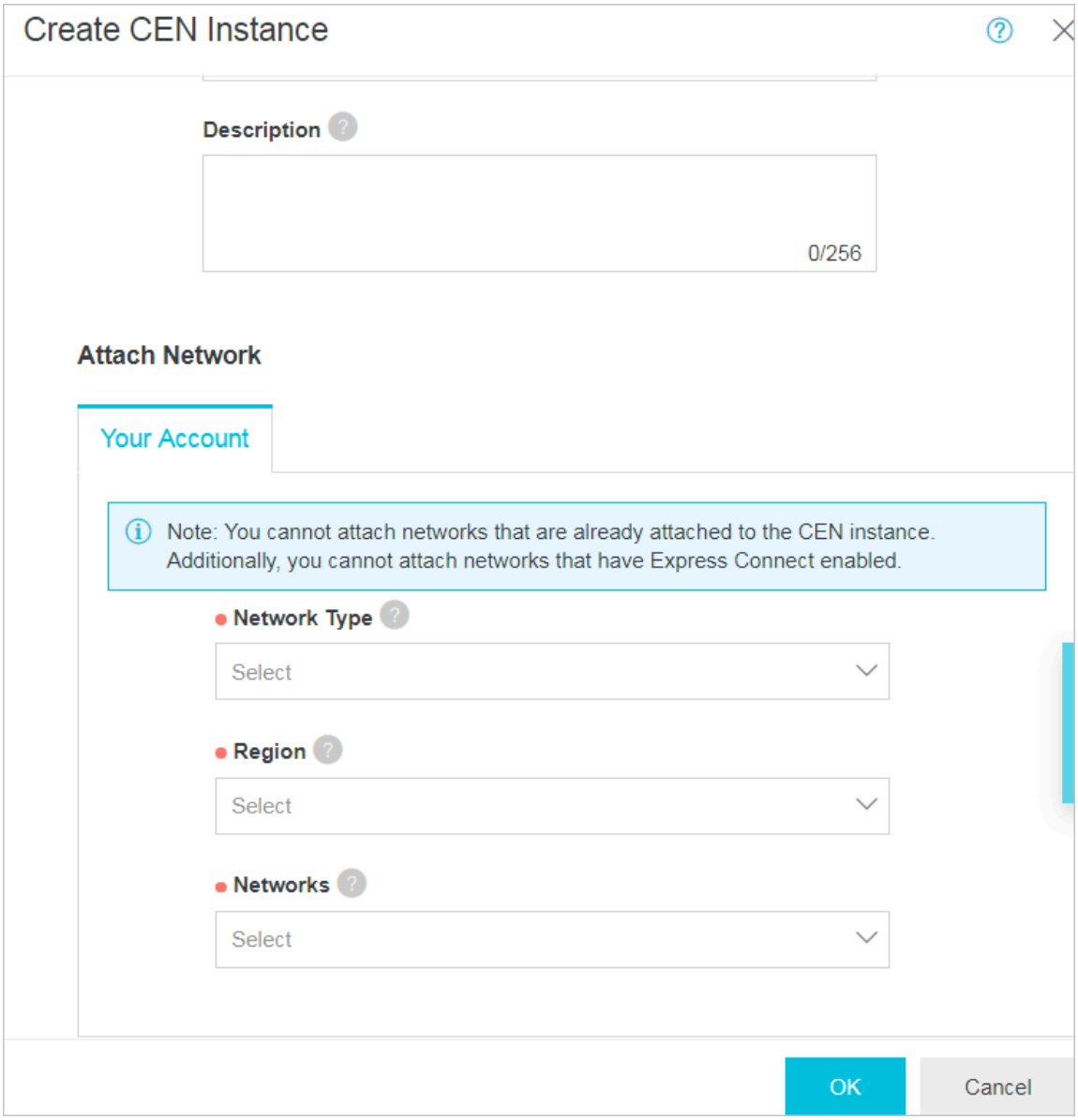
By default, you can only mount a file system on an ECS instance that is hosted by the same VPC as that of the mount target of the file system. If the mount target of the file system and the ECS instance are not in the same VPC, you can use Cloud Enterprise Network (CEN) to establish a connection between both VPCs.

You can use CEN to establish a connection between different VPCs that are located in the same region. After the connection is established, you can enable a cross-VPC mount for the file system.



Procedure

1. **Create a CEN instance.**
   a) **Log on to the** *CEN console*.
   b) **On the Instances page, click Create CEN Instance.**
   c) **Configure the CEN instance.**



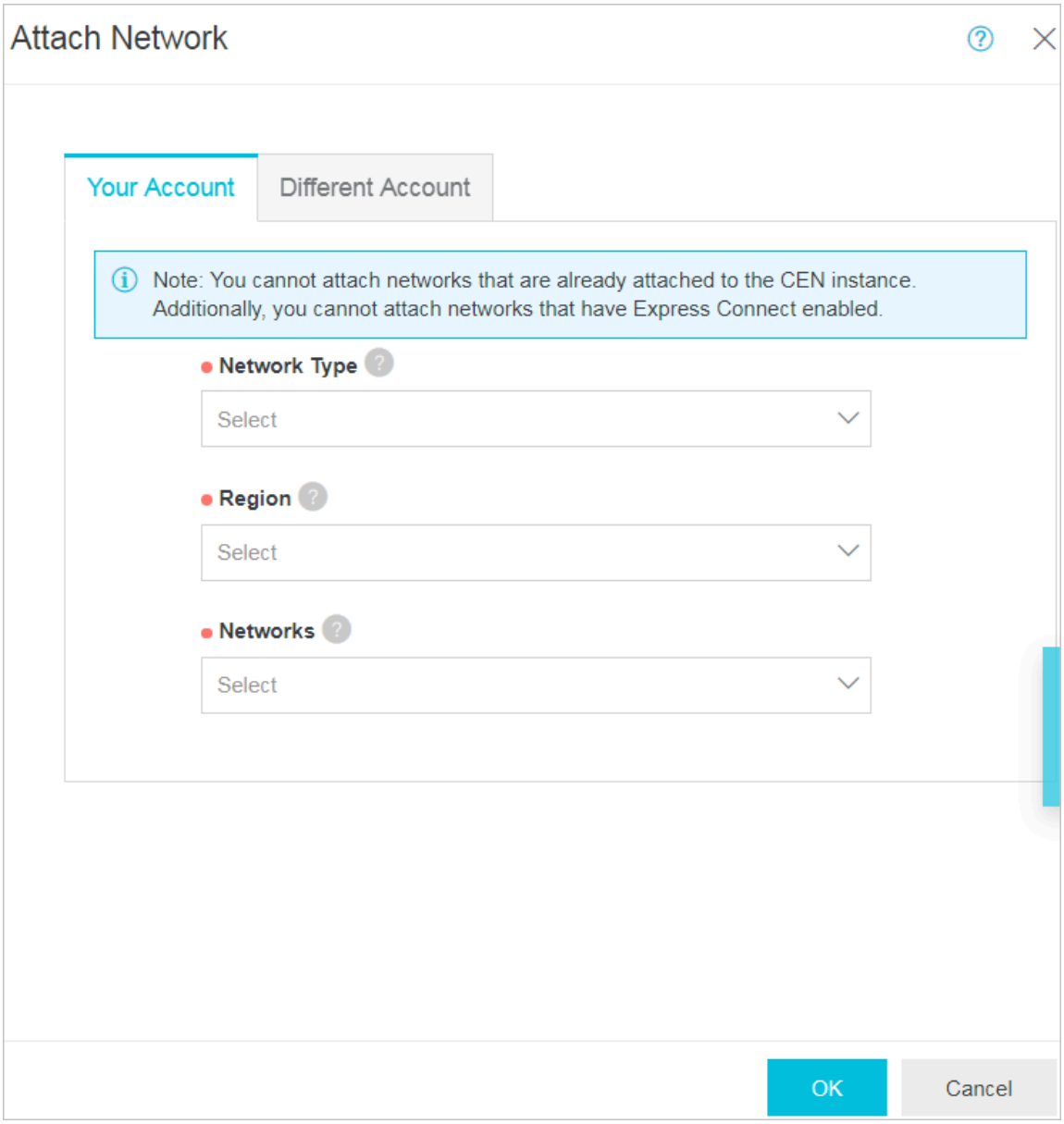
Parameter	Description
Name	The name of the CEN instance. The name must be 2 to 128 characters in length. It can start with a letter. The name can contain letters, digits, hyphens (-), and underscores (_).

Parameter	Description
Description	The description of the CEN instance. The description must be 2 to 256 characters in length and cannot start with `http://` or `https://`.
Attach Network	You can attach networks owned by the current account or a different account to a CEN instance. For more information, see *Attach networks*.

2. Attach a network.

   a) On the Instances page, find the target instance, and click Manage.

   b) On the Networks tab, click Attach Network to configure the network.



Parameter	Description
Account	Select the Your Account tab.
Network Type	The type of network you want to attach to the CEN instance. Valid values: VPC, Virtual Border Router (VBR), and Cloud Connect Network (CCN). Select VPC in this example.
Region	The region that hosts the network. Select China (Qingdao) in this example.

Parameter	Description
Networks	The name of the network you want to attach to the CEN instance. Select a virtual private cloud (VPC) in this example.

c) Repeat the preceding steps to attach another VPC to the CEN instance. In this way, you can establish a connection between two VPCs.

3. Mount a file system.

- For more information about how to mount an NFS file system on an ECS instance running Linux, see *Mount an NFS file system*.
- For more information about how to mount an SMB file system on an ECS instance running Windows, see *Mount an SMB file system*.

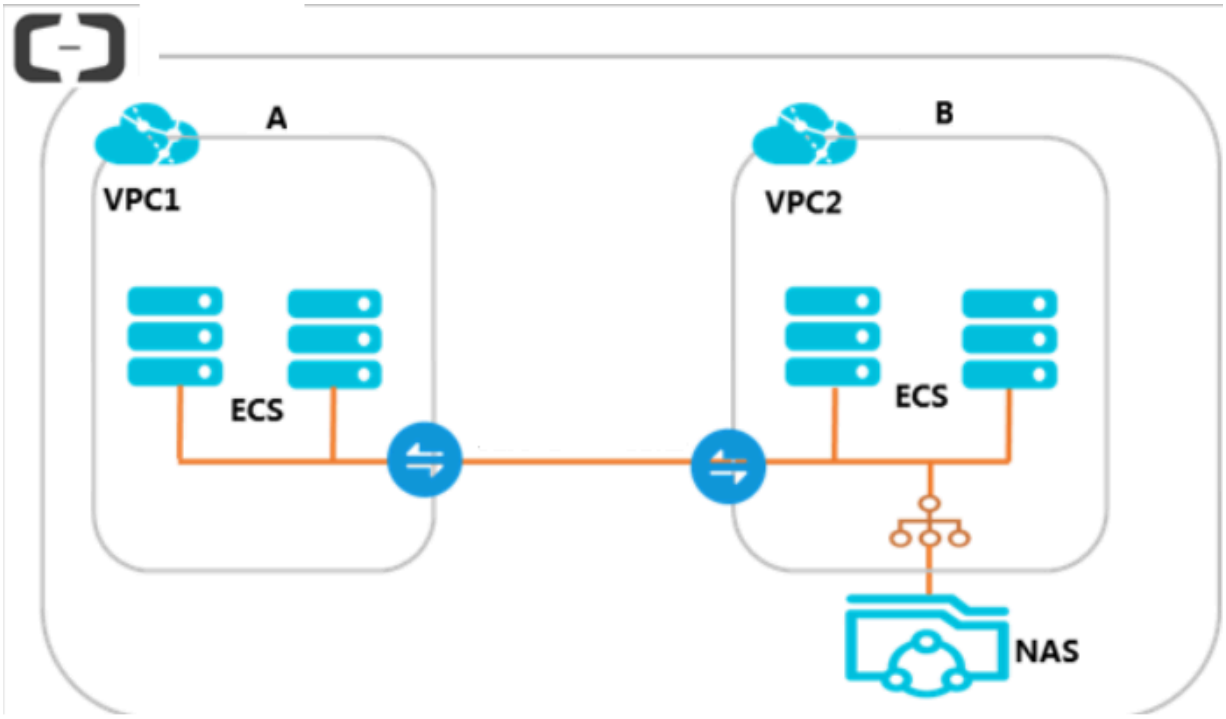
4.7 Enable a cross-account mount for a file system

This topic describes how to enable a cross-account mount for a file system.

Context

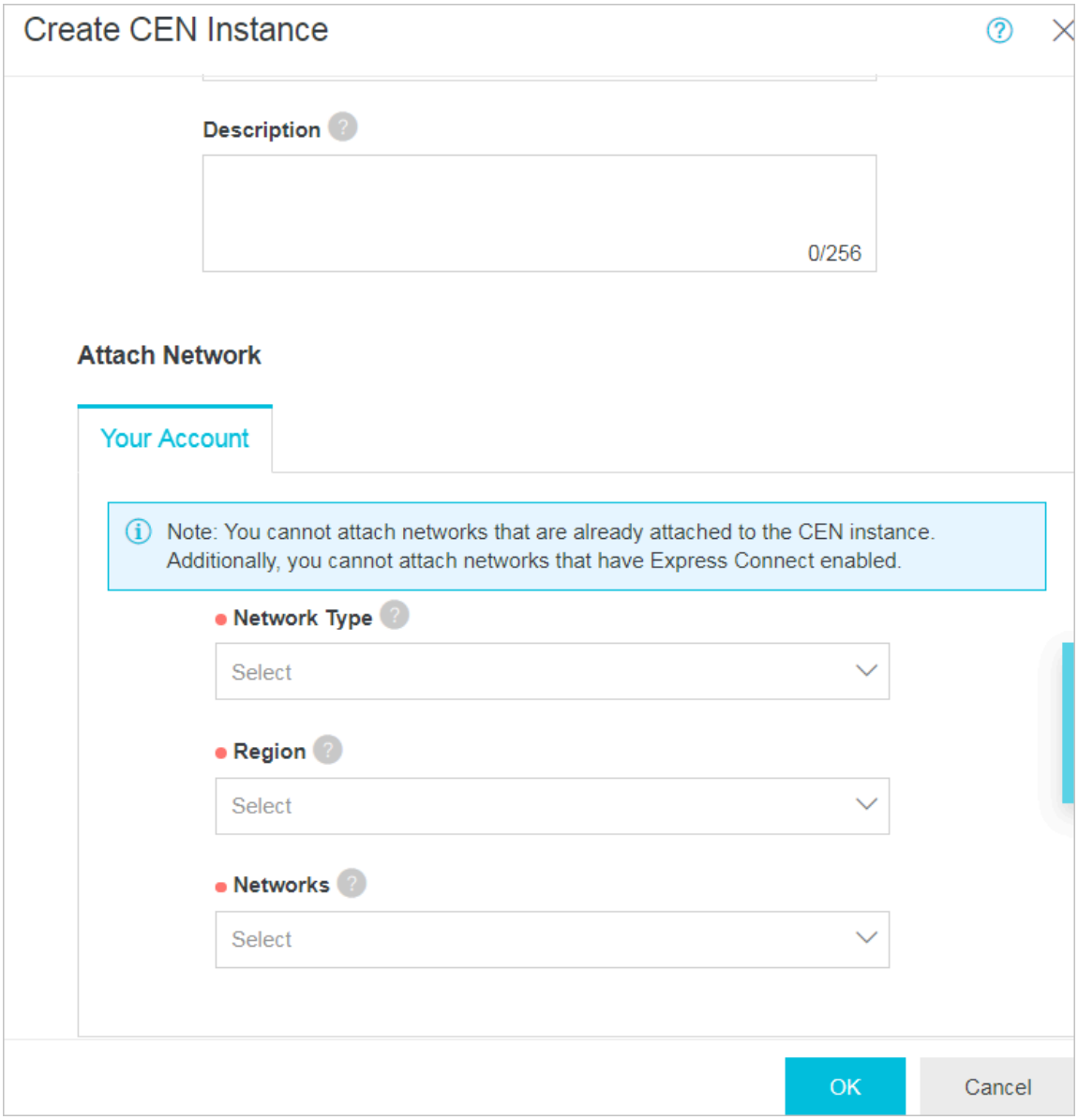
By default, you can only mount a file system on an ECS instance that is owned by the same account as that of the file system. If the ECS instance and the file system belong to different Alibaba Cloud accounts, you must establish a connection between VPCs that host the file system and the instance before the mount operation .

You can use Cloud Enterprise Network (CEN) to connect VPCs owned by different accounts. After you establish the connection, you can enable a cross-account mount for the file system.



Procedure

1. **Use Account A to create a CEN instance.**
   a) **Log on to the** *CEN console*.
   b) **On the Instances page, click Create CEN Instance.**
   c) **Configure the CEN instance.**

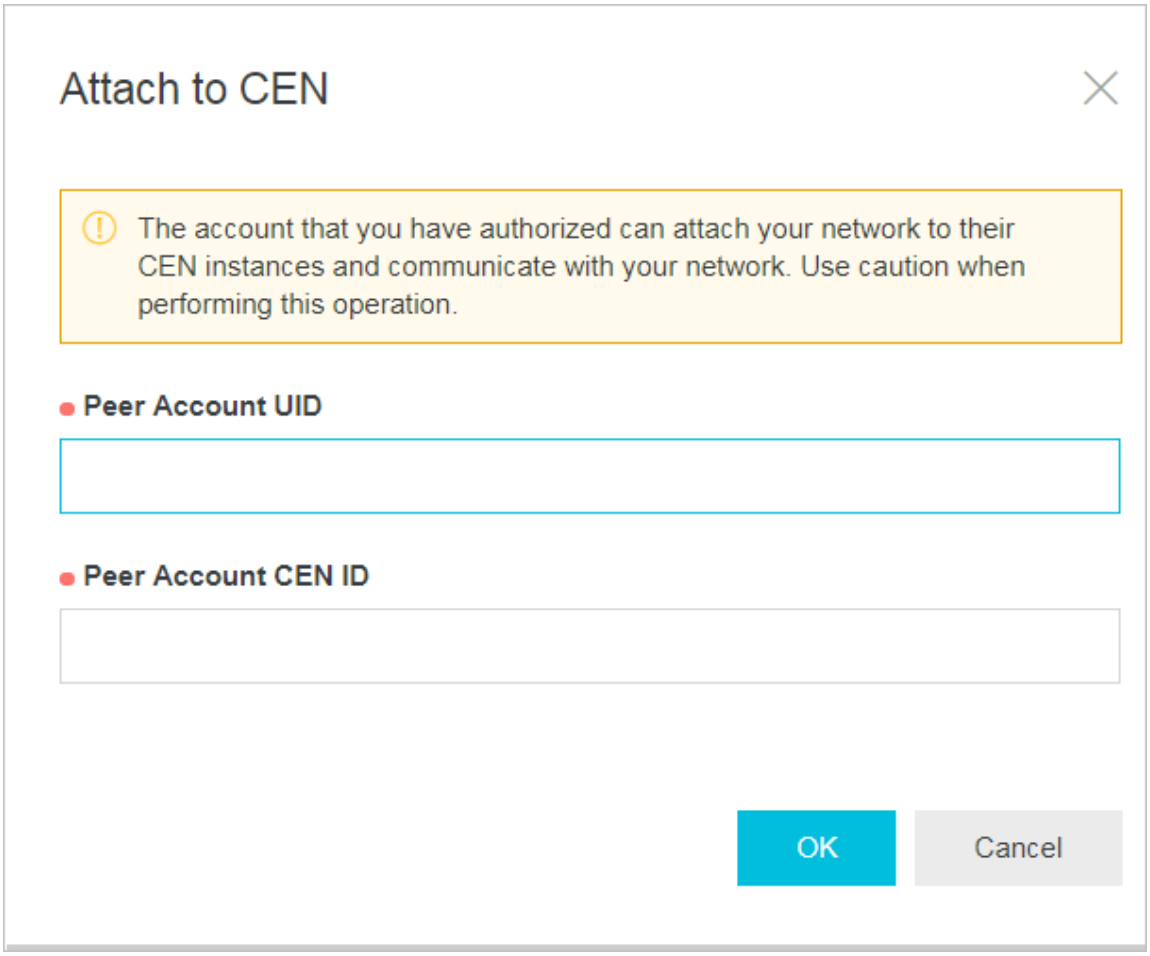


Parameter	Description
Name	The name of the CEN instance. The name must be 2 to 128 characters in length. It can start with a letter. A name can contain letters, digits, hyphens (-), and underscores (_).

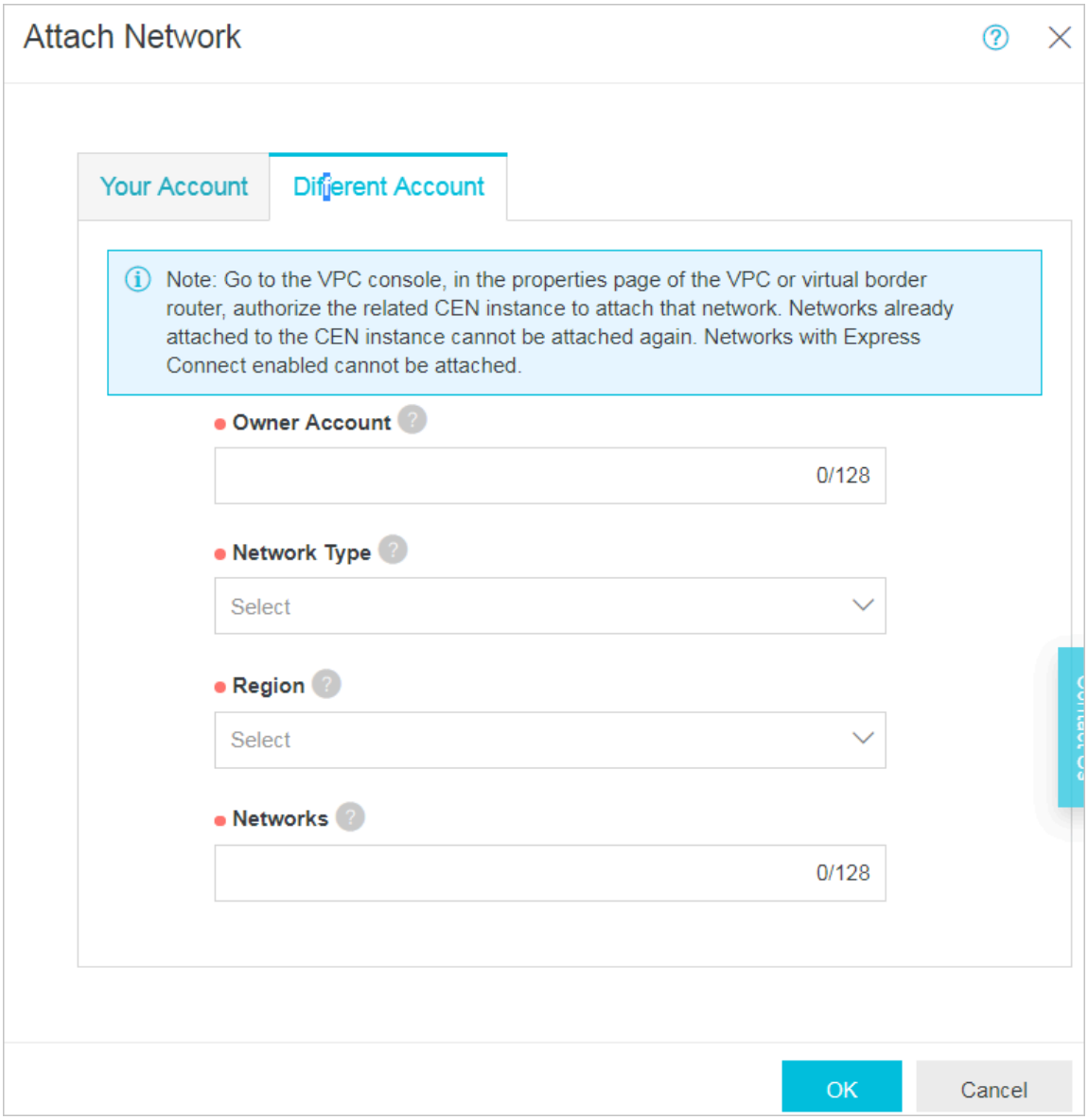
Parameter	Description
Description	The description of the CEN instance. The description must be 2 to 256 characters in length and cannot start with `http://` or `https://`.
Attach Network	You can attach networks owned by the current account or a different account to a CEN instance. For more information, see *Attach networks*.

d) Retrieve the ID of the new CEN instance, which is cbn-xxxxxxxxxx4l7 in this example.

2. **Authorize Account A to attach a network owned by Account B.**
   a) **Log on to the *VPC console* by using Account B.**
   b) **In the left-side navigation pane, select VPCs.**
   c) **Find the target VPC, and click Manage.**
   d) **On the VPC Details page, find the CEN cross account authorization information section, and click CEN Cross Account Authorization.**
   e) **In the Attach to CEN dialog box, enter the `Peer Account UID` and `Peer Account CEN ID`, and click OK.**



3. Attach a network by using Account A.
   a) Log on to the *CEN console* by using Account A.
   b) On the Instances page, find the target instance, and click Manage.
   c) On the Networks tab, click Attach Network to configure the network.



Parameter	Description
Account	Select Different Account.
Owner Account	The ID of the account that owns the target network. Enter the ID of Account B in this example.
Network Type	The type of network you want to attach to the CEN instance. Valid values: VPC, Virtual Border Router (VBR), and Cloud Connect Network (CCN). Select VPC in this example.

Parameter	Description
Region	The region that hosts the network.
Networks	The name of the network to be attached.

d) After the configuration is complete, click OK.

4. Mount a file system.

   - For more information about how to mount an NFS file system on an ECS instance running Linux, see *Mount an NFS file system*.
   - For more information about how to mount an SMB file system on an ECS instance running Windows, see *Mount an SMB file system*.

4.8 Troubleshoot mount issues

This topic describes how to troubleshoot and fix mount issues.

Mount an NFS file system on an ECS instance running Linux

- **Enable automatic troubleshooting by using a script**

  You may fail to mount an NFS file system on an ECS instance running Linux due to several different reasons. You can use the following script to troubleshoot a mount issue and find the root cause.

  1. Log on to a Linux ECS instance on which you fail to mount a file system.
  2. Use the following commands to download and run the check_alinas_nfs_mount.py script. Then, you can follow instructions provided by the script to fix mount issues.

     ```
     wget -N https://code.aliyun.com/nas_team/nas-client-tools/raw/
     master/linux_client/check_alinas_nfs_mount.py -P /tmp/
     ```

     ```
     python2.7 /tmp/check_alinas_nfs_mount.py file-system-id.region.nas
     .aliyuncs.com:/ /mnt
     ```

     In the preceding command, file-system-id.region.nas.aliyuncs.com:/ indicates the domain name of the mount target, and /mnt indicates the target mount

directory. You need to replace the domain name and the target mount directory based on your business requirements.

After all issues are resolved, a specific mount command is displayed and a prompt appears indicating that troubleshooting is complete.

> Note:
> If several questions appear when the script is running, we recommend that you log to the Alibaba Cloud console and confirm the answers. After the answer to each question is confirmed, you can click Yes or No to continue running the script and identify more issues.

3. Copy and run the mount command to enable the mount of a file system.

- More known issues

Several errors prompted by the mount command cannot be fixed by using the script. You can use the following methods to fix these errors.

- Failed to mount the subdirectory of a file system

  Error message: mount.nfs: access denied by server while mounting xxxx.nas.aliyuncs.com:/<dir>

  > Note:
  > If an error message showing "Permission denied" occurs, you can use the script to troubleshoot the issue.

  An error occurs when you attempt to mount a subdirectory of a NAS file system on an ECS instance but the subdirectory does not exist. You can first mount the root directory of the NAS file system. After the root directory is mounted, you can create a subdirectory on the NAS file system and mount the subdirectory again.

- Failed to mount a file system on two instances with duplicate names

  Error message: mount.nfs: Operation not permitted. This error occurs when you mount an NFSv4-compliant file system. However, you need to mount an NFSv3-compliant file system.

  For several kernel versions of Linux, an error may occur in the following scenario: You attempt to mount a file system on an ECS instance with the

same name as that of another ECS instance on which the file system is already mounted. You can perform the following steps to fix the issue:

1. Run the following command on the ECS instance on which you fail to mount a file system.

```
echo 'install nfs /sbin/modprobe --ignore-install nfs
nfs4_unique_id=`cat /sys/class/dmi/id/product_uuid`' >> /etc/
modprobe.d/nfs.conf
```

2. Restart the ECS instance during off-peak hours.

   You can also unmount all available NFS file systems and use the `rmmod` command to uninstall the nfsv4 and nfs kernel modules.

3. Re-mount the NFS file system.

Mount an SMB file system on an ECS instance running Windows

- Enable automatic troubleshooting by using a script

  You may fail to mount an SMB file system on an ECS instance running Windows due to several different reasons. You can use the following script to troubleshoot a mount issue and find the root cause.

  1. Log on to a Windows ECS instance on which you fail to mount a file system.
  2. Use the following commands to download and run the check_alinas_nfs_mount.py script. Then, you can follow instructions provided by the script to fix mount issues.

```
wget https://code.aliyun.com/nas_team/nas-client-tools/raw/master
/windows_client/alinas_smb_windows_inspection.ps1 -OutFile
alinas_smb_windows_inspection.ps1
```

```
.\alinas_smb_windows_inspection.ps1 -MountAddress abcde-123.region
-id.nas.aliyuncs.com -Locale zh-CN
```

  In the preceding command, abcde-123.region-id.nas.aliyuncs.com indicates the domain name of the mount target. You need to replace the domain name with a different domain name that is specific to your environment.

- More known issues

  For more information about issues that occur when you mount a file system on a Windows instance, see *#unique_25*. You can find the corresponding solution to each error code.

5 Unmount a file system

5.1 Unmount a file system from an ECS instance running Linux

This topic describes how to unmount a file system from an ECS instance running Linux.

Procedure

1. **Log on to the *ECS console*.**
2. **Run the `umount /mnt` command to unmount an NFS file system.**

   You need to replace the /mnt directory with a directory specific to your environment.

   The format of the unmount command is `umount /<the directory of a mount point>`.

   Note:

   We recommend that you do not specify any other umount parameters or change their default values.

   When you unmount a file system, an error indicating that the device is busy may occur. In this case, run the kill command to terminate the processes that are accessing the file system.

   a. Install fuser.

   - **fuser is preinstalled in CentOS, RHEL, and Aliyun Linux. You do not need to reinstall fuser on these systems.**
   - **For Ubuntu or Debian, run the `apt install -y fuser` command to install the tool.**

   b. Run the `fuser -mv <the directory of a mount point>` command to view the process ID of each process that is accessing the Apsara File Storage NAS file system.

   c. Run the `kill <pid>` command to terminate a process.

3. Run the `mount -l` command to view the unmount result.

   If an Apsara File Storage NAS file system is not displayed in the unmount result, it indicates that the file system is unmounted.

5.2 Unmount a file system from an ECS instance running Windows

This topic describes how to unmount an SMB file system from an ECS instance running Windows.

Procedure

1. Log on to the *ECS console*.
2. Open the command prompt and run the following command to unmount a file system.

   ```
   net use D: /delete
   ```

   In the preceding command, replace the drive letter D: with a drive letter specific to your environment. You can run the `net use` command to retrieve the drive letter of a mount point.

   Note:

   - You can run the `net use * /delete` command to unmount each available file system one by one in Windows.
   - You can run the `net use * /delete /y` command to unmount all the available file systems without any confirmation in Windows.

3. You can run the `net use` command to view the unmount results.

   If an SMB file system is not displayed in the results, it indicates that the file system is unmounted.

6 Mount a file system to a Container Service for Kubeneters cluster

6.1 Recommended mount types

This topic describes recommended mount types for mounting Apsara File Storage NAS file systems on Kubernetes clusters.

Recommended storage drivers

We recommend that you use the Alibaba Cloud FlexVolume storage driver. This type of storage driver supports multiple data stores, such as Apsara File Storage NAS, Cloud Paralleled File System (CPFS), Object Storage Service (OSS), and Block Storage. It provides you with flexible and diverse configuration parameters, improves user experience, and reduce the complexity of operations and maintenance.

Regardless of Container Service or user-created Kubernetes clusters that you are using, we recommend that you use Alibaba Cloud FlexVolume storage drivers to manage file systems.

You can perform the following steps to install an Alibaba Cloud FlexVolume driver.

- **If you are using Container Service and want to create a cluster, an Alibaba Cloud FlexVolume driver is installed by default. You only need to confirm that the driver version is v1.12.6.52-f6604e5-aliyun or later. If the driver version is earlier than v1.12.6.52-f6604e5-aliyun, we recommend that you update the driver version. For more information, see** *Update Alibaba Cloud FlexVolume drivers*.
- **If you are using user-created Kubernetes clusters, we recommend that you first install an Alibaba Cloud FlexVolume driver. For more information, see** *Install an Alibaba Cloud FlexVolume storage driver*.

Recommended mount types

In terms of flexibility and complexity of operations and maintenance, we recommend that you use persistent volumes (PVs) or persistent volume claims (PVCs) to mount file systems rather than volumes.

- **For more information about static volumes, see** *Mount a static persistent volume through flexVolume*
- **For more information about dynamic volumes, see** *Mount a dynamic persistent volume to access Apsara File Storage NAS through flexVolume*

Not recommended mount types

We recommend that you use persistent volumes (PVs) or persistent volume claims (PVCs) to mount file systems and avoid using volumes. In some scenarios, you must use volumes to mount file systems. In such cases, you can only use Alibaba Cloud FlexVolume storage drivers to mount file systems rather than Kubernetes-native NFS drivers.

6.2 Mount a static persistent volume through flexVolume

This topic describes how to mount a volume, a static persistent volume (PV), or a static persistent volume claim (PVC) to access an Apsara File Storage NAS file system from a Container Service for Kubernetes cluster by using the flexVolume driver.

Prerequisites

1. **You have created a Kubernetes cluster. For more information, see** *#unique_36*.

   If your cluster is a self-built cluster, download and install *Alibaba Cloud flexVolume driver*.
2. **You have created a file system. For more information, see** *Create file systems*.

   The file system you have created and your Kubernetes cluster must be in the same zone.
3. **You have added a mount point. For more information, see** *Add a mount target*.

   The mount point and the Kubernetes cluster must be in the same Virtual Private Cloud (VPC) network.

Context

With the flexVolume driver provided by Alibaba Cloud, you can access Apsara File Storage NAS file systems by using the following methods:

- **Mount a volume**
- **Mount a static PV and PVC**

Mount a volume

Use a nas-deploy.yaml file to create pods.

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: nas-static
  labels:
    app: nginx
spec:
  replicas: 1
  selector:
    matchLabels:
      app: nginx
  template:
    metadata:
      labels:
        app: nginx
    spec:
      containers:
      - name: nginx
        image: nginx
        ports:
        - containerPort: 80
        volumeMounts:
          - name: nas1
            mountPath: "/data"
      volumes:
      - name: "nas1"
        flexVolume:
          driver: "alicloud/nas"
          options:
            server: "0cd8b4a576-grs79.cn-hangzhou.nas.aliyuncs.com"
            path: "/k8s"
            vers: "3"
            options: "nolock,tcp,noresvport"
```

Table 6-1: Parameters

Parameter	Description
server	The mount point of your Apsara File Storage NAS file system.
path	The mounted directory in your Apsara File Storage NAS file system. You can mount a sub-directory as a volume. If no sub-directory exists in the Apsara File Storage NAS file system, the system automatically creates and then mounts a sub-directory.
vers	The version number of Network File System (NFS) mount protocol. Version 3 and version 4.0 are supported. The recommended and default version is version 3.

Parameter	Description
mode	The access permission to the mounted directory. **Note:** · You cannot configure the mode parameter if the root directory is mounted. · If the Apsara File Storage NAS file system stores a large amount of data, the process of mounting the volume may require a long period of time or fail. In this case, we recommend that you do not configure the `mode` parameter.
options	The options for mounting the Apsara File Storage NAS file system. If you do not configure the parameter, the default value is `nolock,tcp,noresvport` for the V3 protocol, and `noresvport` for the V4.0 protocol.

Mount a static PV and PVC

1. Create a PV.

   You can create a PV by using a YAML file or in the Alibaba Cloud Container Service console.

   · Use a nas-pv.yaml file to create a PV.

```
apiVersion: v1
kind: PersistentVolume
metadata:
  name: pv-nas
spec:
  capacity:
    storage: 5Gi
  storageClassName: nas
  accessModes:
    - ReadWriteMany
  flexVolume:
    driver: "alicloud/nas"
    options:
      server: "0cd8b4a576-uih75.cn-hangzhou.nas.aliyuncs.com"
      path: "/k8s"
      vers: "3"
```

```
        options: "nolock,tcp,noresvport"
```

For more information about specific parameters, see *Table 6-1: Parameters*.

- Use the Alibaba Cloud Container Service console to create a PV:

  a. Log on to the *Container Service console*.

  b. Choose Container Service-Kubernetes > Clusters > Persistent Volumes. Select the target cluster and click Create.

  c. In the Create PV dialog box, set related parameters.

Parameter	Description
PV Type	Select NAS.
Volume Name	The name of the PV. It must be unique in the cluster. In this example, use pv-nas as the name.
Capacity	The capacity of the PV. Note: The capacity of the PV cannot exceed the disk capacity.
Access Mode	The access mode is ReadWriteMany by default.
Mount Point Domain Name	The mount point of the Apsara File Storage NAS file system. You can set this parameter based on your business requirements following the example of file-system-id.region.nas.aliyuncs.com.
Subpath	The sub-directory of the Apsara File Storage NAS file system. It must start with a forward slash (/). After the PV is created, the specified sub-directory is mounted as the PV. - If no sub-directory exists in the root directory of an Apsara File Storage NAS file system, the system automatically creates a sub-directory. - You do not need to specify this parameter. By default, the root directory of the NAS file system is mounted.

Parameter	Description
Permissions	The access permission to the mounted directory. For example, you can set this parameter to 755, 644, or 777. - The permission can only be set when a sub-directory is mounted as the PV. - You do not need to specify this parameter. The default permission is the original permission of the Apsara File Storage NAS file system. - If the Apsara File Storage NAS file system stores a large amount of data, the process of mounting the volume may require a long period of time or fail. In this case, we recommend that you do not configure this parameter.
Version	The version number of Network File System (NFS) mount protocol. Version 3 and version 4.0 are supported. The recommended and default version is version 3.
Label	The label of the PV.

d. After you complete the parameter configurations, click Create.

2. Use a nas-pvc.yaml file to create a PVC:

```
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: pvc-nas
spec:
  accessModes:
    - ReadWriteMany
  storageClassName: nas
  resources:
    requests:
      storage: 5Gi
```

3. Use a nas-pod.yaml file to create pods as follows:

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: nas-static
  labels:
    app: nginx
spec:
  replicas: 1
  selector:
    matchLabels:
      app: nginx
  template:
    metadata:
      labels:
```

```
        app: nginx
    spec:
      containers:
      - name: nginx
        image: nginx
        ports:
        - containerPort: 80
        volumeMounts:
          - name: pvc-nas
            mountPath: "/data"
      volumes:
        - name: pvc-nas
          persistentVolumeClaim:
            claimName: pvc-nas
```

6.3 Mount a dynamic persistent volume to access Apsara File Storage NAS through flexVolume

This topic describes how to mount a dynamic persistent volume (PV) to access an Apsara File Storage NAS file system from a Container Service for Kubernetes cluster by using the flexVolume driver.

Prerequisites

1. **You have created a Kubernetes cluster in Alibaba Cloud. For more information, see** *#unique_36*.

   If your cluster is a self-built Kubernetes cluster, download and install *Alibaba Cloud flexVolume driver*.

2. **You have created a file system. For more information, see** *Create file systems*.

   The file system and the Kubernetes cluster must be in the same zone.

3. **You have added a mount point. For more information, see** *Add a mount target*.

   The mount point and the Kubernetes cluster must be in the same Virtual Private Cloud (VPC) network.

Context

A dynamic PV is dynamically provisioned based on the mapping from a sub-directory in an Apsara File Storage NAS file system.

> **Note:**
> **When you use dynamic provisioning, a directory is automatically created in an existing NAS file system and mounted as the target volume.**

Install the NAS controller

Configure a deployment named alicloud-nas-controller by using the following template.

```
kind: Deployment
apiVersion: extensions/v1beta1
metadata:
  name: alicloud-nas-controller
  namespace: kube-system
spec:
  strategy:
    type: Recreate
  template:
    metadata:
      labels:
        app: alicloud-nas-controller
    spec:
      tolerations:
      - operator: "Exists"
      affinity:
        nodeAffinity:
          preferredDuringSchedulingIgnoredDuringExecution:
          - weight: 1
            preference:
              matchExpressions:
              - key: node-role.kubernetes.io/master
                operator: Exists
      priorityClassName: system-node-critical
      serviceAccount: admin
      hostNetwork: true
      containers:
        - name: nfs-provisioner
          image: registry.cn-hangzhou.aliyuncs.com/acs/alicloud-nas-
controller:v1.14.3.8-58bf821-aliyun
          env:
          - name: PROVISIONER_NAME
            value: alicloud/nas
          securityContext:
            privileged: true
          volumeMounts:
          - mountPath: /var/log
            name: log
      volumes:
      - hostPath:
          path: /var/log
        name: log
```

Mount a dynamic PV

1. **Configure StorageClass.**

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: alicloud-nas
mountOptions:
- nolock,tcp,noresvport
- vers=3
parameters:
```

```
  server: "23a9649583-iaq37.cn-shenzhen.nas.aliyuncs.com:/nasroot1/"
  driver: flexvolume
provisioner: alicloud/nas
reclaimPolicy: Delete
```

Parameter	Description
mountOptions	**The options used for mounting the PV.**
server	**The mount points used for mounting the PV,** · **in the** `nfsurl1:/path1, nfsurl2:/path2` **format.** · **If multiple servers are specified, the PV provisioned through StorageClass will poll these servers to select a mount point.**
driver	**The driver used for access to an Apsara File Storage NAS file system. Valid values: flexvolume and nfs. Default value: nfs .**
reclaimPolicy	**The reclaim policy for a PV. We recommend that you set this parameter to Retain.** **If you set this parameter to** `Delete`**, the name of the directory in the Apsara File Storage NAS file system corresponding to the PV will automatically be changed when you delete a PV. For example, path-name will be changed to archived-path-name. If you want to delete the directory in the file system corresponding to the PV, set** `archiveOnDelete` **to** `false` **in Storage Class.**

2. **Access the dynamic PV.**

```
apiVersion: v1
kind: Service
metadata:
  name: nginx
  labels:
    app: nginx
spec:
  ports:
  - port: 80
    name: web
  clusterIP: None
  selector:
    app: nginx
---
apiVersion: apps/v1beta1
kind: StatefulSet
metadata:
  name: web
spec:
  serviceName: "nginx"
```

```
  replicas: 5
  volumeClaimTemplates:
  - metadata:
      name: html
    spec:
      accessModes:
        - ReadWriteOnce
      storageClassName: alicloud-nas
      resources:
        requests:
          storage: 2Gi
  template:
    metadata:
      labels:
        app: nginx
    spec:
      containers:
      - name: nginx
        image: nginx:alpine
        volumeMounts:
        - mountPath: "/data"
          name: html
```