

Alibaba Cloud Apsara File Storage NAS

Console User Guide

Issue: 20190819

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 information, 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.
<code>Courier font</code>	It is used for commands.	Run the <code>cd / d C :/ windows</code> command to enter the Windows system folder.
<i>Italics</i>	It is used for parameters and variables.	<code>bae log list --instanceid Instance_ID</code>
[] or [a b]	It indicates that it is an optional value, and only one item can be selected.	<code>ipconfig [-all -t]</code>

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

Contents

Legal disclaimer.....	I
Generic conventions.....	I
1 Manage permissions.....	1
1.1 Access control for RAM users.....	1
1.2 Create a custom policy.....	3
1.3 Manage permission groups.....	5
2 Manage file systems.....	11
3 Manage mount points.....	14
4 Mount a file system.....	17
4.1 Precautions.....	17
4.2 Mount an NFS file system.....	18
4.3 Mount an SMB file system.....	21
4.4 Enable an automatic mount at startup for an NFS file system.....	25
4.5 Enable an automatic mount at startup for an SMB file system.....	29
4.6 Enable a cross-VPC mount for a file system.....	34
4.7 Enable a cross-account mount for a file system.....	38
5 Unmount a file system.....	44
5.1 Unmount a file system from an ECS instance running Linux.....	44
5.2 Unmount a file system from an ECS instance running Windows.....	45

1 Manage permissions

1.1 Access control for RAM users

Resource Access Management (RAM) enables you to manage user access to Alibaba Cloud resources. You can reduce risks to your Alibaba Cloud accounts by creating RAM user accounts and managing their permissions.

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 data security risks for your enterprise.

Create a RAM user account

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 required settings.
4. Select Console Password Logon and Programmatic Access in the Access Mode field.
5. Select Custom Logon Password in the Console Password field, enter a password, and select Required at Next Logon in the Password Reset field.
6. (Optional) Select Required to Enable MFA in the Multi-factor Authentication field and click OK.
7. Save the new account, password, AccessKey ID, and AccessKey Secret.



Note:

We recommend that you save the AccessKey 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 the 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 before using the user or group to manage resources by using the console or API operations. The following steps take a RAM user account as an example to grant permissions.

The following NAS policies are provided. You can grant one of the following policies to a RAM user account as required.

- **AliyunNASFullAccess:** grants a RAM user account full access to NAS.
- **AliyunNASReadOnlyAccess:** grants a RAM user account read-only access to NAS.



Note:

As only coarse-grained policies are provided in system policies, you can create fine-grained custom policies to meet your business requirements. For more information, see [#unique_5](#).

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.

Add Permissions

Principal

test@████████████████████.onaliyun.com ×

Select Policy

System Policy ▾

AliyunNASFullAccess × 🔍

Policy Name	Note
AliyunNASFullAccess	Provides full access to Network Attached Storage via Management Console.

Selected (1)

Clear

AliyunNASFullAccess ×

Ok

Cancel

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 provide you with fine-grained permissions to meet your actual business requirements. These policies make it easier and more flexible to adapt and manage permissions.

S

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 NAS resources. For more information, see [../SP_65/DNRAM11885314/EN-US_TP_23770.dita#concept_sr_q_fb_k_xdb](#).

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

```
}
```

API operations that you can call to manage NAS file systems are listed in the following table.

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

The NAS resources that are accessible by clients are listed in the following table.

Resource	Description
*	Indicates all 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.

Add Permissions

Principal

test@163.com onaliyun.com

Select Policy

Custom Policy

NASReadOnlyAccess

Selected (1)

Clear

Policy Name	Note
NASReadOnlyAccess	NASReadOnlyAccess

NASReadOnlyAccess

Ok

Cancel

1.3 Manage permission groups

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

Context

A permission group is a whitelist 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 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 a maximum of 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.

- Choose **NAS > Permission Group** and click **Create Permission Group**.
- In the **Create Permission Group** dialog box, configure the required settings.

Create Permission Group

* Region :

China East 1 (Hangzhou) ▼

* Name :

test_01

The group name is a string of 3 to 64 characters including English letters, numbers, underscores (_) or hyphens (-).

* Network type :

VPC ▼

Description :

Must begin with a large or small letter or Chinese, and cannot begin with http:// and https://. can contain Numbers, semicolons (:), underscores (_), or hyphens (-).The length may be 2-128characters.

OK

Cancel

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

3. Add a rule.

- a) Locate the target permission group and click Manage.
- b) On the Permission Group Rules page, click Add Rule.
- c) Configure the required settings.

Add Rule

*

 Authorization Address :

192.168.3.0/24

Virtual machine VPC IP address; a single IP address or a single IP segment is allowed, such as 10.10.1.123 or 192.168.3.0/24

*

 Read/Write Permissions :

Read-only

*

 User Permission :

Do not limit root users (no_squasl

*

 Priority :

1

The scope of the priority value is 1-100, with a default value of 1, or top priority

OK

Cancel

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

Name	Description
User Permission	<p>Indicates whether to limit a Linux user's access to a file system.</p> <p>When a Linux user attempts to access the files or directories of a file system, the specified user permission is checked.</p> <ul style="list-style-type: none"> · 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.
Priority	<p>When an authorized object matches multiple rules, the rule with the highest priority takes effect.</p> <p>1 to 100, in which 1 is the highest priority.</p>

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	Locate the target permission group and click Edit to modify the description of the permission group.
Delete a permission	Locate the target permission group and click Delete to delete the permission group.

Action	Description
View the list of rules	Locate the target permission group and click Manage to view the list of rules in the permission group.
Modify a rule	Click Manage, locate the target rule, and click Edit to modify fields including the Authorization Address, Read/Write Permissions, User Permission, and Priority.
Delete a rule	Click Manage, locate the target rule, and click Delete to delete the rule.

2 Manage file systems

This topic describes how to manage file systems in the Network Attached Storage (NAS) console. The management includes creating and deleting file systems. It also includes viewing a list of file systems and the 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.

Create File System

* Region :

China East 2 (Shanghai) ▼

File systems and computing nodes in different regions are not connected.

* Storage Type :

SSD performance-type ▼

* Protocol Type :

NFS (including NFSv3 and NFSv4) ▼

NFS is recommended in Linux and SMB is recommended in Windows

* Zone :

China East 2 Zone B ▼

File systems and computing nodes in different zones in the same region are connected.

Storage Package :

Default No Package ▼

Bind an unused storage package

OK

Cancel


Name	Description
Region	

Name	Description
Storage Type	
Protocol Type	<p>Valid values: NFS (including NFSv3 and NFSv4) and SMB (2.1 and later).</p> <p>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.</p>
Zone	
Storage Package	

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, locate the target file system and click Edit to modify the name of the file system.

File System ID/Name	Storage Type	Protocol Type	Storage Capacity	Zone	Time Created 	Bound Storage Package	Number of Mount Points	Action
<div><div><div>fs-123456789</div><div>fs-123456789</div></div><div>fs-123456789</div></div>	SSD performance-type	NFS	4.00 KB	China East 2 Zone B	2018-12-26 15:21:15	No	1	<div><div>Add Mount Point</div><div>Manage</div><div>Delete</div></div>
<div><div><div>fs-987654321</div><div>fs-987654321</div></div><div>fs-987654321</div></div>	SSD performance-type	NFS	0 B	China East 2 Zone B	2019-07-15 09:17:42	No	0	<div><div>Add Mount Point</div><div>Manage</div><div>Delete</div></div>

View the details of a file system

Locate 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 points of the file system.

Basic Information

Delete File System

File System ID: fs-12345678

Region: China East 2 (Shanghai)

Zone: China East 2 Zone B

Storage Type: SSD performance-type

Protocol Type: NFS (NFSv3 and NFSv4.0)

File System Usage: 4.00 KB

Created On: 2018-12-26 15:21:15

Storage Package

ID: Buy Package

Capacity:

Started At:

Valid Until:

Mount Point

Kernel Bugs

How to mount

Automatic Mount

Add Mount Point

Mount Point Type

VPC

VSwitch

Mount Address

Mount Command

Permission Group

Status

Action

VPC

VPC-12345678

vsw-12345678

10.10.10.10

V3 Mount:

sudo mount -t nfs -o vers=3,nolock,proto=tcp,noresvport fs-12345678-shanghai.nas.aliyuncs.com:/mnt

V4 Mount:

sudo mount -t nfs -o vers=4,minorversion=0,noresvport fs-12345678-shanghai.nas.aliyuncs.com:/mnt

fs-12345678

Mounted

Delete a file system

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



Note:

- Before deleting a file system, you must remove all mount points of the file system.
- Use caution while deleting a file system. After a file system is deleted, the data on the file system cannot be restored.

3 Manage mount points

This topic describes how to manage mount points in the Network Attached Storage (NAS) console. The management includes creating, deleting, enabling, and disabling mount points. It also includes viewing a list of mount points, and modifying the permission group of a mount point.

Create a mount point

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



Note:

You can create a NAS Capacity file system or NAS Performance file system in a classic network or VPC. You can create a maximum of two mount points for each file system.

1. Log on to the [NAS console](#).
2. Choose NAS > File System List.
3. Locate the target file system and click Add Mount Point.

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

Add Mount Point

The mount point is the entry for the ECS server to visit the file system. The mount point types currently supported are classic network and VPC. Each mount point must be bound to a permission group.

The Linux client implements a default limitation on the number of concurrent requests to the NFS. In the event of poor performance, you can refer to [this document](#) to adjust the configuration.

File System ID :

* Mount Point Type :

VPC

* VPC :

[Go to the VPC console to create a VPC](#)

* VSwitch :

* Permission Group :

VPC default permission group (all

OK

Cancel

Mount Point Type: includes VPC and classic network.

5. After you complete the configuration, click OK.

View a list of mount points

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

0356249afa

Basic Information

Delete File System

File System ID: 0356249afa	Region: China East 1 (Hangzhou)	Zone: China East 1 Zone G
Storage Type: SSD performance-type	Protocol Type: SMB (2.1 and later)	File System Usage: 0 B
Created On: 2019-03-23 14:23:16		

Storage Package

ID: 0356249afa-0356249afa-0356249afa	Capacity: 500.00 GB Upgrade	Started At: 2019-03-23 14:30:14	Valid Until: 2019-05-24 00:00:00 Renew
--------------------------------------	-----------------------------	---------------------------------	--

Mount Point

How to mount

Add Mount Point

Mount Point Type	VPC	VSwitch	Mount Address	Permission Group	Status	Action
VPC	VPC-0356249afa-0356249afa-0356249afa	VSwitch-0356249afa-0356249afa-0356249afa	0356249afa-0356249afa-0356249afa	VPC default permission group	Available	Modify Permission Group Activate Disable Delete

Enable or disable a mount point

You can perform the following actions to control access to the mount point from clients.

- Click **Disable** to disable access to the mount point from clients.
- Click **Activate** to allow access to the mount point from clients.

Delete a mount point

Click **Delete** to delete a mount point.



Note:

Use caution while deleting a mount point. After you delete a mount point, the mount point cannot be restored.

Modify the permission group of a mount point

Click **Modify Permission Group** to modify the permission group of a mount point. For more information about permission groups, see [#unique_10](#).



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 [#unique_15](#).
 - For more information about how to enable an automatic mount on an ECS instance running Windows, see [#unique_16](#).
- 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 [#unique_18](#).

- 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_19](#).
 - For more information about how to use a network address translation (NAT) gateway to mount an on-premises file system, see [#unique_20](#).

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 [#unique_22/unique_22_Connect_42_section_5jo_0kj_jn5](#).
2. You have created a mount point. For more information, see [#unique_23/unique_23_Connect_42_section_6xi_a3u_zkq](#).

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_24](#).

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 , minorversi on = 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
wsiz	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 wsiz 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.

```
debugfs on /sys/kernel/debug type debugfs (rw,relatime)
mqueue on /dev/mqueue type mqueue (rw,relatime)
hugetlbfs on /dev/hugepages type hugetlbfs (rw,relatime)
sunrpc on /var/lib/nfs/rpc_pipefs type rpc_pipefs (rw,relatime)
0:12345678901.cn-hangzhou.nas.aliyuncs.com: on /mnt type nfs4 (rw,relatime,vers=4.0,rsize=1048576,wsiz=1048576,namlen=255,hard,noreportport,proto=tcp,timeo=600,retrans=2,sec=sys,clientaddr=10.0.0.17,local_lock=none,addr=10.0.0.17, netdev)
tmpfs on /run/user/0 type tmpfs (rw,nosuid,nodev,relatime,size=800916k,mode=700)
froot@iZbp19je62it610xd1876Z ~$
```

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

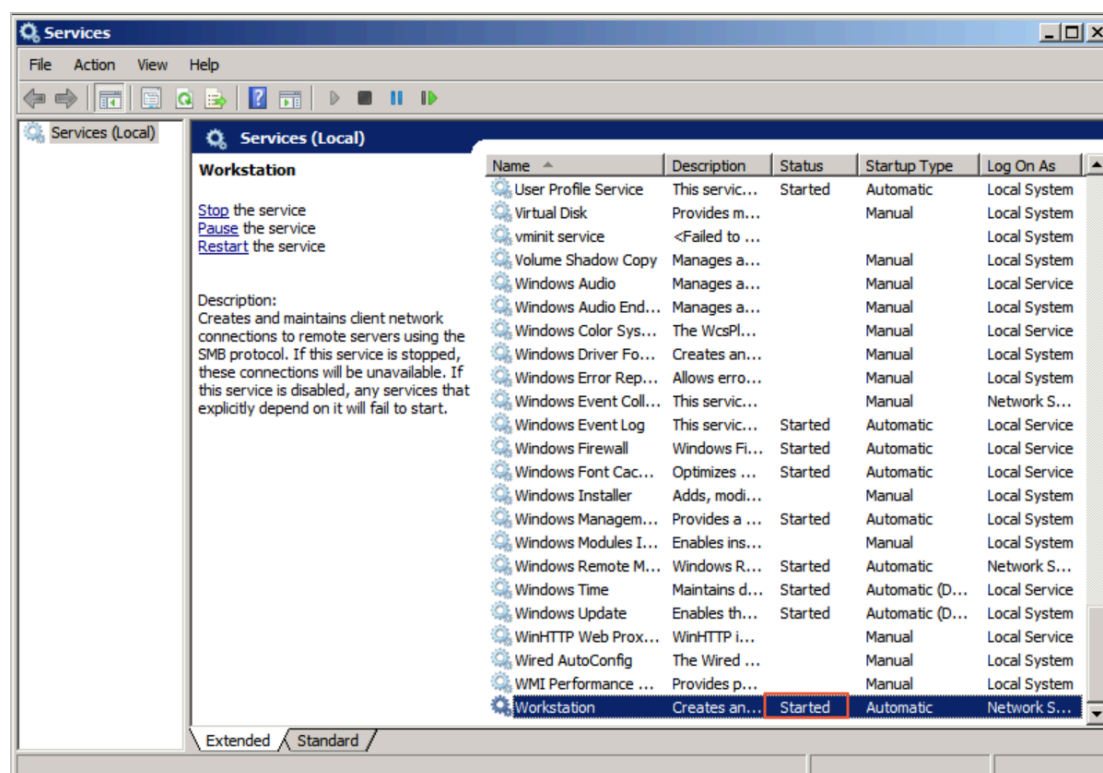
1. You have created a file system. For more information, see [#unique_22/unique_22_Connect_42_section_5jo_0kj_jn5](#).
2. You have created a mount point. For more information, see [#unique_23/unique_23_Connect_42_section_6xi_a3u_zkq](#).

3. Ensure that the following Windows services are started:

- Workstation

- Choose All Programs > Accessories > Run, or press **Win + R** and enter `services . msc` to open the Services console.
- Locate the Workstation service and ensure that the status of the service is **Started**.

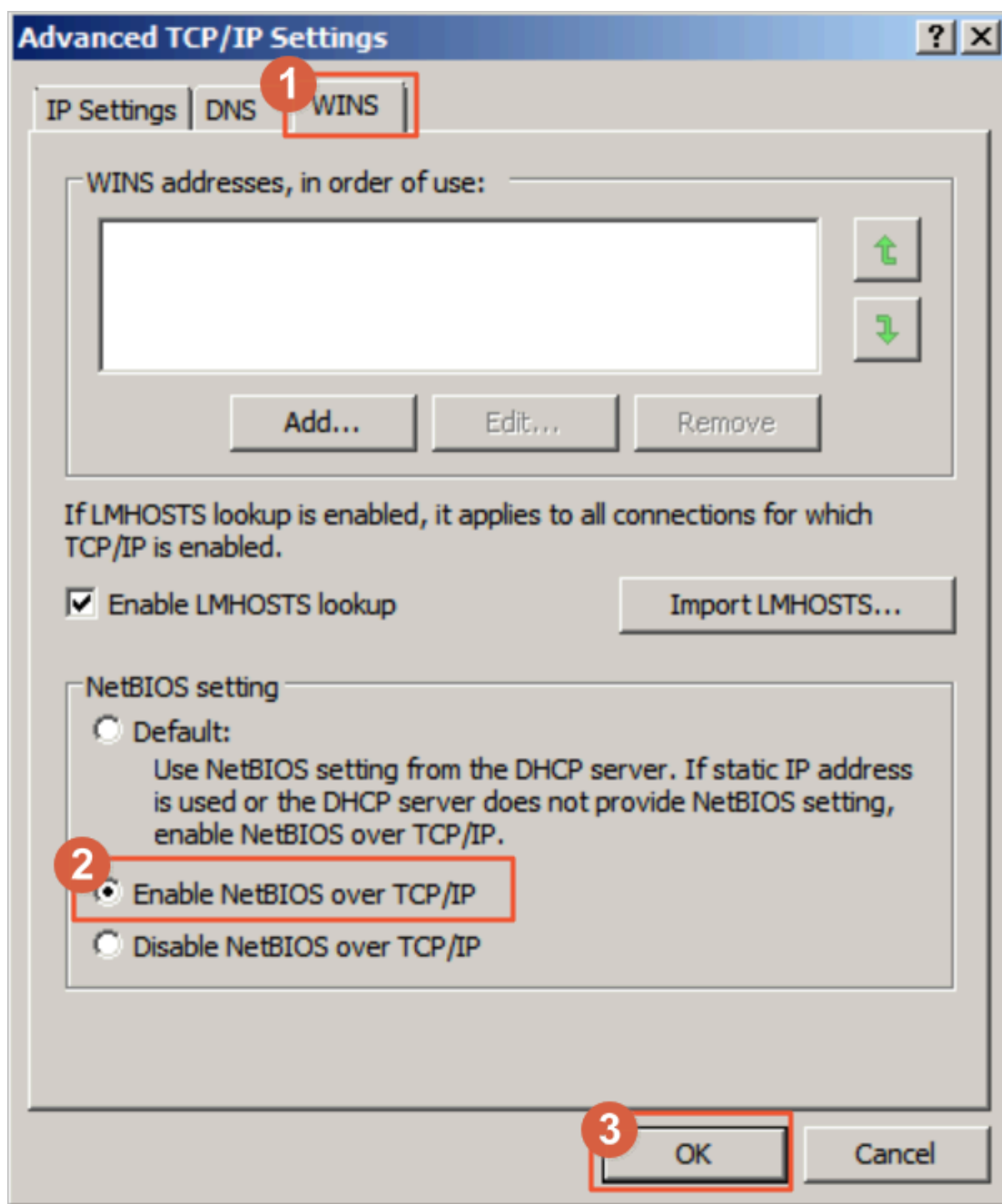
The Workstation service is started by default.



- TCP/IP NetBIOS Helper

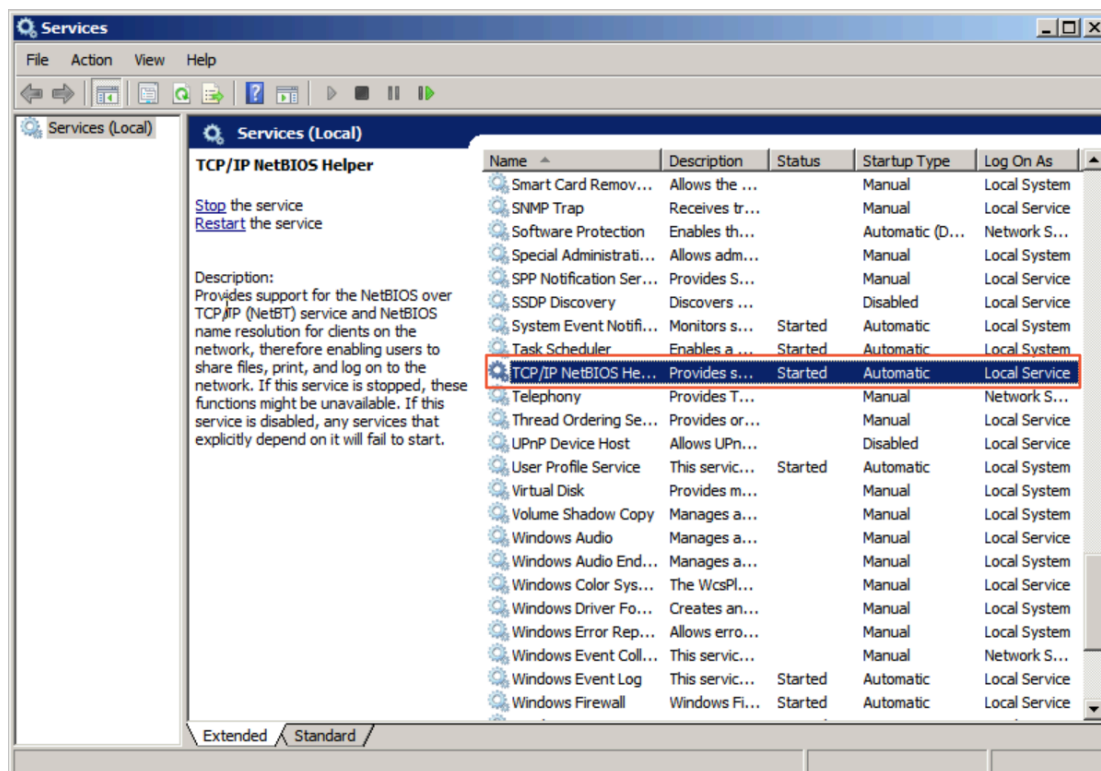
Perform the following steps to start the TCP/IP NetBIOS Helper service:

- Open Network and Sharing Center and click the active network connection.
- 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.
- 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. Log on to the [ECS console](#).
2. 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_27](#).

3. Use the `net use` command to view the results.

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

```
C:\Users\Administrator>net use
New connections will be remembered.

Status          Local        Remote                                           Network
-----
OK              D:          \\6.228.254.2 - Microsoft...nas.aliyuncs.com\myshare
                                           Microsoft Windows Network

The command completed successfully.
```

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 [#unique_22/unique_22_Connect_42_section_5jo_0kj_jn5](#).
2. You have created a mount point. For more information, see [#unique_23/unique_23_Connect_42_section_6xi_a3u_zkq](#).
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. Log on to the [ECS console](#).
2. 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 , minorversi on = 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 , minorversi on =
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	
_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.

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
wsiz	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.

Parameter	Description
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. Run the `reboot` command to restart the ECS instance.

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

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

```
debugfs on /sys/kernel/debug type debugfs (rw,relatime)
mqueue on /dev/mqueue type mqueue (rw,relatime)
hugetlbfs on /dev/hugepages type hugetlbfs (rw,relatime)
sunrpc on /var/lib/nfs/rpc_pipefs type rpc_pipefs (rw,relatime)
0.0.0.0:0.0.0.0:0.0.0.0.cn-hangzhou.nas.aliyuncs.com:/ on /mnt type nfs4 (rw,relatime,vers=4.0,rsz=1048576,wsz=1048576,namlen=255,hard,noreport,proto=tcp,timeo=600,retrans=2,sec=sys,clientaddr=10.0.0.1,local_lock=none,addr=10.0.0.1,netdev)
tmpfs on /run/user/0 type tmpfs (rw,nosuid,nodev,relatime,size=800916k,mode=700)
[root@iZbp19je62it610xd1t876Z ~]#
```

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

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

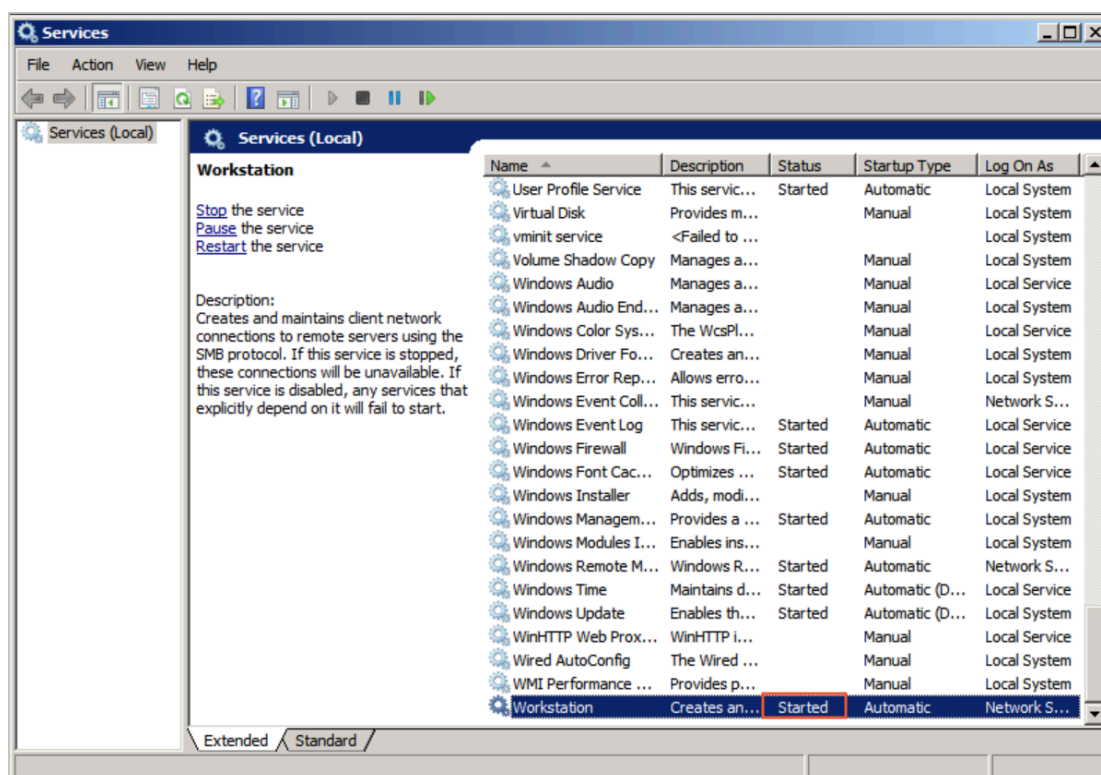
1. You have created a file system. For more information, see [#unique_22/unique_22_Connect_42_section_5jo_0kj_jn5](#).
2. You have created a mount point. For more information, see [#unique_23/unique_23_Connect_42_section_6xi_a3u_zkq](#).

3. Ensure that the following Windows services are started:

- Workstation

- Choose All Programs > Accessories > Run, or press **Win + R** and enter `services . msc` to open the Services console.
- Locate the Workstation service and ensure that the status of the service is Started.

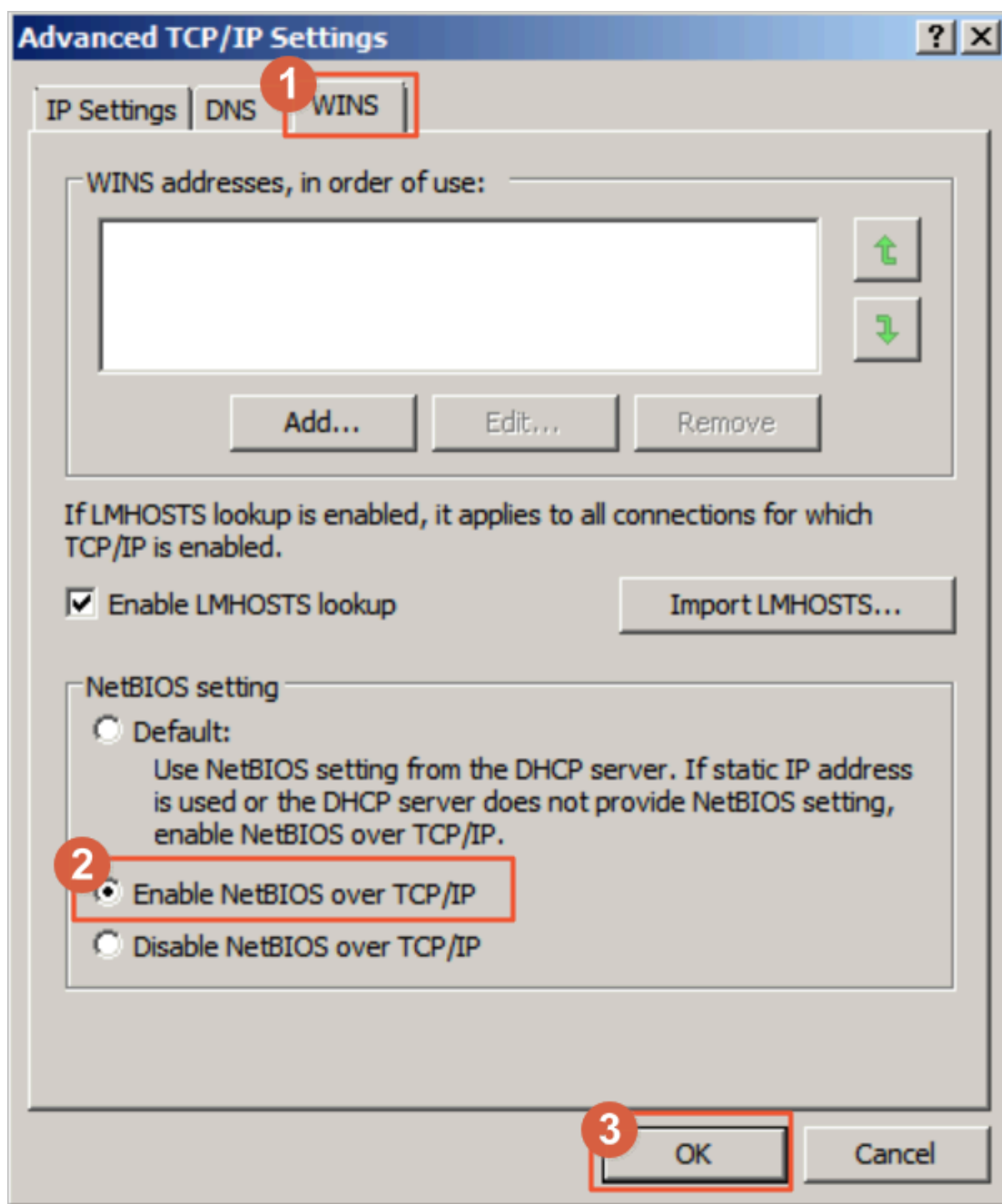
The Workstation service is started by default.



- TCP/IP NetBIOS Helper

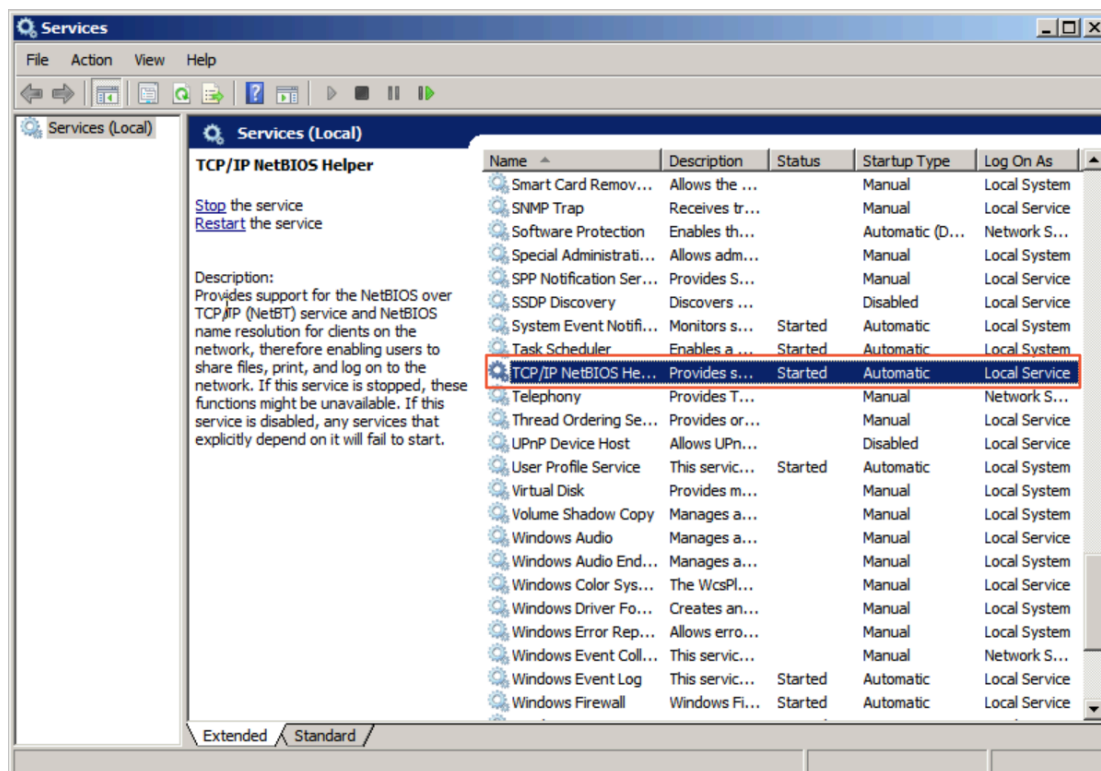
Perform the following steps to start the TCP/IP NetBIOS Helper service:

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

1. Log on to the [ECS console](#).
2. 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
```

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.

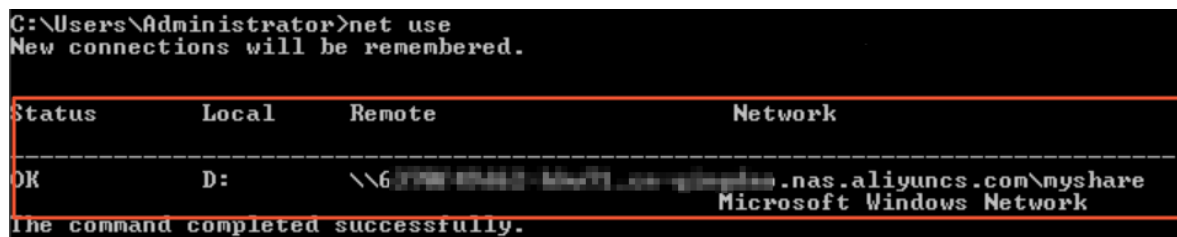
3. Create a scheduled task.

- 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.

4. 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.



```
C:\Users\Administrator>net use
New connections will be remembered.

Status          Local          Remote          Network
-----
OK              D:             \\6.174.104.101\\myshare
                                     Microsoft Windows Network

The command completed successfully.
```

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

Typically, you can only mount a file system on an ECS instance that is hosted by the same VPC as that of the mount point. If the mount point 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. You can enable a cross-VPC mount for the file system after the connection is established.

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.

Create CEN Instance

Description ?

0/256

Attach Network

Your Account

Note: You cannot attach networks that are already attached to the CEN instance. Additionally, you cannot attach networks that have Express Connect enabled.

• Network Type ?

Select

• Region ?

Select

• Networks ?

Select

OK

Cancel

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

Name	Description
Description	<p>The description of the CEN instance.</p> <p>The description must be 2 to 256 characters in length and cannot start with <code>http ://</code> or <code>https ://</code>.</p>
Attach Network	<p>You can attach networks owned by this account or a different account to a CEN instance. For more information, see CEN instances.</p>

2. Attach a network.

- a) On the Instances page, locate the target instance, and click Manage.
- b) On the Networks tab, click Attach Network to configure the network.

Attach Network

Your Account

Different Account

Note: You cannot attach networks that are already attached to the CEN instance. Additionally, you cannot attach networks that have Express Connect enabled.

• Network Type ?

Select

• Region ?

Select

• Networks ?

Select

OK

Cancel

Name	Description
Account	Select the Your Account tab.
Network Type	The type of network to be attached. Valid values : VPC, Virtual Border Router (VBR), and Cloud Connect Network (CCN). Select VPC.
Region	The region that hosts the network. Select China (Qingdao).

Issue: 20190819

37

Name	Description
Networks	The name of the network to be attached. Select a VPC network.

- c) Repeat the preceding steps to attach another VPC network to the CEN instance to establish a connection between the 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. Assume that you have multiple Alibaba Cloud accounts and want to allow mutual access between a file system and an ECS instance from different accounts. At this point, you must establish a connection between VPCs that host the file system and the ECS instance respectively.

You can use Alibaba Cloud Cloud Enterprise Network (CEN) to connect VPCs owned by different accounts.

Procedure

1. Create a CEN instance by using Account A.
 - a) Log on to the [CEN console](#).
 - b) On the Instances page, click Create CEN Instance.
 - c) Configure the CEN instance.

Create CEN Instance

Description ?

0/256

Attach Network

Your Account

Note: You cannot attach networks that are already attached to the CEN instance. Additionally, you cannot attach networks that have Express Connect enabled.

• Network Type ?

Select

• Region ?

Select

• Networks ?

Select

OK

Cancel

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


Name	Description
Description	<p>The description of the CEN instance.</p> <p>The description must be 2 to 256 characters in length and cannot start with <code>http ://</code> or <code>https ://</code>.</p>
Attach Network	<p>You can attach networks owned by this account or a different account to a CEN instance. For more information, see CEN instances.</p>

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

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) Locate the target VPC, and click Manage.
- d) On the VPC Details page, locate 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.

Attach to CEN

 The account that you have authorized can attach your network to their CEN instances and communicate with your network. Use caution when performing this operation.

● **Peer Account UID**

● **Peer Account CEN ID**

OK

Cancel

3. Attach a network by using Account A.

- a) Log on to the [CEN console](#) by using Account A.
- b) On the Instances page, locate the target instance, and click Manage.
- c) On the Networks tab, click Attach Network to configure the network.

Attach Network

Your Account

Different Account

Note: Go to the VPC console, in the properties page of the VPC or virtual border router, authorize the related CEN instance to attach that network. Networks already attached to the CEN instance cannot be attached again. Networks with Express Connect enabled cannot be attached.

Owner Account ?

0/128

Network Type ?

Select

Region ?

Select

Networks ?

0/128

OK

Cancel

Name	Description
Account	Select Different Account tab.
Owner Account	The ID of the account that owns the target network. Enter the ID of Account B.
Network Type	The type of network to be attached. Valid values : VPC, Virtual Border Router (VBR), and Cloud Connect Network (CCN). Select VPC.
Region	The region that hosts the network.

Name	Description
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](#).

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.

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 and avoid changing the default values of these parameters.

When unmounting a file system, an error indicating that the device is busy may occur. Use 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 NAS file system.

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

3. Run the `mount -l` command to verify the unmount results.

If a 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.