Scalable File Service

Getting Started

Issue 01

Date 2025-07-25

HUAWEI TECHNOLOGIES CO., LTD.

Copyright © Huawei Technologies Co., Ltd. 2025. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

Trademarks and Permissions


and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Security Declaration

Vulnerability

Huawei's regulations on product vulnerability management are subject to the *Vul. Response Process.* For details about this process, visit the following web page:
https://www.huawei.com/en/psirt/vul-response-process
For vulnerability information, enterprise customers can visit the following web page:
https://securitybulletin.huawei.com/enterprise/en/security-advisory

Contents

 Copyright © Huawei Technologies Co., Ltd.

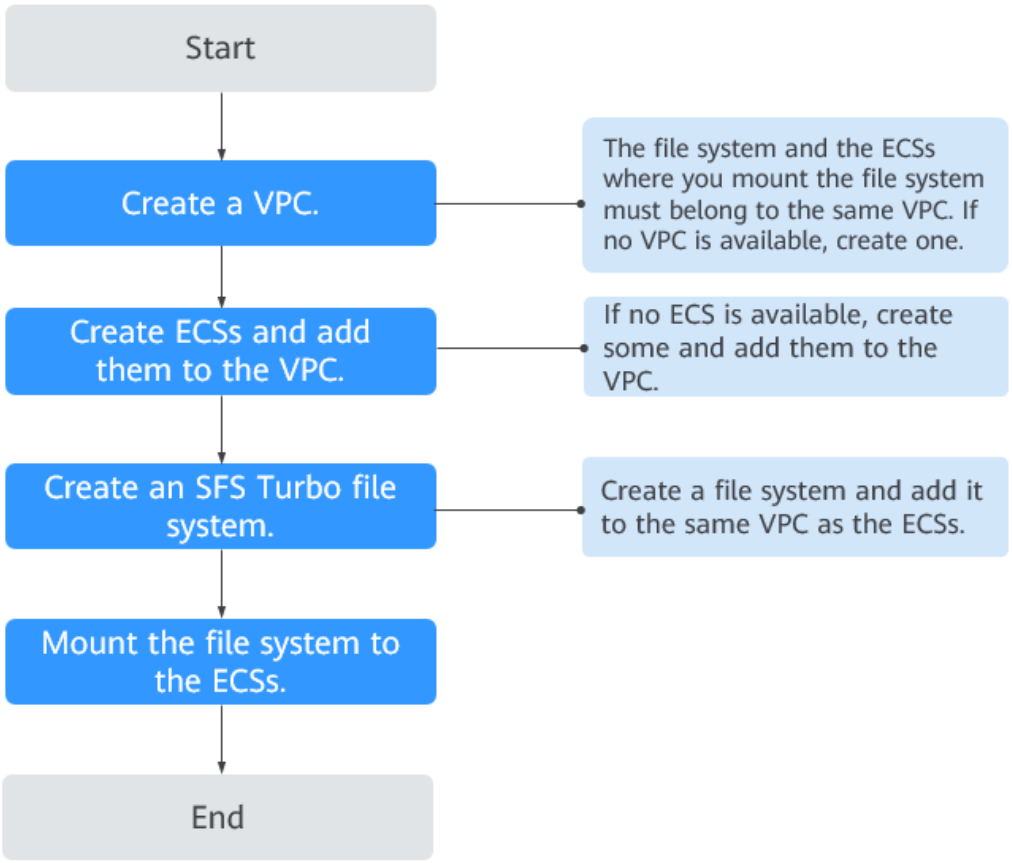
1 Overview

This section describes how to use SFS.

After creating a file system, you cannot directly access the file system. Instead, you need to mount the file system to ECSs.

Figure 1-1 shows the process for creating and mounting an SFS Turbo file system.

Figure 1-1 Process for using SFS Turbo



 Copyright © Huawei Technologies Co., Ltd.

2 Make Preparations

Before using SFS, you need to make the following preparations:

- **Registering a HUAWEI ID and Enabling Huawei Cloud Services**
- **Creating an IAM User**

Registering a HUAWEI ID and Enabling Huawei Cloud Services

If you already have a HUAWEI ID, skip this part. To create a HUAWEI ID, do as follows:

1. Visit **www.huaweicloud.com/eu/** and click **Sign Up**.
2. On the displayed page, register an account as prompted.

   After you have successfully registered, the system automatically redirects you to your personal information page.

Creating an IAM User

If you want to allow multiple users to manage your resources without sharing your password or private key, you can create users using IAM and grant permissions to the users. These users can use specified login links and their own accounts to access the public cloud and help you efficiently manage resources. You can also set account security policies to ensure the security of these accounts and reduce enterprise information security risks.

If you have registered with the public cloud but have not created an IAM user, you can create a user on the IAM console. For example, to create an SFS administrator, perform the following steps:

1. Enter your username and password to log in to the management console.
2. In the upper right corner of the page, hover the mouse over the username and select **Identity and Access Management**.
3. In the navigation pane on the left, choose **Users**.
4. On the **Users** page, click **Create User**.
5. Enter user information on the **Create User** page.
   - **Username**: Enter a username, for example, **sfs_admin**.
   - **Email Address**: Email address of the IAM user. This parameter is mandatory if the access type is specified as **Set by user**.

 Copyright © Huawei Technologies Co., Ltd.

- (Optional) **Mobile Number**: Mobile number of the IAM user.
- (Optional) **Description**: Enter the description of the user, for example, **SFS administrator**.

6. Select **Management console access** for **Access Type** and **Set now** for **Password**. Enter a password and click **Next**.

   NOTE

   An SFS administrator can log in to the management console and manage users. You are advised to select **Set now** for **Password Type** when you create an SFS administrator for your domain. If you create an SFS administrator for another user, you are advised to select **Set by user** for **Password Type** instead so that the user can set their own password.

7. (Optional) Add the user to the **admin** user group and click **Create**.

   User group **admin** has all the operation permissions. If you want to grant fine-grained permissions to IAM users, see **Creating a User and Granting SFS Permissions**.

   The user is displayed in the user list. You can click the IAM user login link to log in to the console.

 Copyright © Huawei Technologies Co., Ltd.

3 Create a File System

You can create a file system and mount it to multiple servers. Then the servers can share this file system.

Prerequisites

1. Before creating an SFS Turbo, file system, ensure that a VPC is available.

   If no VPC is available, create one by referring to section "Creating a VPC" in the *Virtual Private Cloud User Guide*.

2. Before creating an SFS Turbo file system, ensure that ECSs are available and are in the created VPC.

   If no ECS is available, create an ECS by referring to "Creating an ECS" in the *Elastic Cloud Server User Guide*.

Logging In to the Management Console

Step 1 Visit the Huawei Cloud website at **www.huaweicloud.com/eu/**.

Step 2 Register an account.

Before using SFS, you need to register a HUAWEI ID. This account can be used to access all Huawei Cloud services, including SFS. If you already have an account, start from **Step 3**.

1. In the upper right corner of the page, click **Sign Up**.
2. Complete the registration as instructed.

   After you have successfully registered, the system automatically redirects you to your personal information page.

Step 3 Log in to the management console.

1. In the upper right corner of the displayed page, click **Console**.
2. Enter the username and password as prompted, and click **Sign In**.

Step 4 After logging in to the management console, select the region where the service is located from the drop-down list in the upper left corner of the page.

Step 5 Choose **Storage** > **Scalable File Service** to go to the SFS console.

 Copyright © Huawei Technologies Co., Ltd.

Step 6 It is recommended that you top up your account and subscribe to SFS so that the service can be used properly. For details about how to purchase SFS, see **How Do I Purchase SFS?**

----End

Procedure

Step 1 Log in to the management console using a cloud account.

1. Log in to the management console and select a region and a project.
2. Choose **Storage** > **Scalable File Service**.

Step 2 In the upper right corner of the page, click **Create File System**.

Step 3 Configure the parameters. **Table 3-1** describes the parameters.

Table 3-1 File system parameters

Parameter	Description	Remarks
Billing Mode	Mandatory	-
Region	Mandatory Region of the tenant. Select the region from the drop-down list in the upper left corner of the page.	You are advised to select the region where the servers reside.
AZ	Mandatory A geographical area with an independent network and an independent power supply.	You are advised to select the AZ where the servers reside.
Type	Mandatory The following types are supported: Standard, Standard-Enhanced (discontinued), Performance, Performance-Enhanced (discontinued), 20 MB/s/TiB, 40 MB/s/TiB, 125 MB/s/TiB, 250 MB/s/TiB, 500 MB/s/TiB, and 1,000 MB/s/TiB.	Select **Standard**. **NOTE** Once a file system is created, its storage class cannot be changed. If you want to change the storage class, you need to create another file system. Therefore, you are advised to plan the storage class carefully in advance.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Remarks
Capacity	Maximum capacity allowed for a single file system. When the used capacity of a file system reaches this value, no more data can be written to the file system. You need to expand the file system capacity. The capacity of an SFS Turbo file system cannot be reduced. Set an appropriate file system capacity based on your service needs.	Supported ranges: Supported ranges: • Standard: 500 GB to 32 TB • Performance: 500 GB to 32 TB • Standard-Enhanced (discontinued): 10 TB to 320 TB • Performance-Enhanced (discontinued): 10 TB to 320 TB • 20 MB/s/TiB: 3.6 TB to 1 PB • 40 MB/s/TiB: 1.2 TB to 1 PB • 125 MB/s/TiB: 1.2 TB to 1 PB • 250 MB/s/TiB: 1.2 TB to 1 PB • 500 MB/s/TiB: 1.2 TB to 1 PB • 1,000 MB/s/TiB: 1.2 TB to 1 PB
Protocol Type	Mandatory SFS Turbo supports NFS for file system access.	The default value is **NFS**.
Bandwidth (GB/s)	Defines the cache bandwidth, which is recommended for workloads with heavy reads and infrequent writes. The higher the bandwidth, the larger the capacity required.	• If you select the 20 MB/s/TiB, 40 MB/s/TiB, 125 MB/s/TiB, 250 MB/s/TiB, 500 MB/s/TiB, or 1,000 MB/s/TiB type, this parameter and its value will show up. Bandwidth size = Capacity x Bandwidth density (type value). • If you select the Standard, Standard-Enhanced, Performance, or Performance-Enhanced file system type, this parameter will not show up.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Remarks
VPC	Mandatory Select a VPC and its subnet. ● VPC: A server cannot access file systems in a different VPC. Select the VPC to which the server belongs. ● Subnet: A subnet is an IP address range in a VPC. In a VPC, a subnet segment must be unique. A subnet provides dedicated network resources that are logically isolated from other networks, improving network security. **NOTE** ● Only one VPC can be added when a file system is created. Multi-VPC file sharing can be implemented through VPC peering connection. For details about VPC peering connection, see section "VPC Peering Connection" in *Virtual Private Cloud User Guide*.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Remarks
Security Group	Mandatory A security group is a virtual firewall that provides secure network access control policies for file systems. You can define different access rules for a security group to protect the file systems that are added to this security group. When creating an SFS Turbo file system, you can select only one security group. You are advised to use an independent security group for an SFS Turbo file system to isolate it from service nodes. The security group rule configuration affects the normal access and use of SFS Turbo. For details about how to configure a security group rule, see section "Adding a Security Group Rule" in the *Virtual Private Cloud User Guide*. After an SFS Turbo file system is created, the system automatically enables the security group port required by the NFS protocol in the SFS Turbo file system. This ensures that the SFS Turbo file system can be accessed by your ECS and prevents file system mounting failures. The inbound ports required by the NFS protocol are ports 111, 2049, 2051, 2052, and 20048. If you need to change the enabled ports, go to the VPC console, choose **Access Control** > **Security Groups**, locate the target security group, and change the ports.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Remarks
Encryption	Optional Specifies whether a file system is encrypted. You can create a file system that is encrypted or not, but you cannot change the encryption attribute of an existing file system. If **Encryption** is selected, the following parameters will be displayed: • **KMS key name** **KMS key name** is the identifier of the key, and you can use **KMS key name** to specify the KMS key that is to be used for encryption. Select an existing key from the drop-down list, or click **View KMS List** to create a new key. For details, see in the . • **KMS key ID** After you select a key name, the system automatically shows the key ID.	-
Enterprise Project	This parameter is provided for enterprise users. When creating a file system, you can add the file system to an existing enterprise project. An enterprise project is a cloud resource management mode, in which cloud resources and members are centrally managed by project. The default project is **default**. Select an enterprise project from the drop-down list.	You can select only created enterprise projects. To create an enterprise project, click in the upper right corner of the console page.
Name	Mandatory User-defined name of the file system.	The name can contain only letters, digits, and hyphens (-). It must contain more than four characters but no more than 64 characters.

Step 4 Click **Create Now**.

Step 5 Confirm the file system information and click **Submit**.

Step 6 Complete the creation and go back to the file system list.

 Copyright © Huawei Technologies Co., Ltd.

If the status of the created file system is **Available**, the file system is created successfully. If the status is **Creation failed**, contact the administrator.

----End

 Copyright © Huawei Technologies Co., Ltd.

4 Mount a File System

4.1 Mounting an NFS File System to ECSs (Linux)

After creating a file system, you need to mount the file system to servers so that they can share the file system.

In this section, ECSs are used as example servers. Operations on BMSs are the same as those on ECSs.

To use SFS Turbo as the storage backend for CCE, see **Storage**. Then complete the deployment on the CCE console.

Prerequisites

- You have checked the type of the operating system (OS) on each ECS. Different OSs use different commands to install the NFS client.
- You have created a file system and have obtained the mount point of the file system.
- At least one ECS is available.

Constraints

NOTE

This constraint only applies to local paths (mount points) and does not affect other files or directories.

Metadata of the local paths (mount points) cannot be modified. Specifically, the following operations cannot be performed on the local paths' metadata:

- **touch**: Update file access time and modification time.

- **rm**: Delete files or directories.

 Copyright © Huawei Technologies Co., Ltd.

- **cp**: Replicate files or directories.
- **mv**: Move files or directories.
- **rename**: Rename files or directories.
- **chmod**:Modify permissions on files or directories.
- **chown**: Change file or directory owners.
- **chgrp**: Change file or directory groups.
- **ln**: Create hard links.
- **link**: Create hard links.
- **unlink**: Delete hard links.

The **atime**, **ctime**, and **mtime** attributes of a local path (root directory of the mount point) are the current time. So each time the root directory attribute is queried, the current time of the server is returned.

Procedure

Step 1 Log in to the management console using a cloud account.

1. Log in to the management console and select a region and a project.
2. Choose **Compute** > **Elastic Cloud Server** to go to the ECS console.

Step 2 Log in to the ECS as user **root**.

NOTE

If you log in to the ECS as a non-root user, see **Mounting a File System to a Linux ECS as a Non-root User**.

Step 3 Install the NFS client.

1. **Install the NFS client.**
   a. Run the following command to check whether the NFS software package is installed.
      - In CentOS, Red Hat, Oracle Enterprise Linux, SUSE, EulerOS, Fedora, or OpenSUSE:

        rpm -qa|grep nfs
      - In Debian or Ubuntu:

        dpkg -l nfs-common

      If no such command output is displayed, go to **b**.
      - In CentOS, Red Hat, EulerOS, Fedora, or Oracle Enterprise Linux:
        ```
        libnfsidmap
        nfs-utils
        ```
      - In SUSE or OpenSUSE:
        ```
        nfsidmap
        nfs-client
        ```
      - In Debian or Ubuntu:
        ```
        nfs-common
        ```

 Copyright © Huawei Technologies Co., Ltd.

b. Run the following command to install the NFS software package.

NOTE

The following commands require that ECSs be connected to the Internet. Or, the installation will fail.

- In CentOS, Red Hat, EulerOS, Fedora, or Oracle Enterprise Linux:
  sudo yum -y install nfs-utils
- In Debian or Ubuntu:
  sudo apt-get install nfs-common
- In SUSE or OpenSUSE:
  zypper install nfs-client

Step 4 Run the following command to create a local path for mounting the file system:

mkdir *Local path*

NOTE

If there is any resource, such as a disk, already mounted on the local path, create a new path. (NFS clients do not refuse repeated mounts. If there are repeated mounts, information of the last successful mount is displayed.)

Step 5 Run the following command to mount the file system to the ECS that belongs to the same VPC as the file system. Currently, the file system can be mounted to Linux ECSs using NFSv3 only.

Table 4-1 describes the variables.

To mount an SFS Turbo file system, run the following command: **mount -t nfs -o vers=3,timeo=600,noresvport,nolock,tcp** *Mount point Local path*

NOTICE

After a client ECS is restarted, it loses the file system mount information. You can configure auto mount in the **fstab** file to ensure that the ECS automatically mounts the file system when it restarts. For details, see **4.4 Mounting a File System Automatically**.

Table 4-1 Parameter description

Parameter	Description
vers	File system version. Only NFSv3 is supported currently, so the value is fixed to **3**.
timeo	Waiting time before the NFS client retransmits a request. The unit is 0.1 second. The recommended value is **600**.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
noresvport	Whether the NFS client uses a new TCP port when a network connection is re-established. It is strongly recommended you use the **noresvport** option, which ensures that your file system maintains uninterrupted availability after a network reconnection or recovery.
lock/nolock	Whether to lock files on the server using the NLM protocol. If **nolock** is selected, the lock is valid for applications on one host. For applications on another host, the lock is invalid. The recommended value is **nolock**. If this parameter is not specified, **lock** is selected by default. In this case, other servers cannot write data to the file system.
Mount point	The format for an SFS Turbo file system is *File system IP address*:/, for example, **192.168.0.0:/**.
Local path	A local directory on the ECS used to mount the file system, for example, **/local_path**.

For more mounting parameters for performance optimization during file system mounting, see **Table 4-2**. Use commas (,) to separate parameters. The following command is an example:

mount -t nfs -o vers=3,timeo=600,nolock,rsize=1048576,wsize=1048576,hard,retrans=3,noresvport,ro,async,noatime,nodiratime *Mount point Local path*

Table 4-2 Parameters for file system mounting

Parameter	Description
rsize	Maximum number of bytes that can be read from the server each time. The actual data is less than or equal to the value of this parameter. The value of **rsize** must be a positive integer that is a multiple of **1024**. If the entered value is smaller than **1024**, the value is automatically set to **4096**. If the entered value is greater than **1048576**, the value is automatically set to **1048576**. By default, the setting is performed after the negotiation between the server and the client. You are advised to set this parameter to the maximum value **1048576**.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
wsize	Maximum number of bytes that can be written to the server each time. The actual data is less than or equal to the value of this parameter. The value of **wsize** must be a positive integer that is a multiple of **1024**. If the entered value is smaller than **1024**, the value is automatically set to **4096**. If the entered value is greater than **1048576**, the value is automatically set to **1048576**. By default, the setting is performed after the negotiation between the server and the client. You are advised to set this parameter to the maximum value **1048576**.
soft/hard	**soft** indicates that a file system is mounted in soft mount mode. In this mode, if an NFS request times out, the client returns an error to the invoking program. **hard** indicates that a file system is mounted in hard mount mode. In this mode, if the NFS request times out, the client continues to request until the request is successful. The default value is **hard**.
retrans	Number of retransmission times before the client returns an error. Recommended value: **1**
ro/rw	• **ro**: indicates that the file system is mounted as read-only. • **rw**: indicates that the file system is mounted as read/write. The default value is **rw**. If this parameter is not specified, the file system will be mounted as read/write.
noresvport	Whether the NFS client uses a new TCP port when a network connection is re-established. It is strongly recommended you use the **noresvport** option, which ensures that your file system maintains uninterrupted availability after a network reconnection or recovery.
sync/async	**sync** indicates that data is written to the server immediately. **async** indicates that data is first written to the cache before being written to the server. Synchronous write requires that an NFS server returns a success message only after all data is written to the server, which brings long latency. The recommended value is **async**.
noatime	If you do not need to record the file access time, set this parameter. This prevents overheads caused by access time modification during frequent access.
nodiratime	If you do not need to record the directory access time, set this parameter. This prevents overheads caused by access time modification during frequent access.

 Copyright © Huawei Technologies Co., Ltd.

> **NOTE**
>
> You are advised to use the default values for the parameters without usage recommendations.

Step 6 Run the following command to view the mounted file system:

mount -l

If the command output contains the following information, the file system has been mounted.

Mount point on */local_path* type nfs (rw,vers=3,timeo=600,nolock,addr=)

Step 7 After the file system is mounted successfully, access the file system on the ECSs to read or write data.

If the mounting fails or times out, rectify the fault by referring to **Troubleshooting**.

> **NOTE**
>
> The maximum size of a file that can be written to an SFS Turbo file system is 32 TB, and that for an SFS Turbo Enhanced file system is 320 TB.

----End

4.2 Mounting an NFS File System to ECSs (Windows)

After creating a file system, you need to mount the file system to servers so that they can share the file system.

This section uses Windows Server 2012 as the example OS to describe how to mount an NFS file system. For other versions, perform the steps based on the actual situation.

In this section, ECSs are used as example servers. Operations on BMSs are the same as those on ECSs.

Prerequisites

- You have created a file system and have obtained the mount point of the file system.
- At least one ECS that is in the same VPC as the file system is available.

Procedure

Step 1 Log in to the management console using a cloud account.

1. Log in to the management console and select a region and a project.
2. Choose **Compute** > **Elastic Cloud Server** to go to the ECS console.

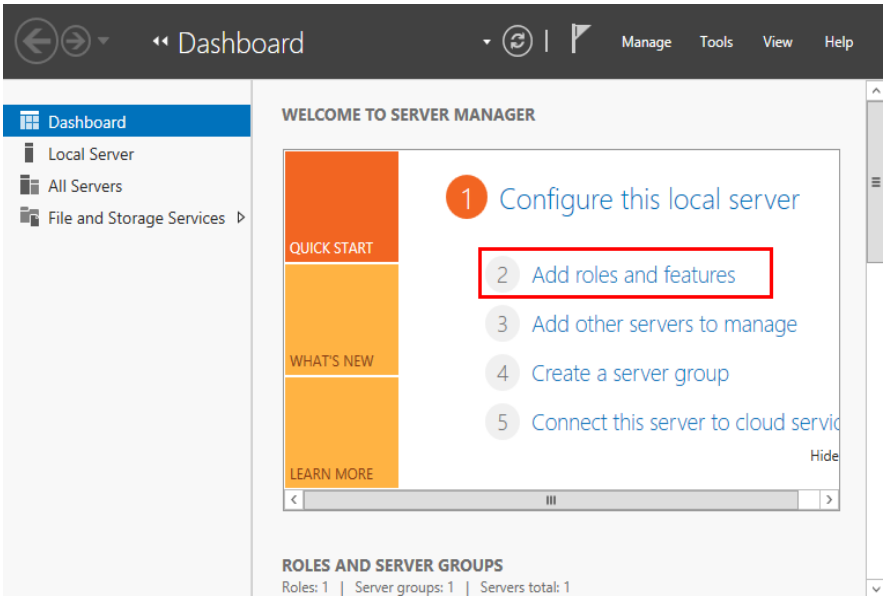
Step 2 On the ECS console, log in to the ECS running Windows Server 2012.

Step 3 Install the NFS client.

1. Click **Server Manager** in the lower left corner. The **Server Manager** window is displayed, as shown in **Figure 4-1**.

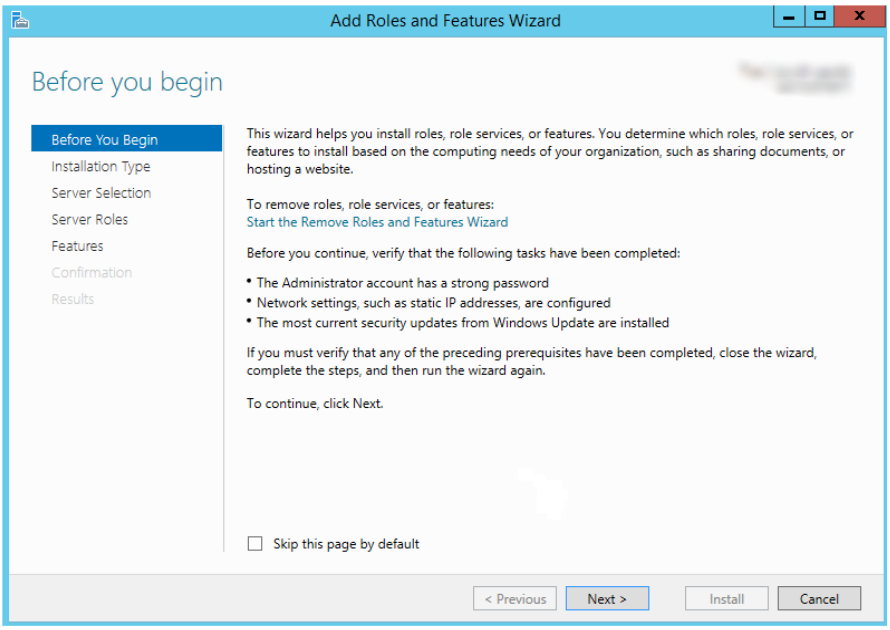
 Copyright © Huawei Technologies Co., Ltd.

Figure 4-1 Server Manager



2. Click **Add Roles and Features**. See **Figure 4-2**.

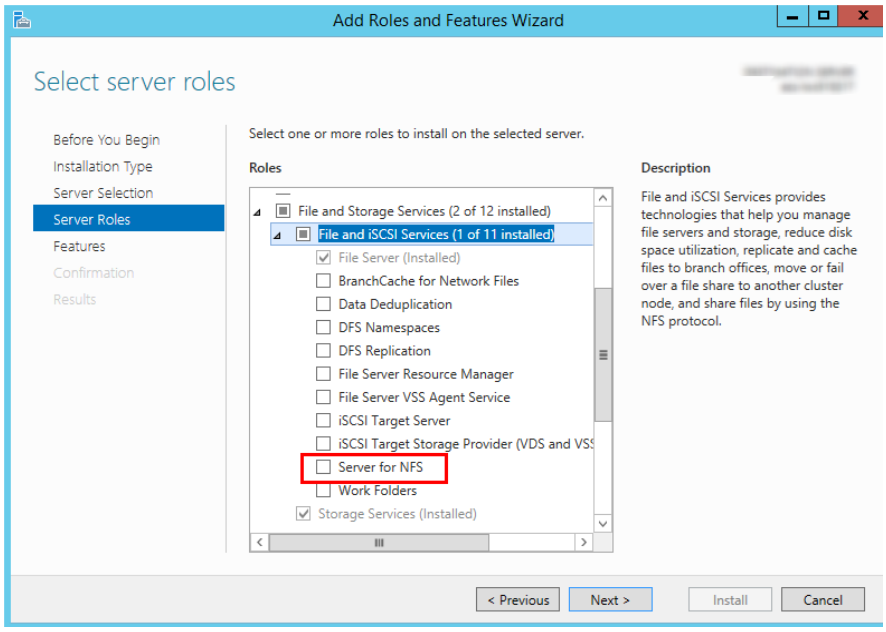
Figure 4-2 Wizard for adding roles and features



3. Click **Next** as prompted. On the **Server Roles** page, select **Server for NFS**, as shown in **Figure 4-3**.

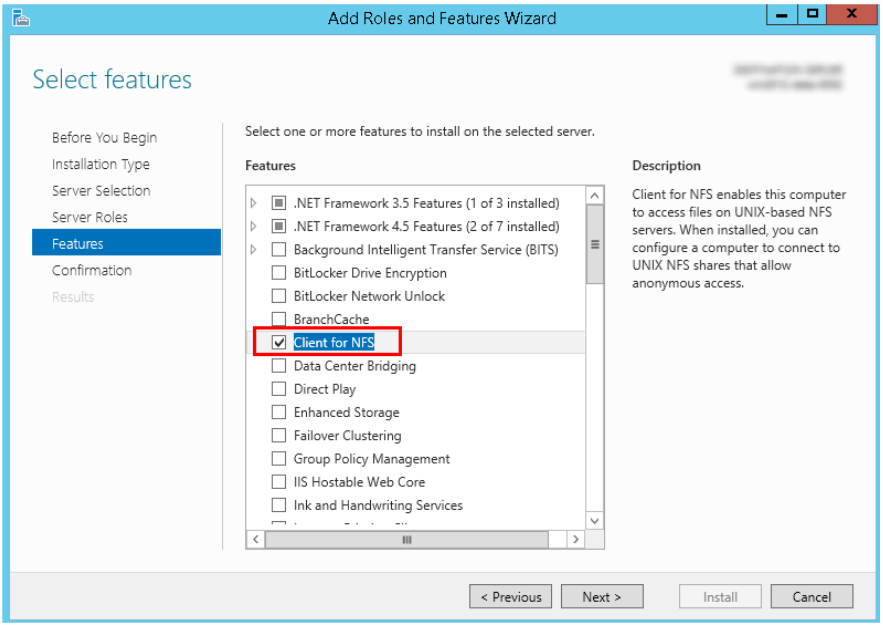
 Copyright © Huawei Technologies Co., Ltd.

Figure 4-3 Selecting the server for NFS



4. Click **Next**. In the **Features** page, select **Client for NFS** and click **Next**, as shown in **Figure 4-4**. Confirm the settings and then click **Install**. If you install the NFS client for the first time, after the installation is complete, restart the client and log in to the ECS again as prompted.

Figure 4-4 Selecting the NFS client

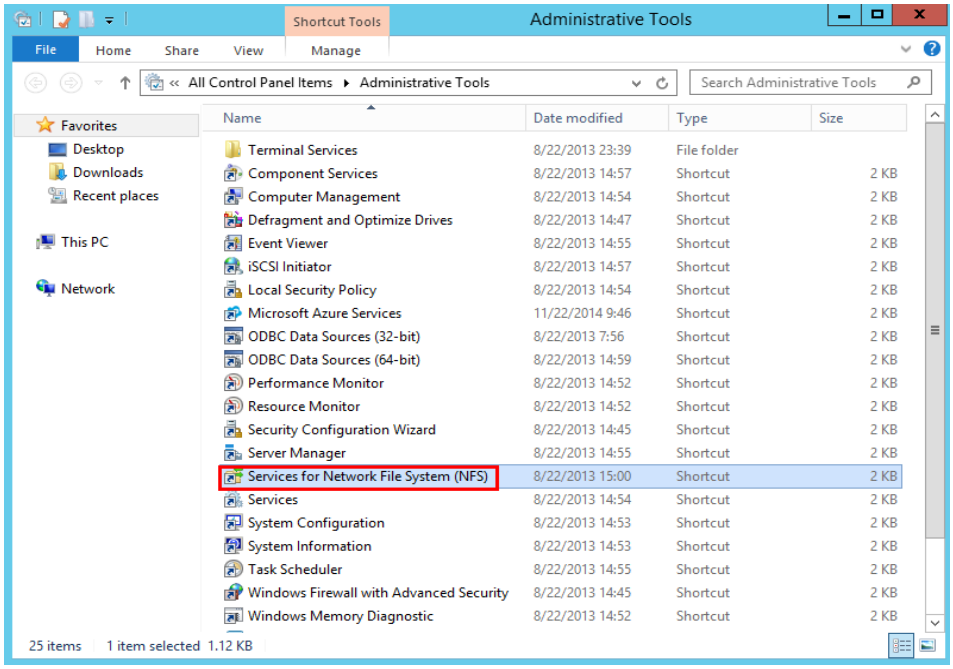


Step 4 Modify the NFS transfer protocol.

1. Choose **Control Panel** > **System and Security** > **Administrative Tools** > **Services for Network File System (NFS)**, as shown in **Figure 4-5**.

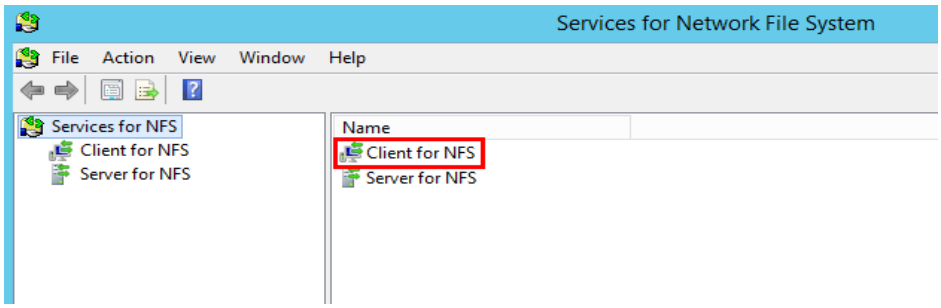
 Copyright © Huawei Technologies Co., Ltd.

Figure 4-5 Administrative tools



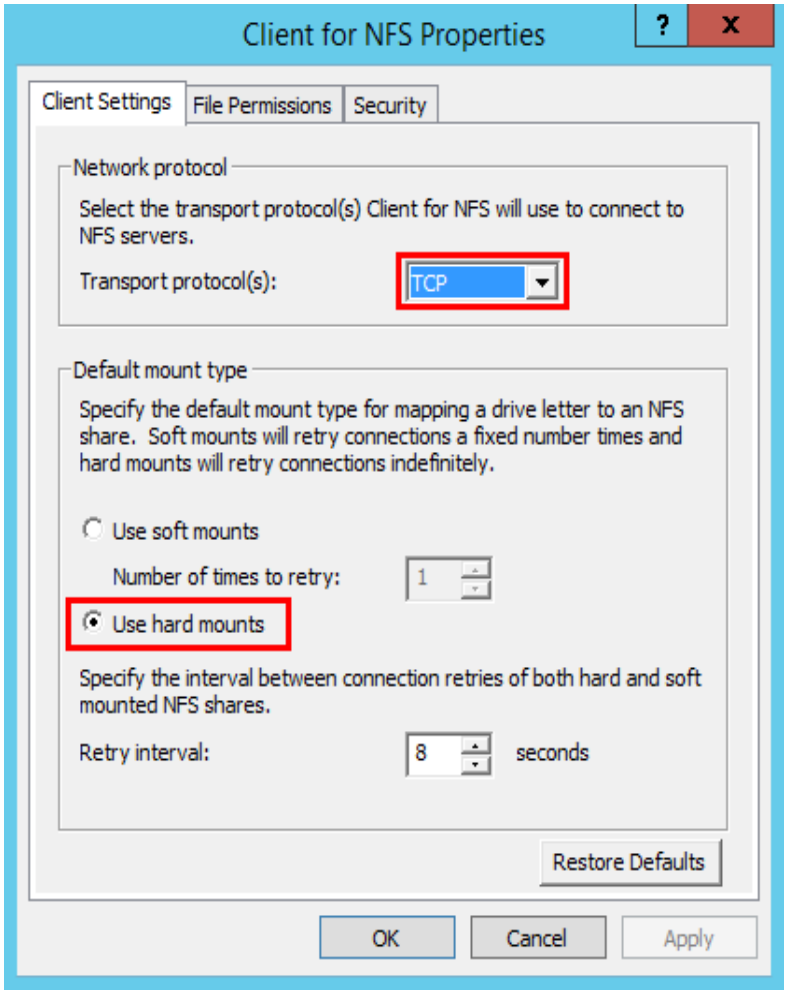
2. Right-click **Client for NFS**, choose **Properties**, change the transport protocol to **TCP**, and select **Use hard mounts**, as shown in **Figure 4-6** and **Figure 4-7**.

Figure 4-6 Services for NFS



 Copyright © Huawei Technologies Co., Ltd.

Figure 4-7 Client for NFS properties



Step 5 Run the following command in the Command Prompt of the Windows Server 2012 (**X** is the drive letter of the free disk). Select the ECS that is in the same VPC as the file system to mount the file system.

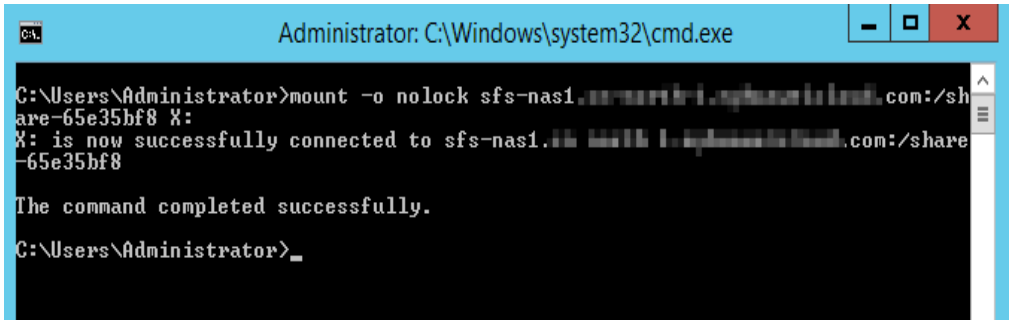
NOTE

- Free drive letter of the disk: A drive letter that is not in use, such as drive letter E or X.

You can move the cursor to the mount point and click next to the mount point to copy the mount point. If the information shown in **Figure 4-8** is displayed, the mounting is successful.

 Copyright © Huawei Technologies Co., Ltd.

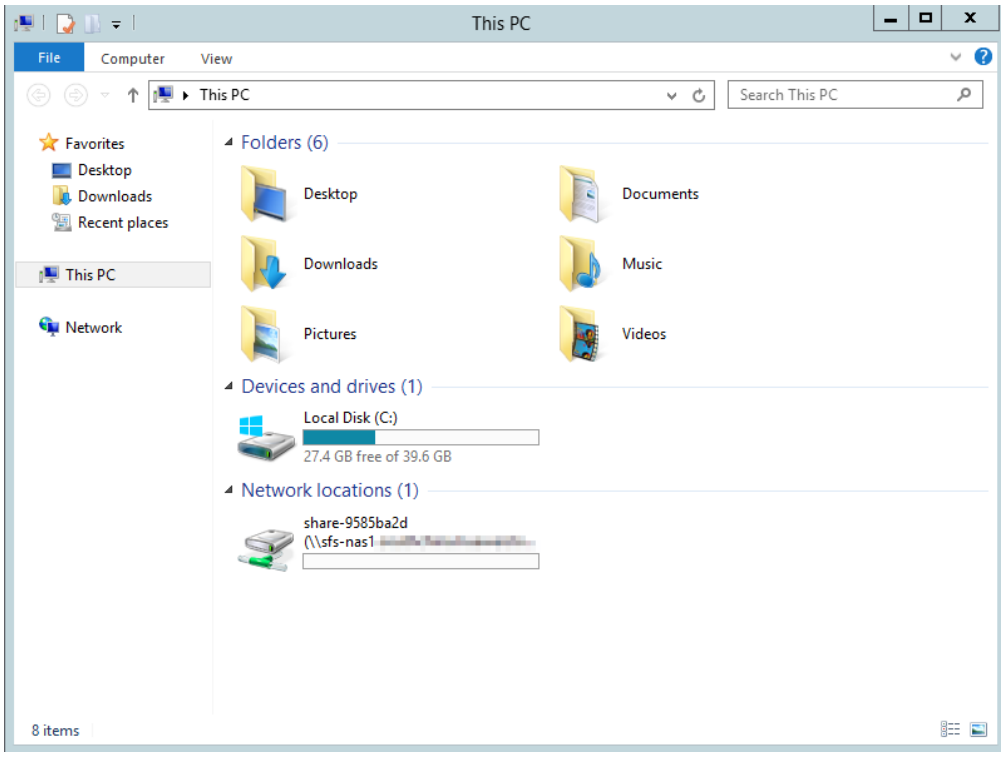
Figure 4-8 Running the command



Step 6 After the file system is mounted successfully, you can view the mounted file system on the **This PC** window, as shown in **Figure 4-9**.

If the mounting fails or times out, rectify the fault by referring to **Troubleshooting**.

Figure 4-9 Successful mounting



NOTE

To distinguish different file systems mounted on an ECS, you can rename file systems by right-clicking a file system and choose **Rename**.

----End

 Copyright © Huawei Technologies Co., Ltd.

4.3 Mounting an SFS Turbo File System to Windows

After creating a file system, you need to mount it to cloud servers so that they can share the file system.

This section uses Windows Server 2019 as an example to describe how to mount an SMB SFS Turbo file system to ECSs.

NOTE

You need to **submit a service ticket** to apply for using the SMB protocol.

Operations on BMSs are the same as those on .

To simply mount a file system, see **Mounting an SMB File System in Windows**.

To mount a file system as an Active Directory (AD) domain user, perform the following steps:

Step 1: **Adding an SMB File System to an AD Domain**

Step 2: **Mounting and Using an SMB File System on a Windows ECS as an AD Domain User**

Step 3: **Managing ACLs of an SMB File System**

Constraints

Constraint	Description
File system functions	SMB file systems do not support OBS or NAS storage backends. A file system can use either NFS or SMB. It cannot use both protocols. When restoring data from a file system backup, the file system protocol cannot be changed. In another word, a backup of an NFS file system cannot be used to create an SMB file system, and a backup of an SMB file system cannot be used to create an NFS file system. SMB file systems do not support multi-VPC access.

 Copyright © Huawei Technologies Co., Ltd.

Constraint	Description
SMB protocol functions	• Extended attributes are not supported. • IOCTL or FSCTL operations such as sparse files, file compression, NIC status queries, and reparse points are not supported. • Alternate data streams (ADS) are not supported. • LDAP authentication is not supported. • Direct, SMB Multichannel, and SMB Directory Leasing are not supported. • Change Notify is not supported. • Symbolic links and hard links are not supported. • Locks (including OpLock, OpenLock, BRL, and Lease) and Persistent File Handle are not supported.
SMB protocol version	SMB 2.0, SMB 2.1, and SMB 3.0 are supported.
SMB client	On all compute nodes to which a file system is mounted and for all users who use the shared file system, a specific file or directory can have up to 10,000 active file handles.

Mounting an SMB File System in Windows

Step 1 Prepare the environment. Perform this step only once on each Windows ECS where you want to mount the file system. Do not perform it for each mount.

1. Enable the Workstation service. Normally, Workstation is enabled by default.
   a. Choose **All Programs** > **Accessories** > **Run** or press **Win+R** and then enter **services.msc** to access the local services.
   b. Find Workstation and check that its status is **Running** and startup type is **Automatic**.

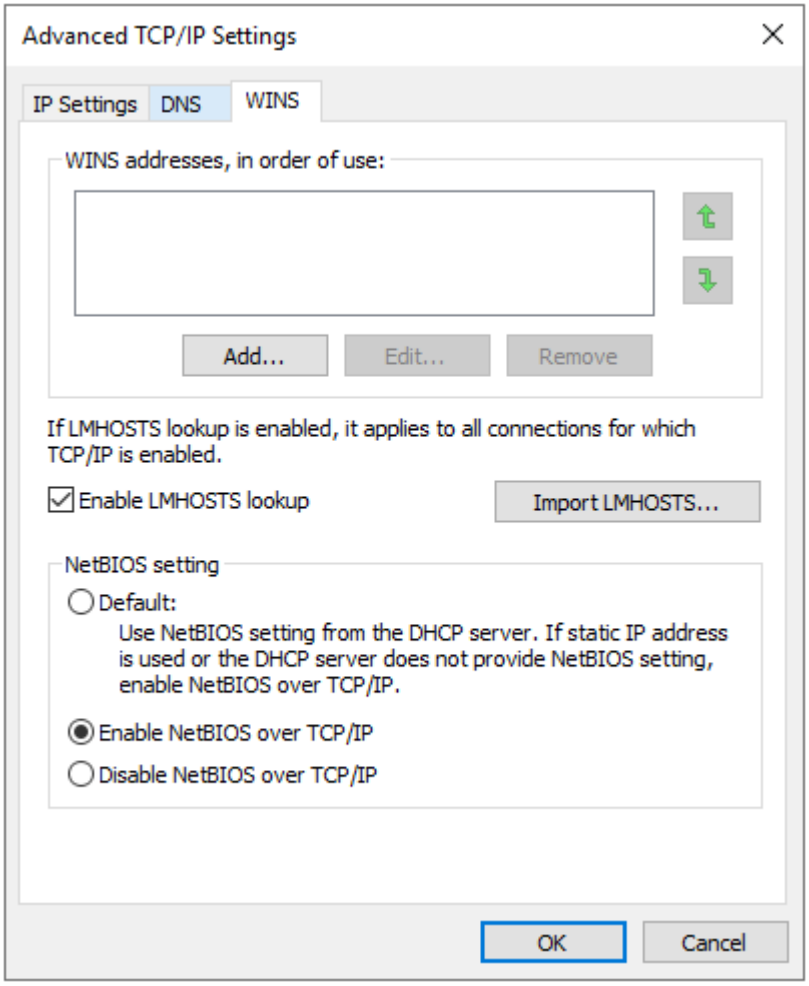
 Copyright © Huawei Technologies Co., Ltd.

Figure 4-10 Services (Local) > Workstation

2. Enable TCP/IP NetBIOS Helper. Normally, TCP/IP NetBIOS Helper is enabled by default.
   a. Open Network and Sharing Center and click the network that the ECS is connected to.
   b. Click **Properties**. On the displayed page, double-click **Internet Protocol Version 4 (TCP/IPv4)**. Then, click **Advanced**.
   c. In the displayed dialog box, choose **WINS** > **Enable NetBIOS over TCP/IP**, and click **OK**.

 Copyright © Huawei Technologies Co., Ltd.

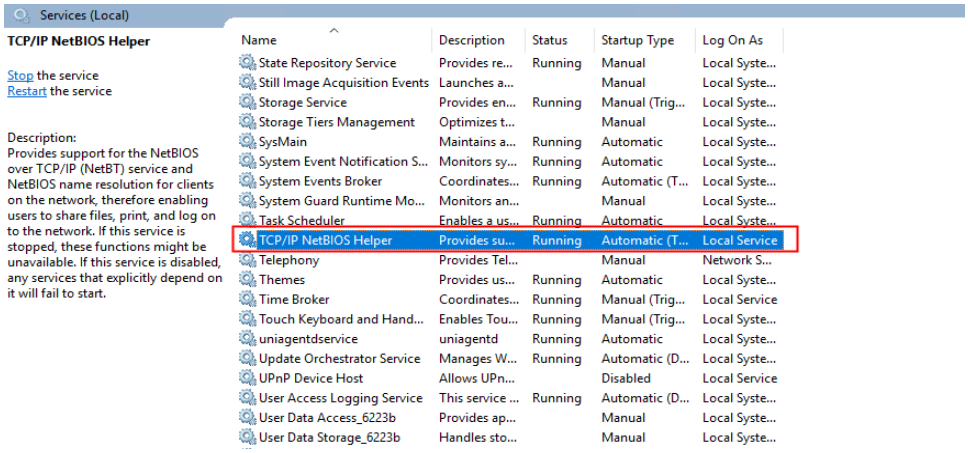
Figure 4-11 Enable NetBIOS over TCP/IP



d. Choose **All Programs** > **Accessories** > **Run** or press **Win+R** and then enter **services.msc** to access the local services.

e. Find TCP/IP NetBIOS Helper and check that its status is **Running** and startup type is **Automatic**.

Figure 4-12 Services (Local) > TCP/IP NetBIOS Helper



Step 2 Mount the SMB file system.

 Copyright © Huawei Technologies Co., Ltd.

1. Open Command Prompt and run the following command to mount the SMB file system:

```
#Guest authentication
net use X: \\huawei.com\share
#Anonymous authentication
net use X: \\huawei.com\share "" /user:
#AD domain authentication
net use X: \\huawei.com\share  PASSWORD /user: example.com\USERNAME
```

Table 4-3 Mount parameters

Parameter	Description
X	The drive letter on the Windows OS to be used for mount. If letter X has been used or there are multiple mounted NAS file systems, use another letter.
huawei.com	The mount address automatically generated when you create an SMB file system. Replace it with the actual address.
share	The name of the SMB file system, which cannot be changed.
example.com	The domain name of the AD domain server.
USERNAME	The name of the AD domain user.
PASSWORD	The password of the AD domain user.

NOTE

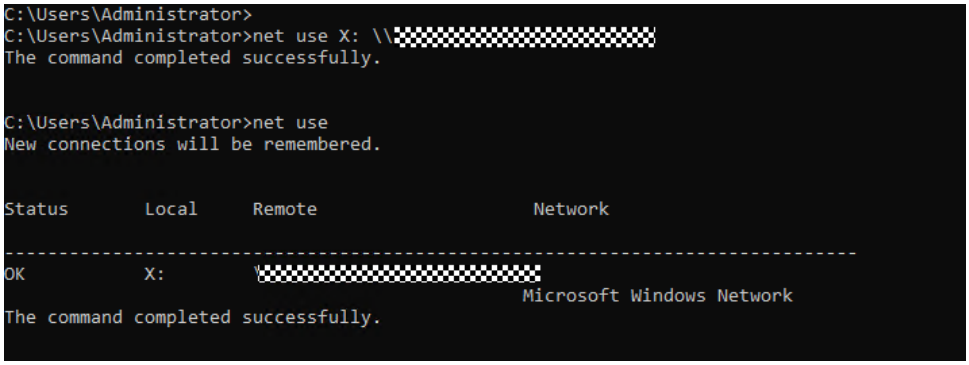
Guest authentication and anonymous authentication are only used when the file system is not added to a domain. If the file system is added to a domain, unmount the current mount and use AD domain authentication. If the file system is then removed from the domain, unmount the mount and wait for about 30 seconds before mounting it again. Anonymous authentication is recommended then.

2. Check that the file system has been mounted.

```
net use
```

If information similar to **Figure 4-13** is returned, the file system has been mounted. You can read data from or write data to the SMB file system on the ECS.

Figure 4-13 Mount command

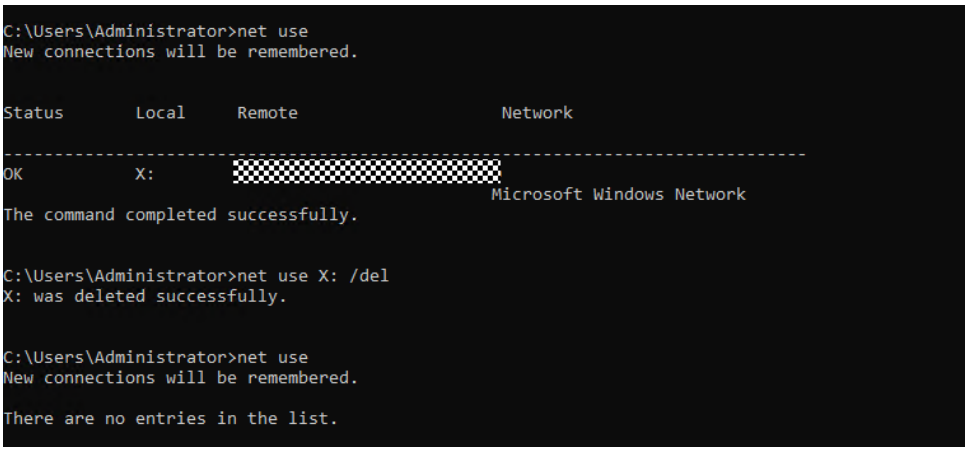


 Copyright © Huawei Technologies Co., Ltd.

3. Unmount as needed.

```
#Unmounting a specific mount
net use X: /del
#Unmounting all mounts
net use * /del
```

Figure 4-14 Unmount command



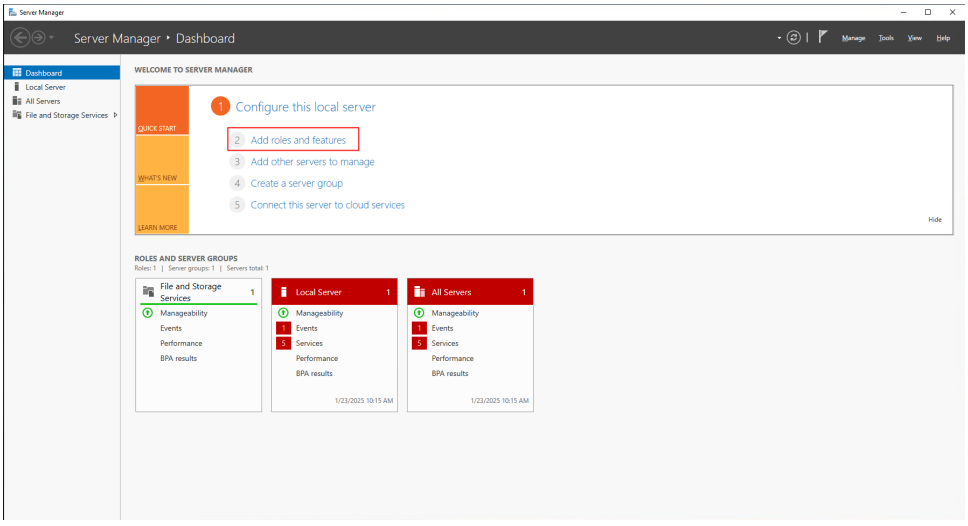
----End

Adding an SMB File System to an AD Domain

Step 1 Set up an AD domain server. A Windows ECS that is in the same VPC as the SMB file system is required. In this example, a server running Windows Server 2019 Standard Edition is used as an example.

1. Log in to the Windows ECS.
2. In the search box in the lower left corner of the desktop, search for **Server Manager** to open Server Manager.
3. Choose **Dashboard** > **Add roles and features**.

Figure 4-15 Add roles and features



 Copyright © Huawei Technologies Co., Ltd.

4. On the Add Roles and Features Wizard, choose **Installation Type** > **Role-based or feature-based installation** and click **Next**. Then, choose **Server Selection** > **Select a server from the server pool** and click **Next**.

Figure 4-16 Selecting **Role-based or feature-based installation**

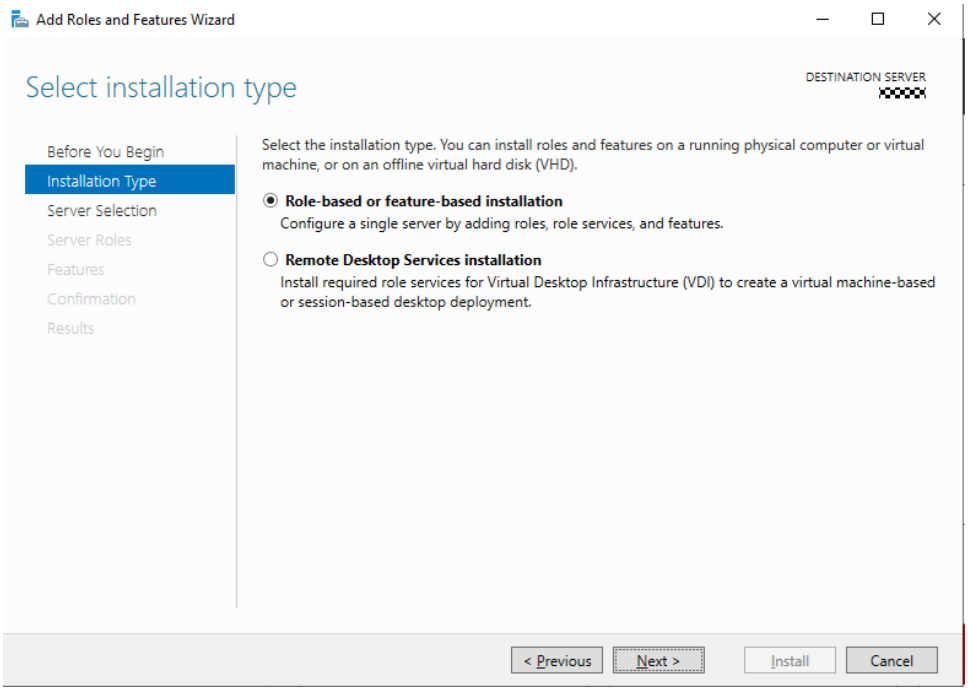
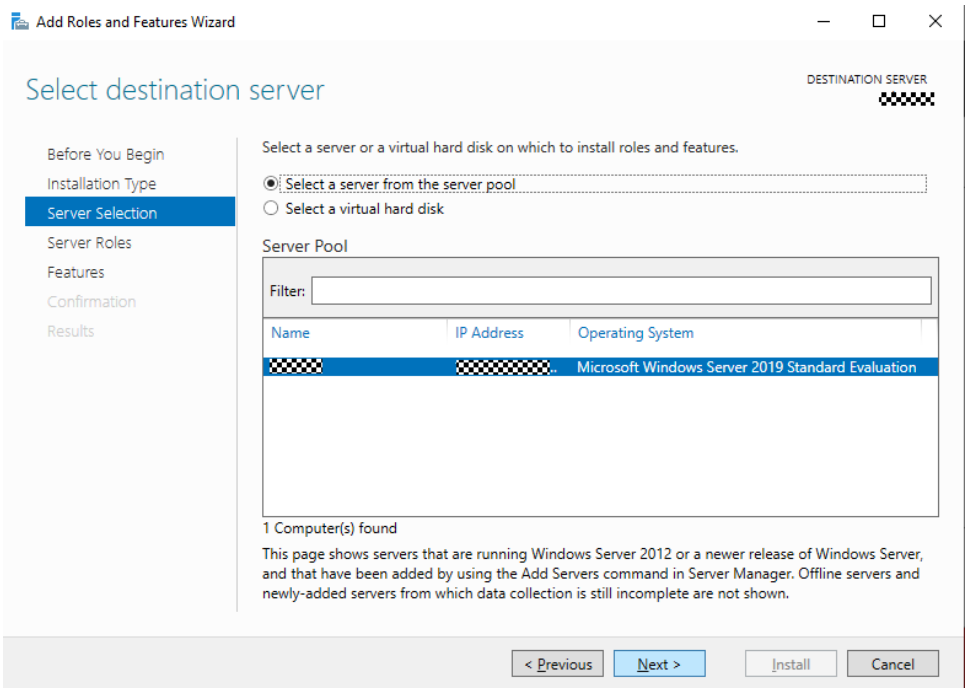


Figure 4-17 Selecting **Select a server from the server pool**



5. Select **Active Directory Domain Services**, click **Next**, and then click **Install**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 4-18 Selecting **Active Directory Domain Services**

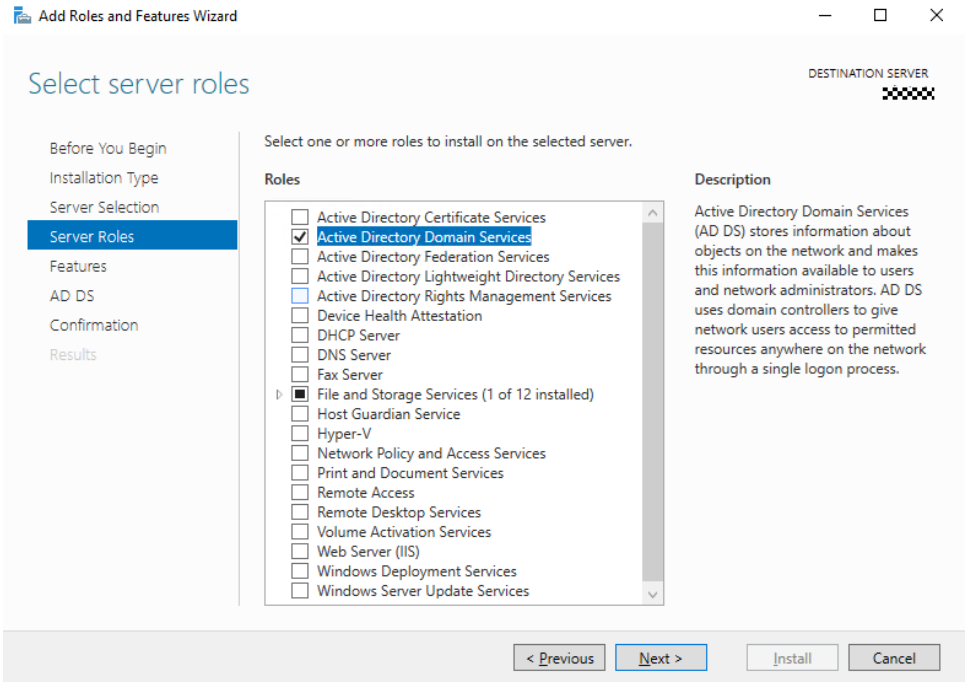
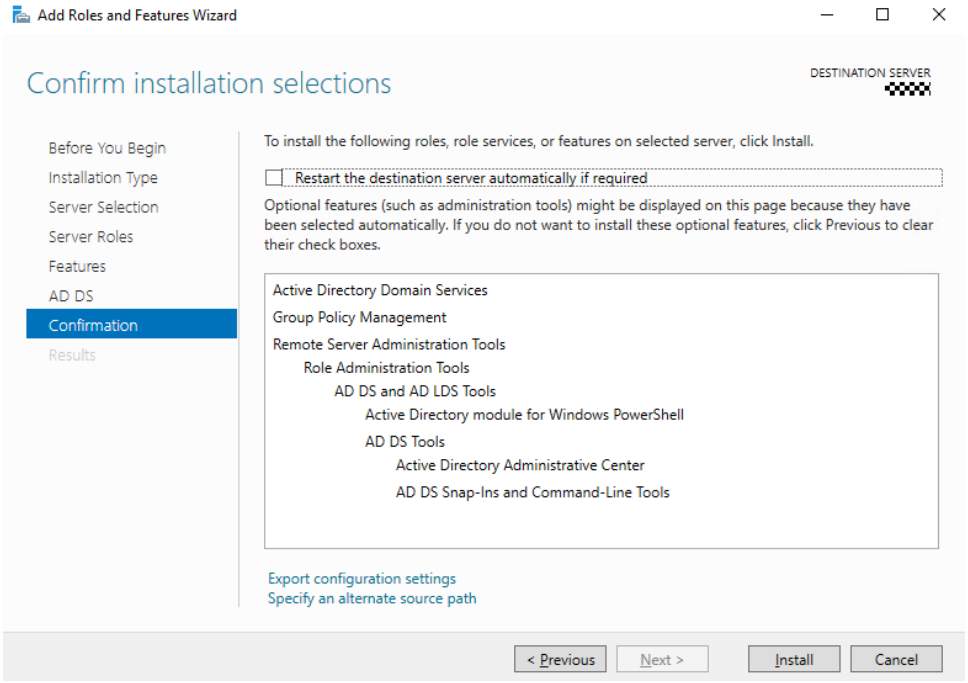


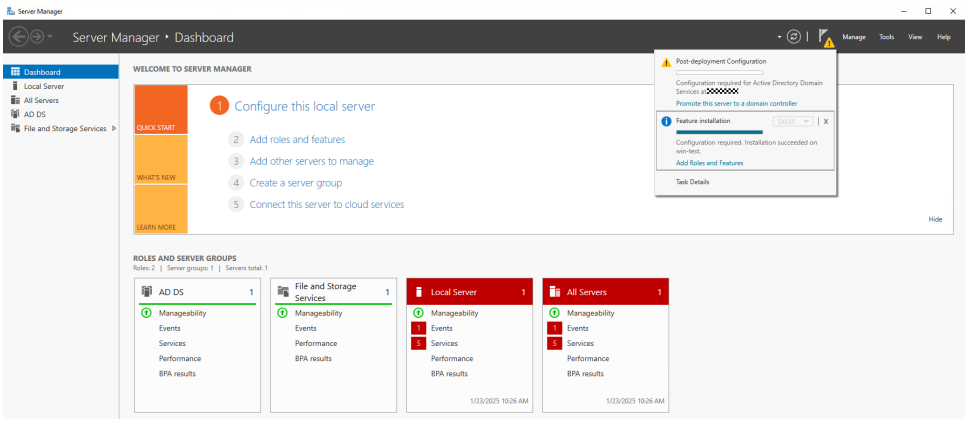
Figure 4-19 Confirm installation selections



6. After the installation is complete, click the task icon in the upper right corner of Server Manager and click **Promote this server to a domain controller**.

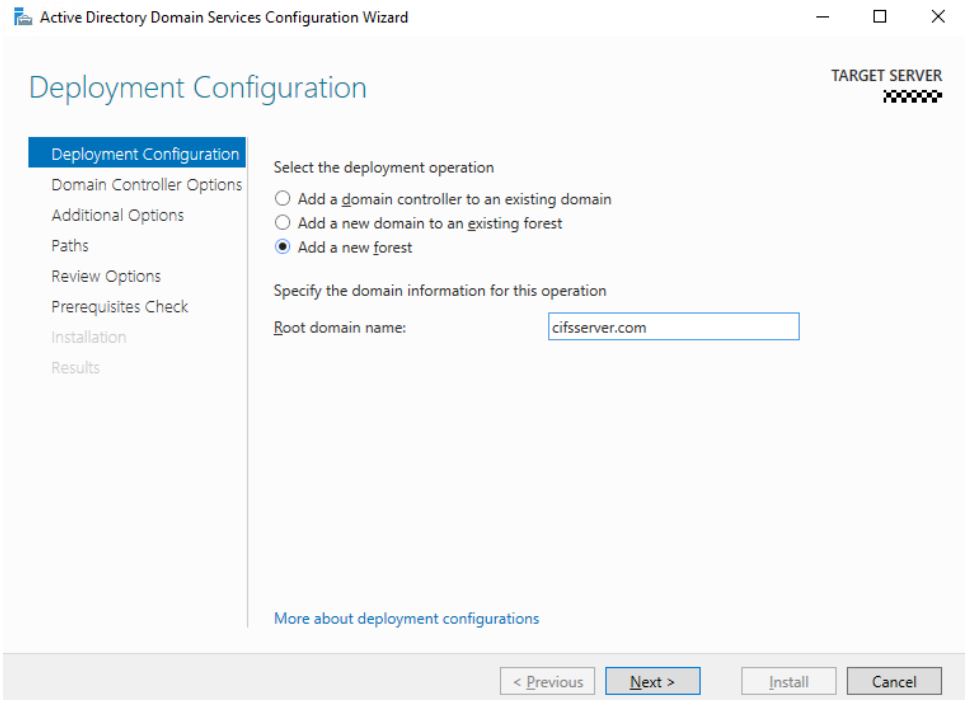
 Copyright © Huawei Technologies Co., Ltd.

Figure 4-20 Server Manager > Promote this server to a domain controller



7. In the window of Active Directory Domain Services Configuration Wizard, choose **Deployment Configuration** > **Add a new forest** and enter the domain name in the **Root domain name** text box.

Figure 4-21 Add a new forest



8. Choose **Domain Controller Options** > **Doman Name System (DNS) server**, configure **Type the Directory Services Restore Mode (DSRM) password**, and click **Next** until the **Paths** tab is displayed. Select the AD domain data and log folders.

 Copyright © Huawei Technologies Co., Ltd.

Figure 4-22 Configuring **Type the Directory Services Restore Mode (DSRM) password**

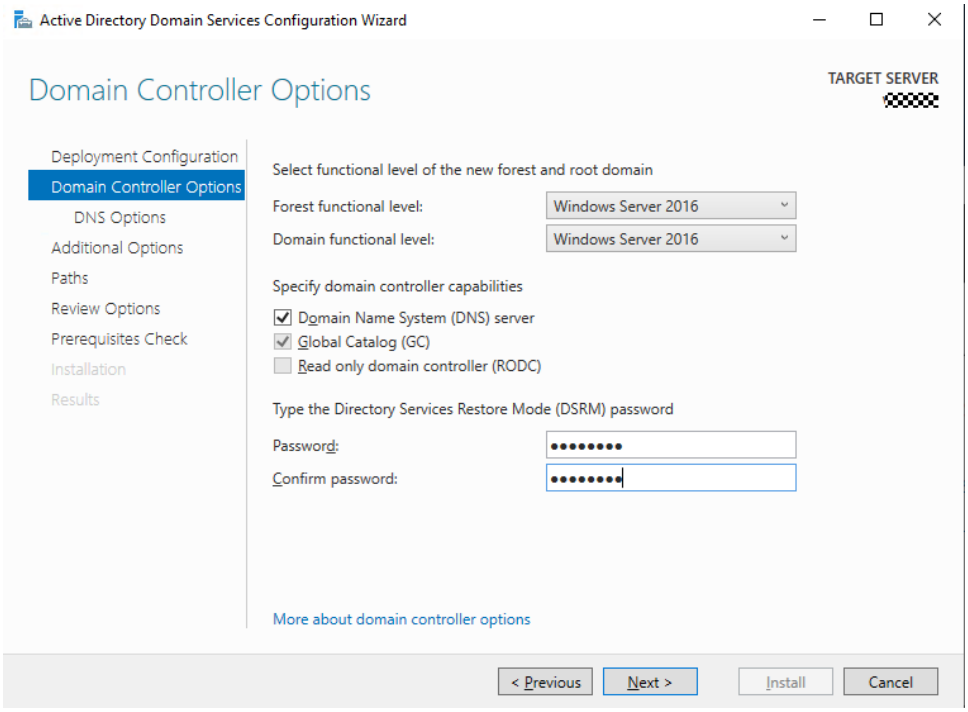
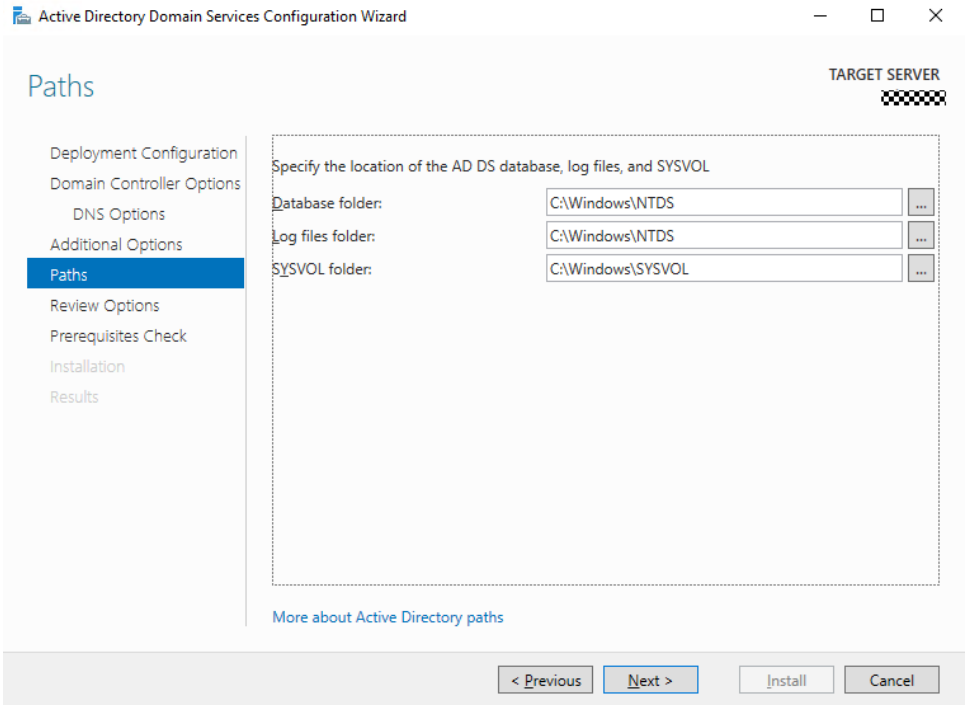


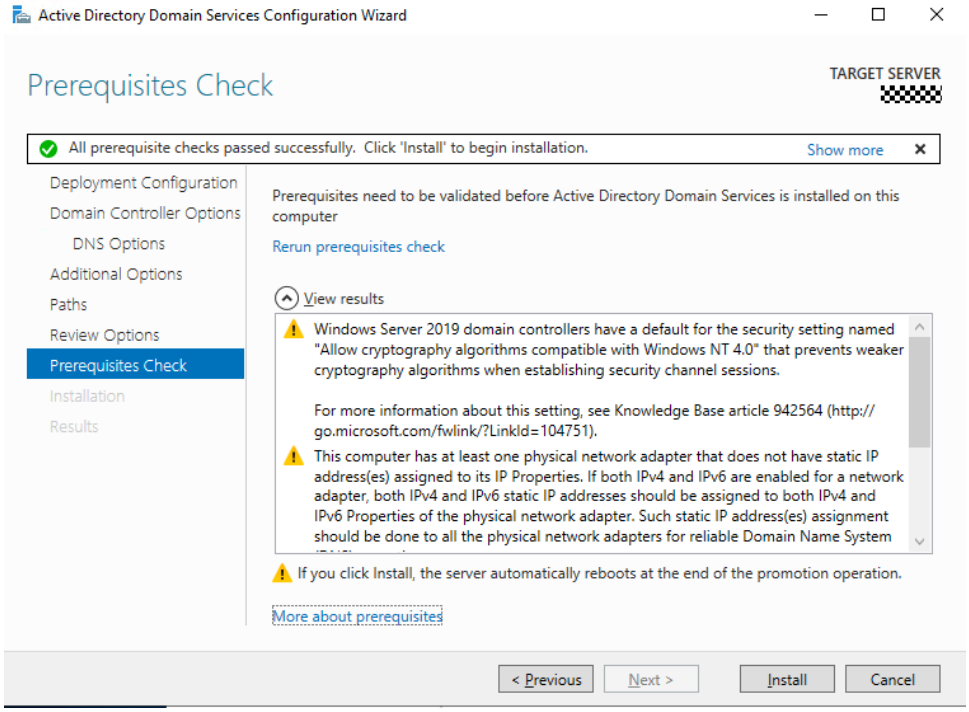
Figure 4-23 Selecting the AD domain data and log folders



9. Click **Next** on the **Review Options** tab, complete the prerequisites check, and click **Install**. After the installation is complete, restart the environment where the AD domain server is located. In this example, restart the ECS.

 Copyright © Huawei Technologies Co., Ltd.

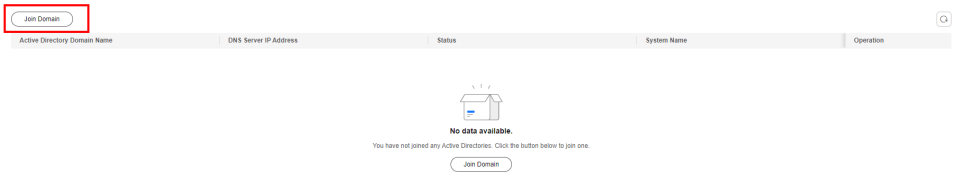
Figure 4-24 Installing the AD domain services



Step 2 Add the file system to the AD domain.

- **The process of joining a domain is as follows:**
  a. Log in to the SFS console.
  b. In the SFS Turbo file system list, find the file system you want to add to a domain and click its name to go to its details page.
  c. On the **Active Directory Configuration** tab, click **Join Domain**.

  Figure 4-25 Active Directory Configuration



  d. Enter the Active Directory configuration information.

 Copyright © Huawei Technologies Co., Ltd.

Figure 4-26 Entering configuration information

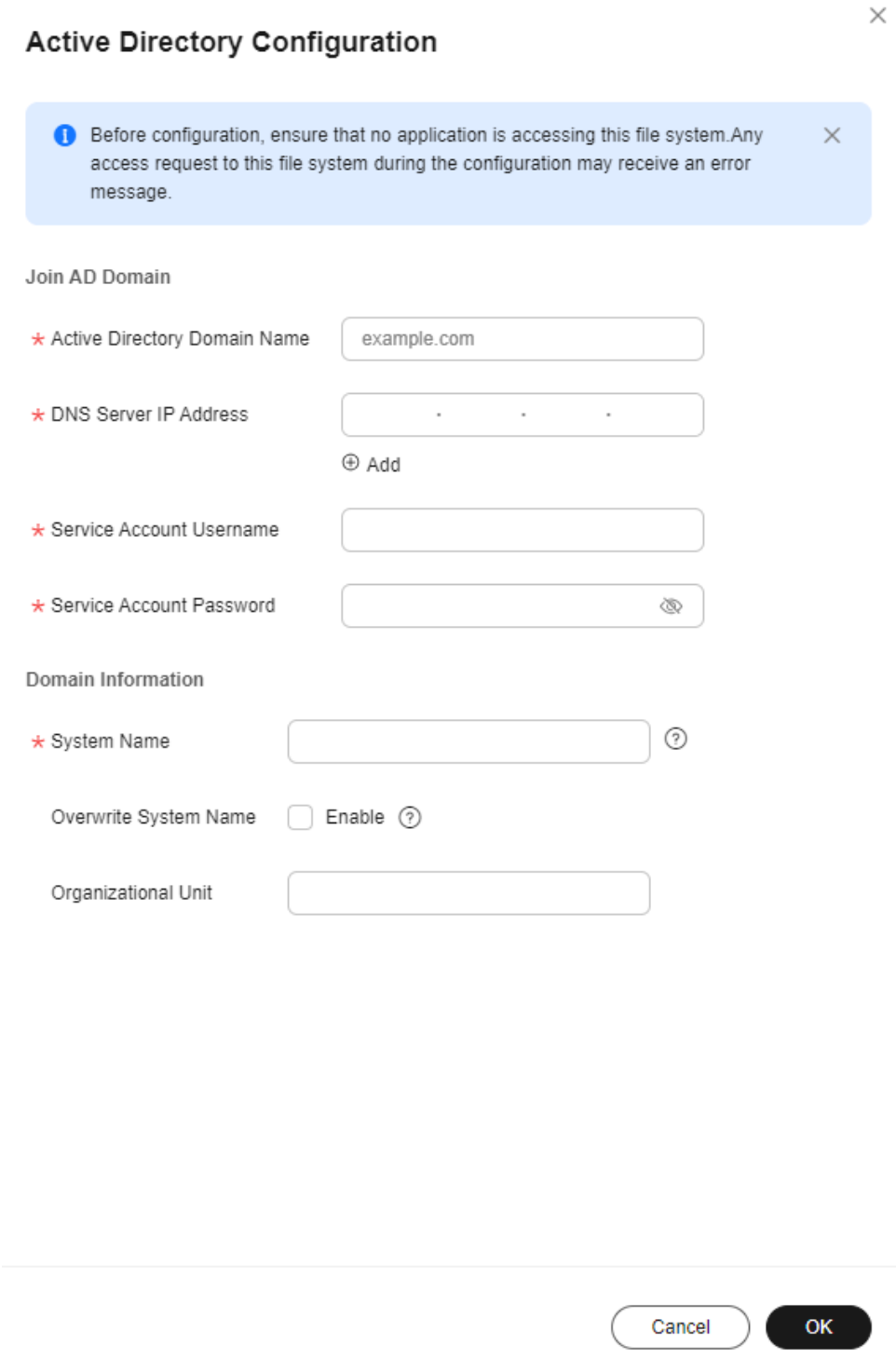


Table 4-4 Parameters required for joining an AD domain

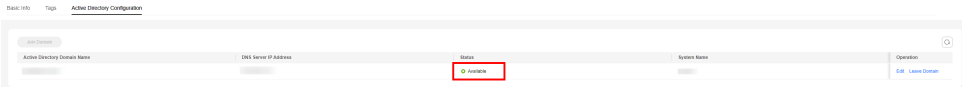
Parameter	Description
Active Directory Domain Name	The name of the AD domain, for example, **example.com**.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
DNS Server IP Address	The IP address of the DNS server that resolves the domain name. You can click **+** to add an alternative DNS server IP address. A maximum of three IP addresses can be added.
Service Account Username	The administrator account of the AD domain server, for example, **administrator**.
Service Account Password	The password of the AD domain server administrator account.
System Name	The unique name of the file system in the AD domain server. If a duplicate name is specified, the file system cannot be added to the domain.
Overwrite System Name	Once enabled, if there is a file system with the same name in the domain controller, the file system you specify will overwrite the one in the domain controller.
Organizational Unit	The unit of the AD domain server that the file system is added to. If not specified, the file system is added to the **Computers** unit, for example, **cn=Computers,dc=example,dc=com**.

e. Wait a few seconds and you can see the Active Directory domain name, DNS server IP address, status, and system name.

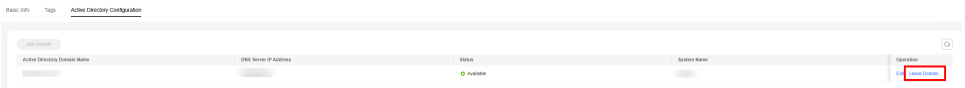
Figure 4-27 Domain joined successfully



- **The process of leaving a domain is as follows:**

  a. Locate the domain that the file system has joined and click **Leave Domain** in the **Operation** column.

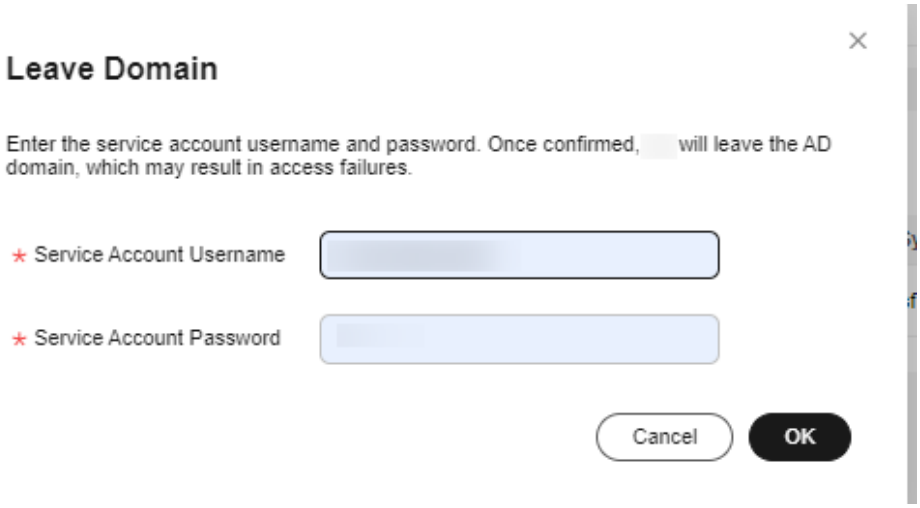
Figure 4-28 Leave Domain button



Copyright © Huawei Technologies Co., Ltd.

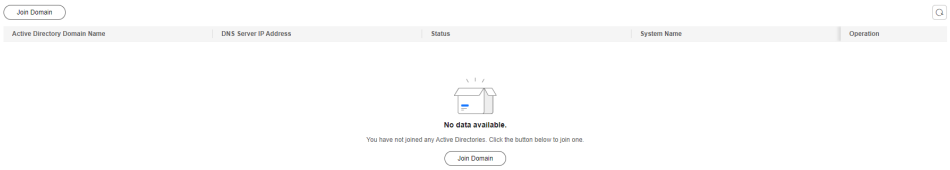
b. Enter the username and password of the AD domain account, and click **OK**.

Figure 4-29 Page for entering the username and password to leave the domain



c. Check that the AD domain disappears from the **Active Directory Configuration** page.

Figure 4-30 Domain left successfully



----End

Mounting and Using an SMB File System on a Windows ECS as an AD Domain User

This part describes how to mount an SMB file system as an AD domain user in Windows, how to access the SMB file system as an AD domain user, and how to view and edit the ACL of a file or directory.

Prerequisites: The SMB file system has been added to the AD domain by referring to **Adding an SMB File System to an AD Domain**.

Method 1: Adding a Windows ECS to an AD Domain and Mounting the SMB File System

The following example uses Windows Server 2019 as an example to describe how to add a Windows ECS to an AD domain and mount an SMB file system.

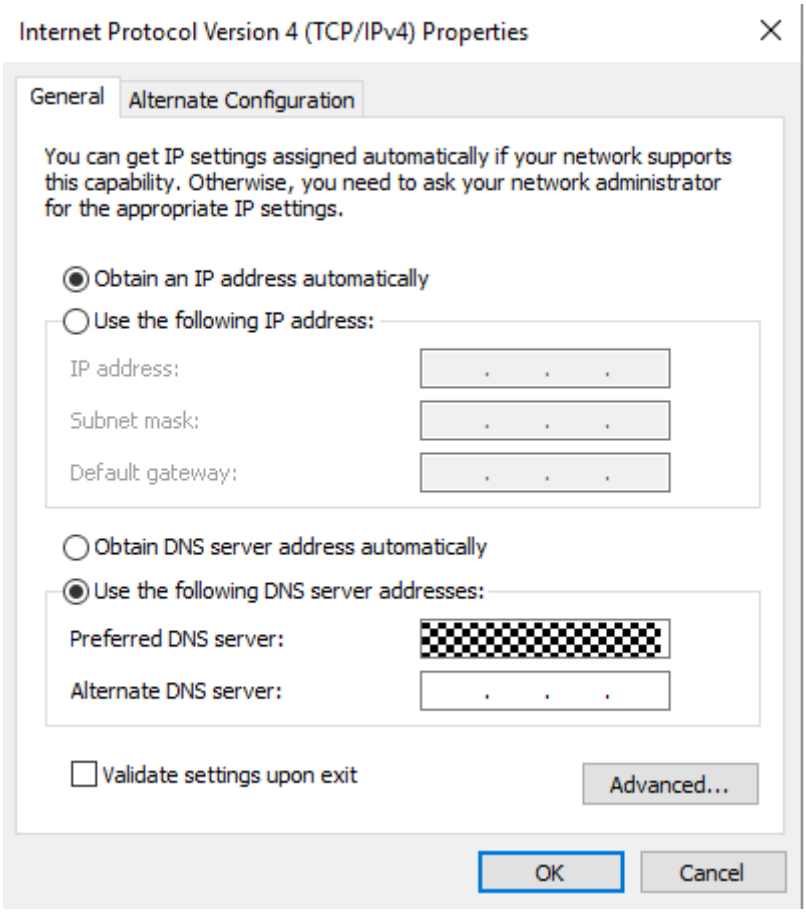
Step 1 Configure the DNS server address on the Windows ECS.

1. Log in to the Windows ECS.
2. In the lower left corner of the desktop, click **Start**.

 Copyright © Huawei Technologies Co., Ltd.

3. On the **Start** menu bar, click **Control Panel**.
4. In the Control Panel, choose **Network & Internet** > **Network and Sharing Center**.
5. Under **View your active networks**, click **Ethernet**.
6. In the displayed dialog box, click **Properties**.
7. Under **This connection uses the following items**, select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.
8. In the displayed dialog box, click **Use the following DNS server addresses** and enter the IP address of the AD domain server.

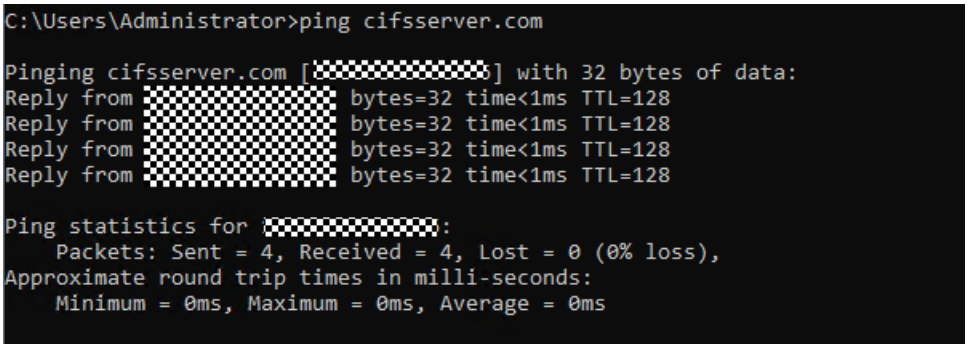
Figure 4-31 Configuring the DNS server IP address



9. Open Command Prompt and ping the AD domain name to check the connectivity between the Windows ECS and the AD domain.

 Copyright © Huawei Technologies Co., Ltd.

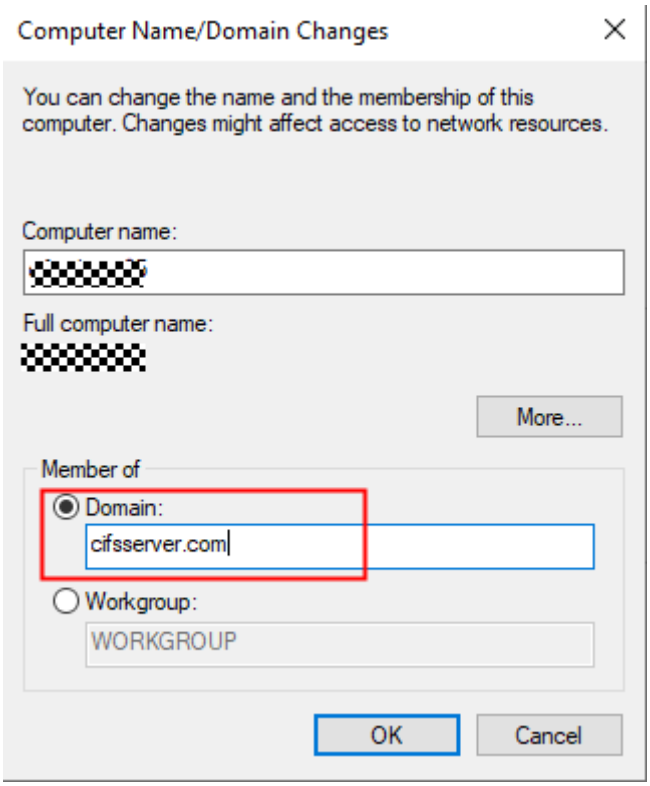
Figure 4-32 Running the ping command



Step 2 Add the Windows ECS to the AD domain.

1. In the Control Panel, choose **System and Security** > **System**.
2. In the **Computer name, domain, and workgroup settings** area, click **Change settings**.
3. In the **System Properties** dialog box, click **Change**.
4. In the **Computer Name/Domain Changes** dialog box, enter the name of the AD domain. Then, click **OK**.

Figure 4-33 Computer Name/Domain Changes dialog box



5. Restart the Windows ECS for the configuration to take effect.

Step 3 Mount the SMB file system.

Log in to the Windows ECS as an AD domain user and run the following command to mount the SMB file system:

```
net use X: \\huawei.com\share /user:example.com\USERNAME PASSWORD
```

 Copyright © Huawei Technologies Co., Ltd.

Table 4-5 Parameters required for mounting an SMB file system

Parameter	Description
huawei.com	The mount address automatically generated when you create an SMB file system. Replace it with the actual address.
share	The name of the SMB file system, which cannot be changed.
example.com	The domain name of the AD domain server.
USERNAME	The name of the AD domain user.
PASSWORD	The password of the AD domain user.

----End

Method 2: Connecting a Windows ECS to the AD Domain Server and Mounting the SMB File System

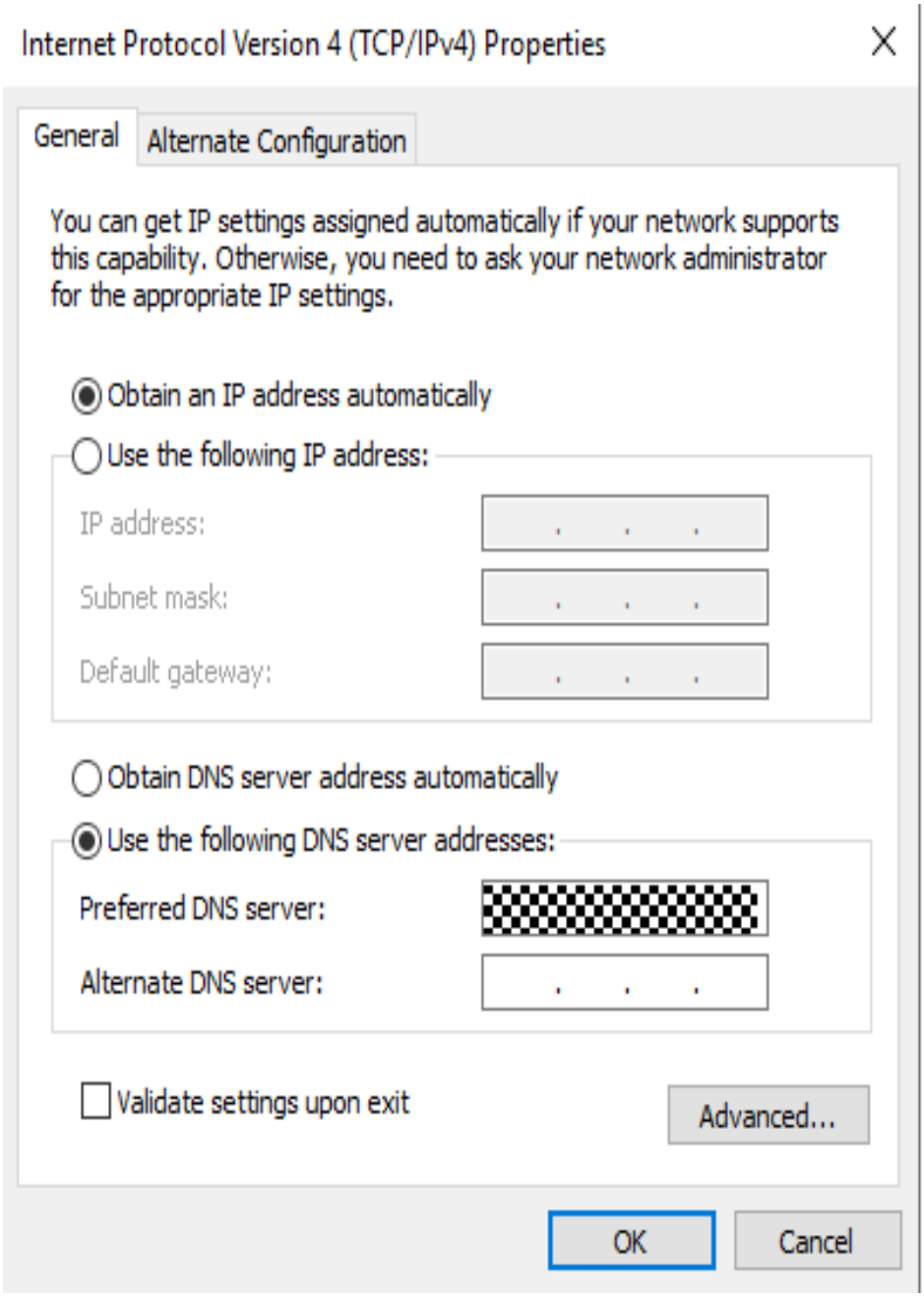
The following example uses Windows Server 2019 as an example to describe how to connect a Windows ECS to an AD domain and mount an SMB file system.

Step 1 Configure the DNS server address on the Windows ECS.

1. Log in to the Windows ECS.
2. In the lower left corner of the desktop, click **Start**.
3. On the **Start** menu bar, click **Control Panel**.
4. In the Control Panel, choose **Network & Internet** > **Network and Sharing Center**.
5. Under **View your active networks**, click **Ethernet**.
6. In the displayed dialog box, click **Properties**.
7. Under **This connection uses the following items**, select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.
8. In the displayed dialog box, click **Use the following DNS server addresses** and enter the IP address of the AD domain server.

 Copyright © Huawei Technologies Co., Ltd.

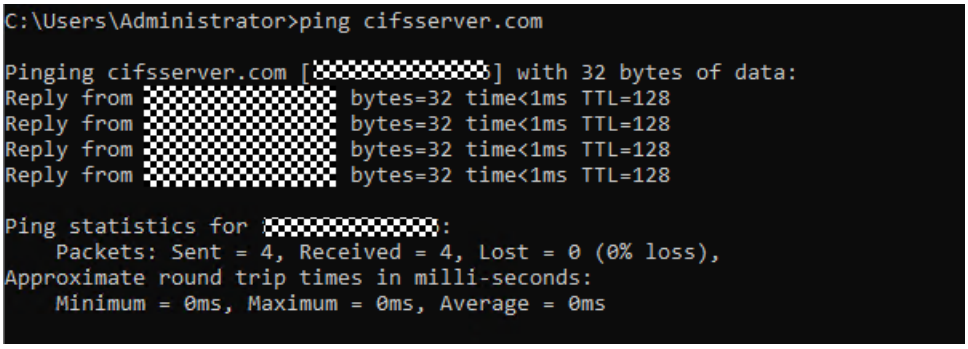
Figure 4-34 Configuring the DNS server IP address



9. Open Command Prompt and ping the AD domain name to check the connectivity between the Windows ECS and the AD domain.

 Copyright © Huawei Technologies Co., Ltd.

Figure 4-35 Running the ping command



Step 2 Mount the SMB file system.

Log in to the Windows ECS as an AD domain user and run the following command to mount the SMB file system:

```
net use X:  \\huawei.com\share /user:example.com\USERNAME PASSWORD
```

Table 4-6 Parameters required for mounting an SMB file system

Parameter	Description
huawei.com	The mount address automatically generated when you create an SMB file system. Replace it with the actual address.
share	The name of the SMB file system, which cannot be changed.
example.com	The domain name of the AD domain server.
USERNAME	The name of the AD domain user.
PASSWORD	The password of the AD domain user.

----End

Managing ACLs of an SMB File System

After you enabled the ACL function and mount an SMB file system as an AD domain user, you can view or edit the ACL of a file or directory using the following methods:

Method 1: Using the mklink Command Line Tool

You can use the mklink command line tool to create a symbolic link for the mounted SMB file system on a Windows local disk to view or edit the ACLs of files or directories.

Step 1 Log in to the Windows ECS.

Step 2 Enter Command Prompt in the search box and open Command Prompt.

Step 3 Run the following command to create a file system mapping:

```
mklink /D C:\myshare \\huawei.com\share
```

 Copyright © Huawei Technologies Co., Ltd.

Table 4-7 Parameter description

Parameter	Description
C:\myshare	The path of the symbolic link.
\\huawei.com\share	The shared path of the SMB file system.

Step 4 After the file system is mapped to a local disk, you can view or edit the ACLs of files or directories on the local disk. For details, see "Method 2: Using Windows File Explorer."

NOTE

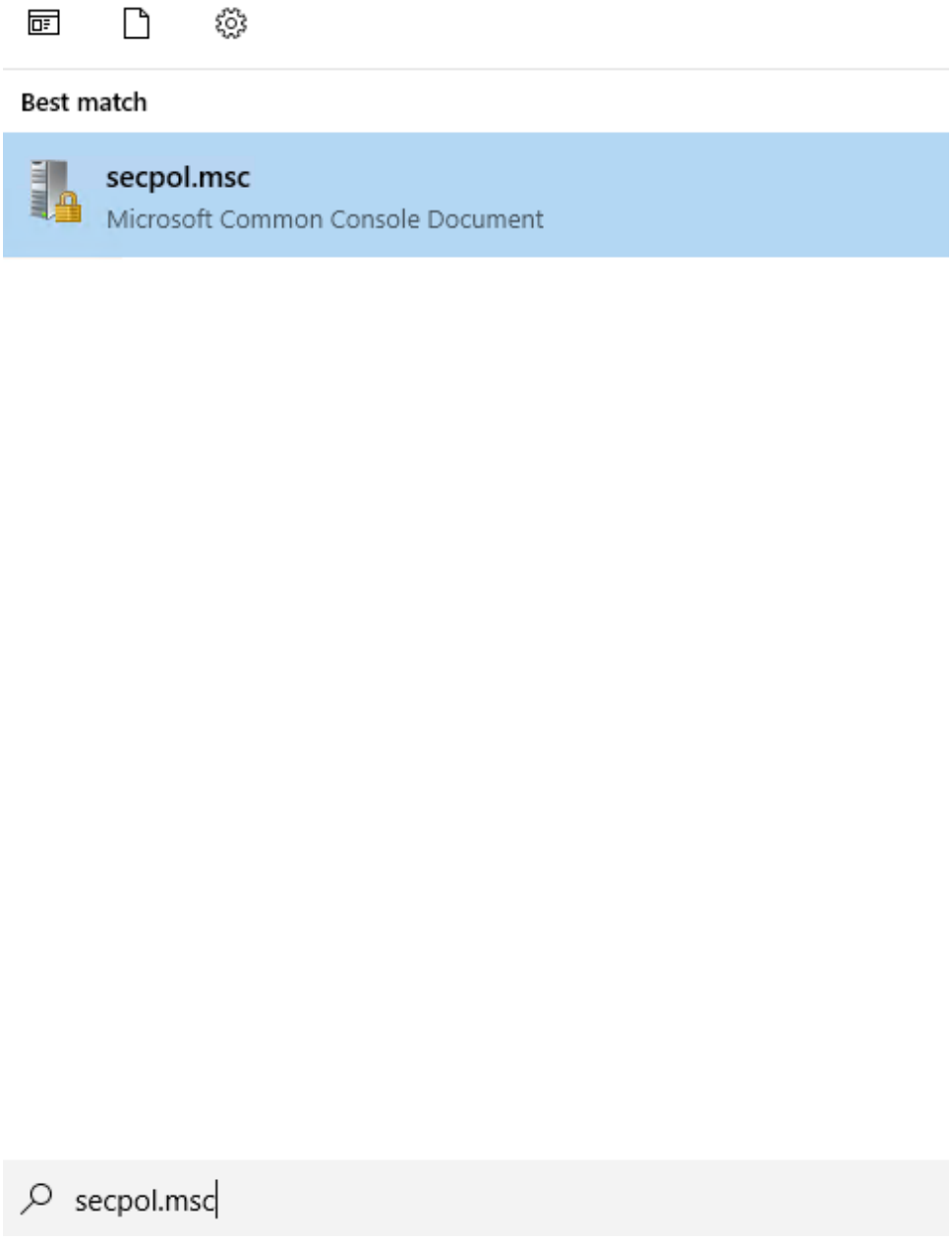
If you are a non-administrator user who does not have permissions to perform this operation. Perform the **next step** to obtain the permissions.

Step 5 Grant a non-administrator user the permissions to use the symbolic link. Skip this step if you are the system administrator.

1. Log in to the Windows ECS as the system administrator.
2. Open the search bar and run secpol.msc.

 Copyright © Huawei Technologies Co., Ltd.

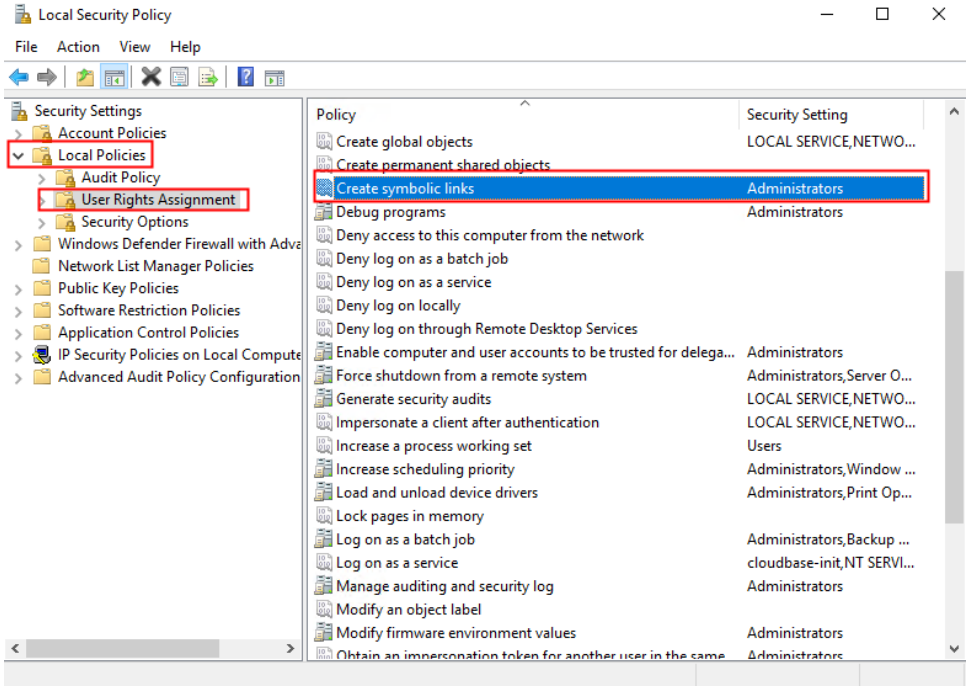
Figure 4-36 Searching for and running secpol.msc



3. In the **Local Security Policy** dialog box, choose **Local Policies** > **User Rights Assignment** and add the user to **Create symbolic links** group policy.

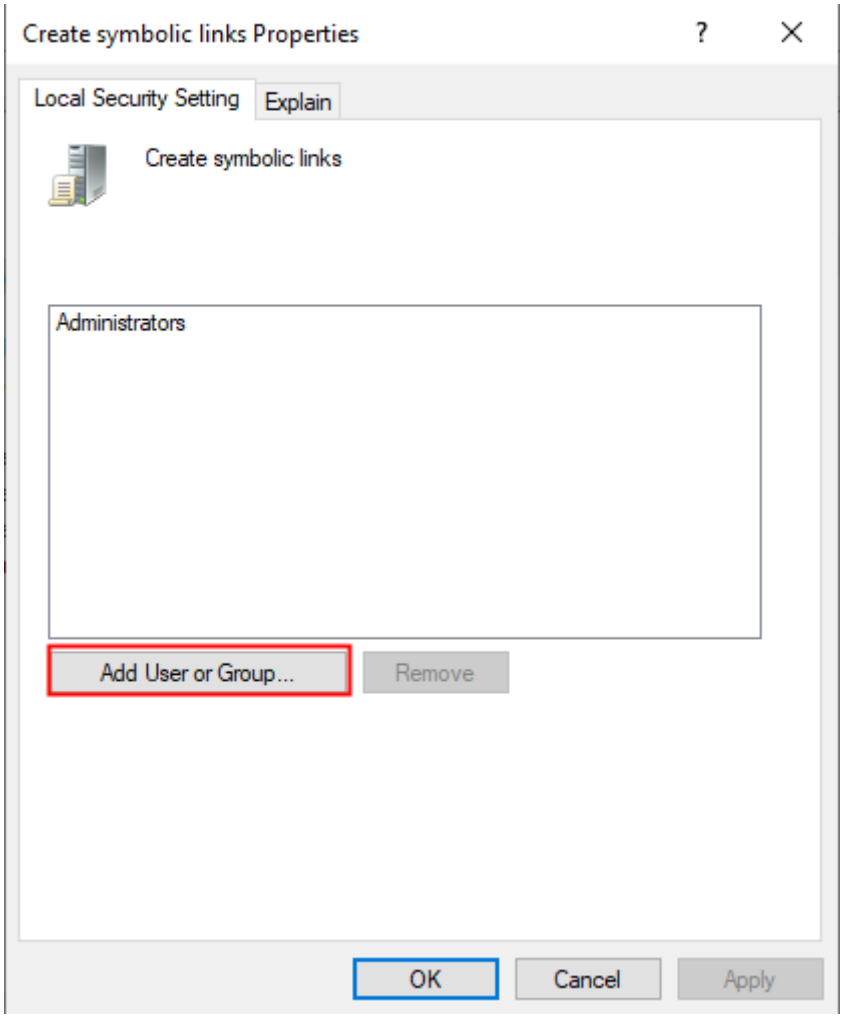
 Copyright © Huawei Technologies Co., Ltd.

Figure 4-37 Local Security Policy dialog box



 Copyright © Huawei Technologies Co., Ltd.

Figure 4-38 Add User or Group



----End

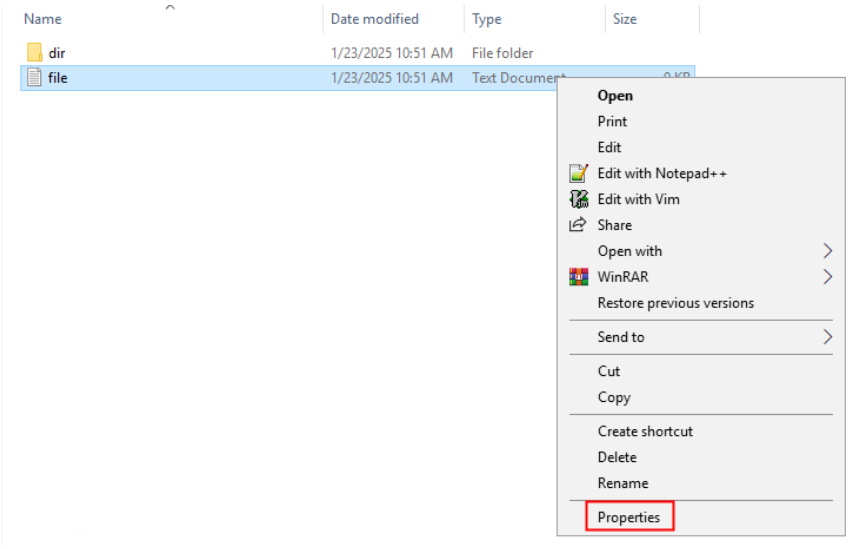
Method 2: Using Windows File Explorer

You can create a symbolic link for the SMB file system on a Windows local disk and view or edit the ACLs of files or directories in Windows File Explorer.

Step 1 Find the target file or directory and right-click **Properties** from the shortcut menu.

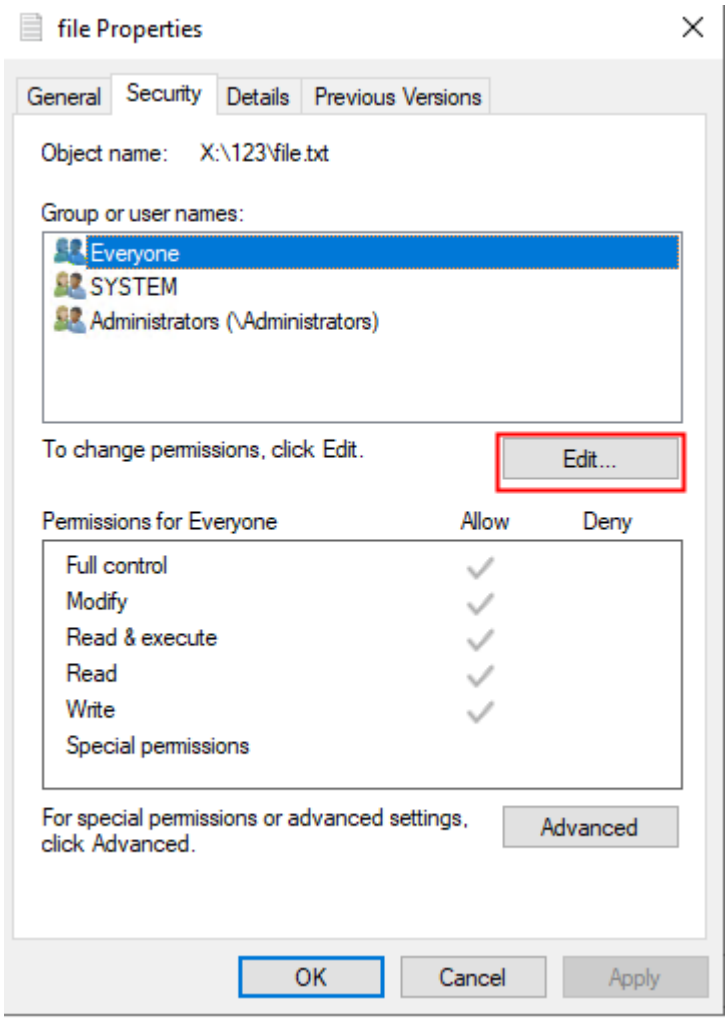
 Copyright © Huawei Technologies Co., Ltd.

Figure 4-39 Choosing **Properties**



Step 2 In the displayed dialog box, click the **Security** tab and then click **Edit**.

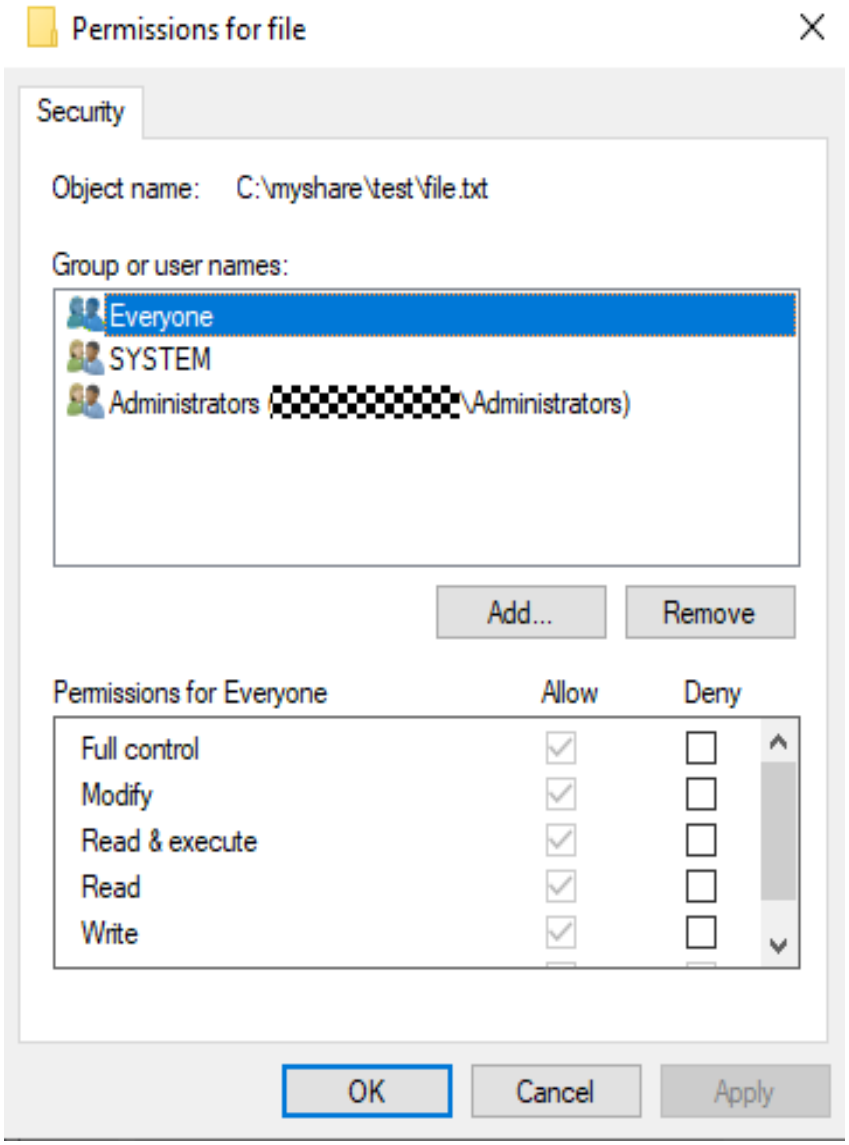
Figure 4-40 Selecting **Edit**



 Copyright © Huawei Technologies Co., Ltd.

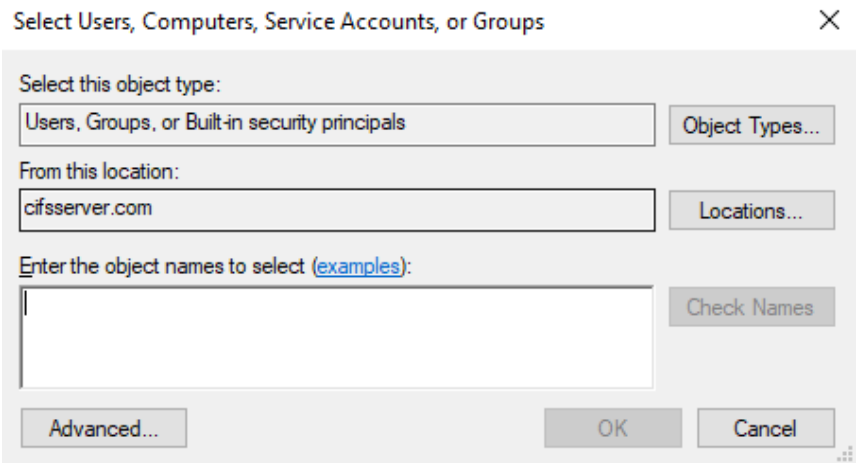
Step 3 In the displayed dialog box, click **Add** and enter information as prompted.

Figure 4-41 Permissions dialog box



 Copyright © Huawei Technologies Co., Ltd.

Figure 4-42 Entering information

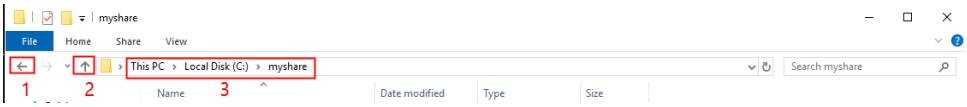


 Copyright © Huawei Technologies Co., Ltd.

NOTE

1. When using Windows File Explorer to view an SMB file system, if you need to revert a disk path, use the Back button (marked with 1 in the following figure) or the Up button (marked with 2 in the following figure). Do not select a part of a path (marked with 3 in the following figure) to revert.

   Figure 4-43 Reverting a local disk path

2. When using Windows File Explorer to access and use an SMB file system, the SMB file system is not added to the AD domain of the user. If you access the file system using the network path **\\huawei.com\share** instead of the local disk path **C:\myshare**, you will fail to configure ACLs because the system cannot determine whether the file system is added to the domain due to unavailable function.

   Figure 4-44 Unable to determine whether the computer is added to the domain

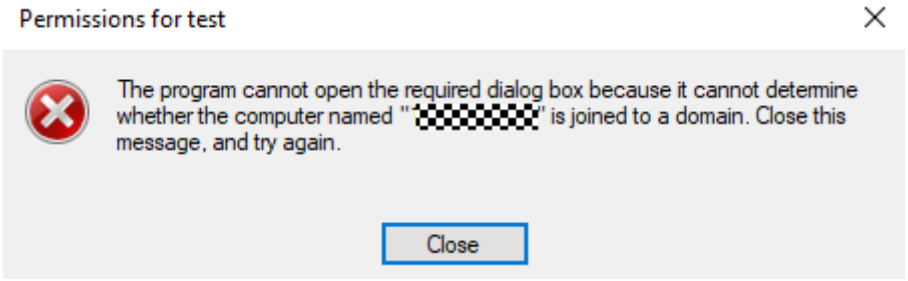
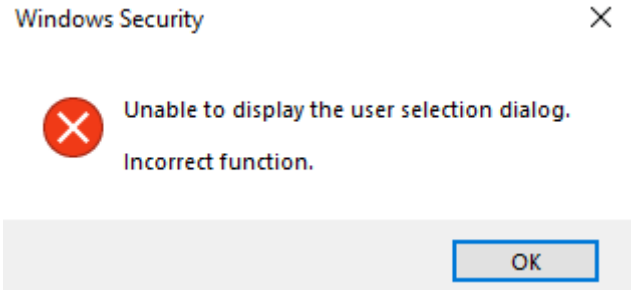
   

   Figure 4-45 Incorrect function

CAUTION

Modifying **C:\myshare** permissions using Windows File Explorer will not modify the permissions of the file system root directory. To modify the permissions on the root directory, use the **Set-Acl Powershell** or **icacls** command.

----End

Method 3: Using the icacls Command

Icacls is a Windows command-line utility that you can use to check or view the ACLs on files or directories.

 Copyright © Huawei Technologies Co., Ltd.

> **NOTE**
>
> Do not modify the ACL of the root directory. Otherwise, the file system may fail to be accessed.
>
> If the ACL of the root directory is maliciously deleted, run the following commands to restore the ACL. **X:** is the drive letter used for mount. If the ACL cannot be edited or root directory cannot be accessed because the everyone permissions are deleted, you need to restore the everyone permissions of the root directory as a super user or AD domain administrator.

```
icacls X:\ /grant BUILTIN\Administrators:(OI)(CI)(F)
icacls X:\ /grant "CREATOR OWNER":(OI)(CI)(IO)(F)
icacls X:\ /grant  "NT AUTHORITY\SYSTEM":(OI)(CI)(F)
icacls X:\ /grant    Everyone:(F)
```

Examples of editing an ACL are as follows:

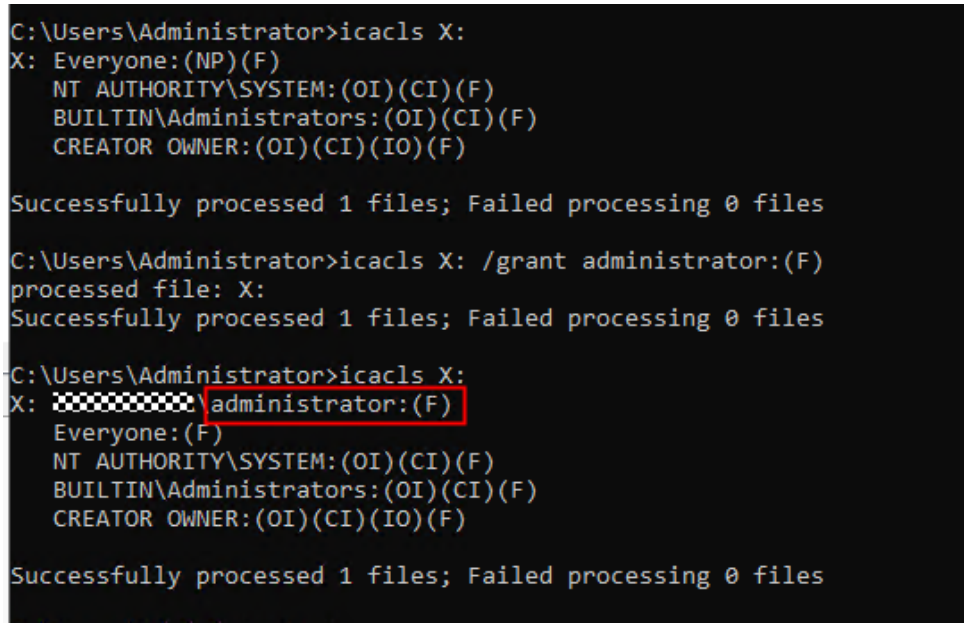
```
#Obtaining the control permission list of the X: directory (the read permission of the directory is required)
icacls X:
#Granting the full control permissions to the user
icacls X: /grant <Username>: (F)
#Granting the full control permissions to the administrator
icacls X: /grant administrator:(F)
#Deleting all permissions of the user
icacls X: /remove <Username>
#Deleting all permissions of everyone
icacls X: /remove everyone
```

Step 1 Log in to the Windows ECS.

Step 2 Enter Command Prompt in the search box and open Command Prompt.

Step 3 Configure the ACL permissions of the file.

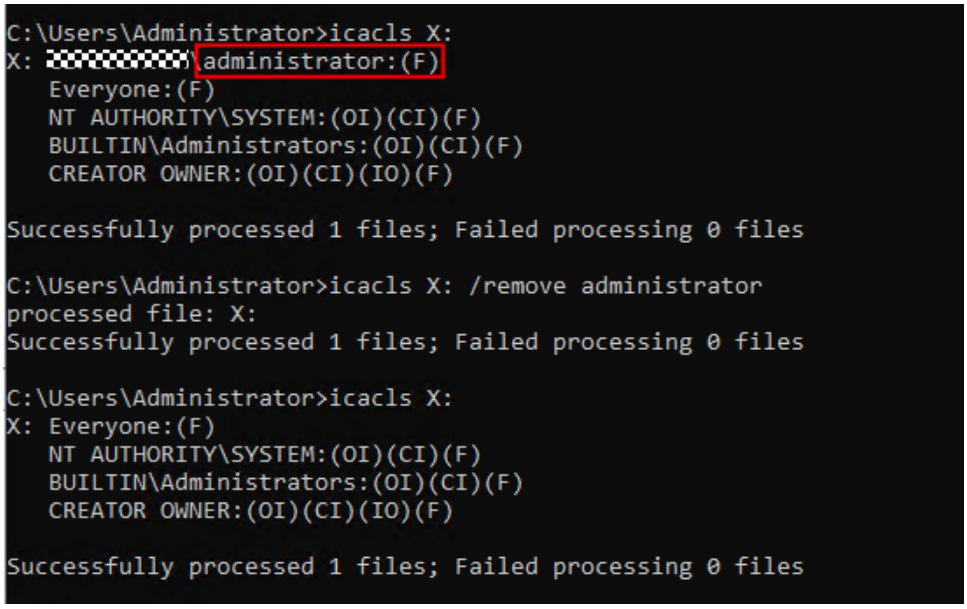
Figure 4-46 Configuring the ACL permissions of the file



Step 4 Remove the ACL permissions of a user.

 Copyright © Huawei Technologies Co., Ltd.

Figure 4-47 Removing the ACL permissions of a user



----End

Method 4: Using PowerShell

Step 1 Log in to the Windows ECS.

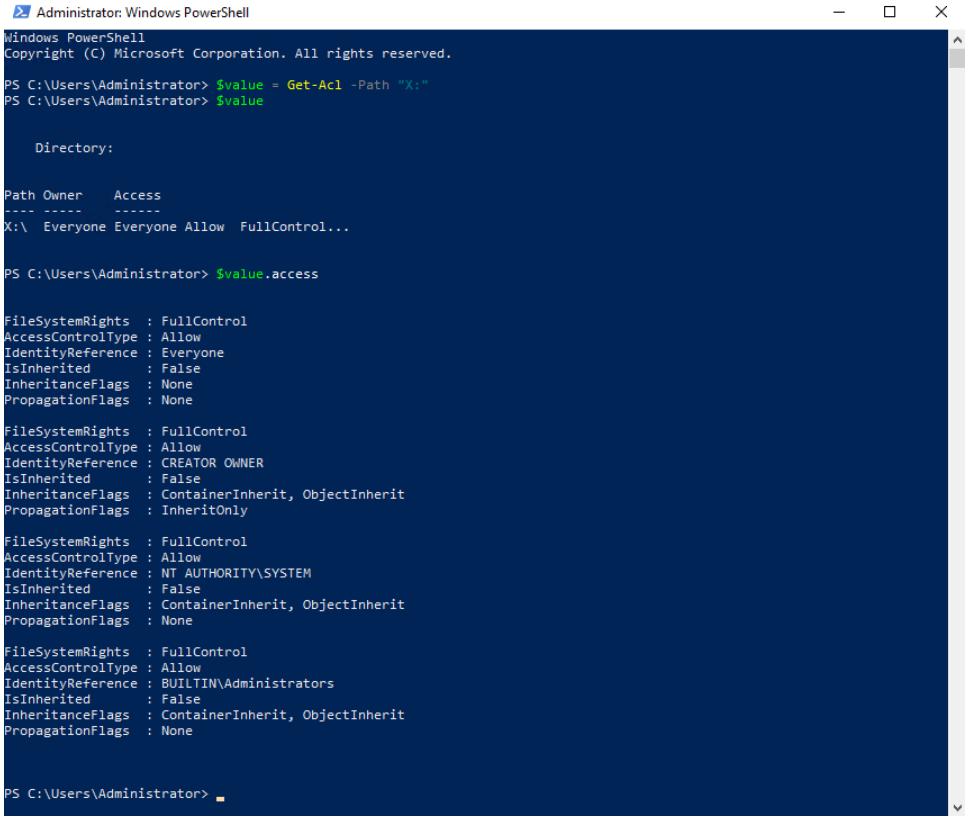
Step 2 In the search box, enter **Windows PowerShell** to open Windows PowerShell.

Step 3 Check the file ACL permissions.

```
#Get properties
$value = Get-Acl -Path "X:"
$value.Access
```

 Copyright © Huawei Technologies Co., Ltd.

Figure 4-48 Checking ACLs using PowerShell

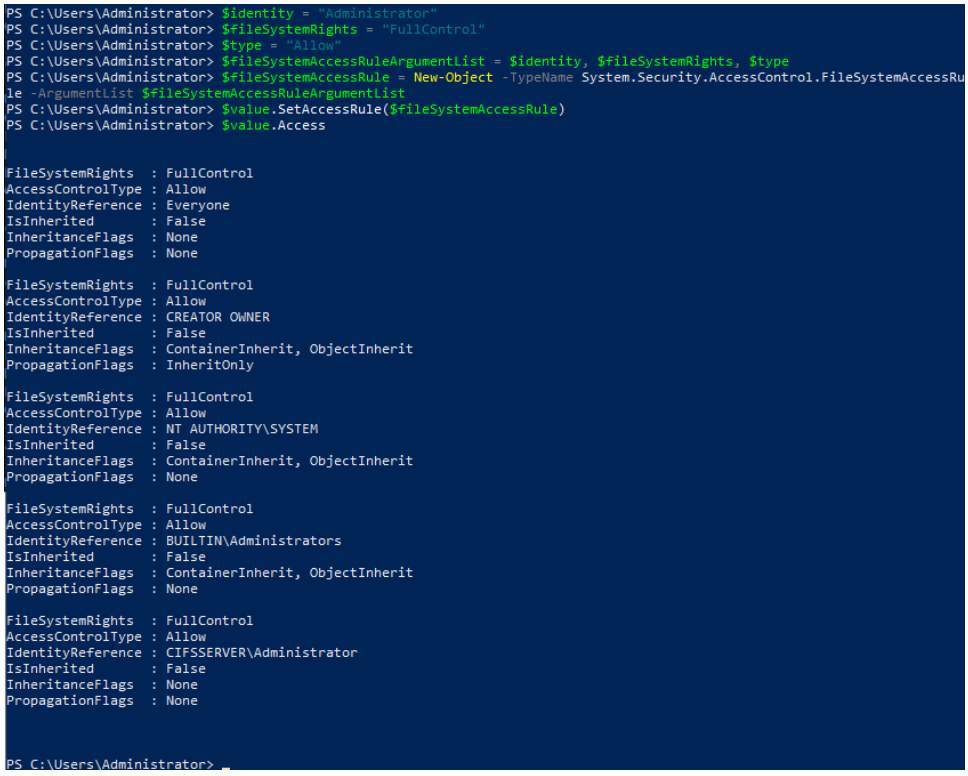


Step 4 Configure the ACL permissions of the file.

```
#Set properties
$identity = "Administrator"
$fileSystemRights = "FullControl"
$type = "Allow"
# Create new rule
$fileSystemAccessRuleArgumentList = $identity, $fileSystemRights, $type
$fileSystemAccessRule = New-Object -TypeName System.Security.AccessControl.FileSystemAccessRule -
ArgumentList
$fileSystemAccessRuleArgumentList
# Apply new rule
$value.SetAccessRule($fileSystemAccessRule)
$value.Access
#Set ACL
Set-Acl $value -Path "X:"
```

 Copyright © Huawei Technologies Co., Ltd.

Figure 4-49 Configuring ACLs using PowerShell



CAUTION

Configure appropriate permissions for the file system root directory when creating the file system. Or, due to the permissions inheritance, you may need to separately modify the permissions of subdirectories and files after modifying the root directory permissions.

----End

4.4 Mounting a File System Automatically

File system mount information may be lost after a server is restarted. You can configure auto mount on the server to avoid losing the mount information.

Restrictions

Because service startup sequences in different OSs vary, some servers running CentOS may not support the following auto mount plans. In this case, manually mount the file system.

Procedure (Linux)

Step 1 Log in to the management console using a cloud account.

1. Log in to the management console and select a region and a project.

 Copyright © Huawei Technologies Co., Ltd.

2. Choose **Compute** > **Elastic Cloud Server** to go to the ECS console.

Step 2 Log in to the ECS as user **root**.

Step 3 Run the **vi /etc/fstab** command to edit the **/etc/fstab** file.

At the end of the file, add the file system information, for example:

```
Mount point /local_path nfs vers=3,timeo=600,nolock 0 0
```

Replace *Mount point* and */local_path* with actual values. You can obtain the mount point from the **Mount Address** column of the file system. Each record in the **/etc/fstab** file corresponds to a mount. Each record has six fields, as described in **Field Description**.

NOTICE

For optimal system performance, configure file system information based on the previous example configuration. If needed, you can customize part of mount parameters. However, the customization may affect system performance.

Step 4 Press **Esc**, input **:wq**, and press **Enter** to save and exit.

After the preceding configurations are complete, the system reads mount information from the **/etc/fstab** file to automatically mount the file system when the ECS restarts.

Step 5 (Optional) Run the following command to view the updated content of the **/etc/fstab** file:

cat /etc/fstab

Step 6 If auto mount fails due to a network issue, add the **sleep** option and a time in front of the mount command in the **rc.local** file, and mount the file system after the NFS service is started.

```
sleep 10s && sudo mount -t nfs -o vers=3,timeo=600,noresvport,nolock,tcp Mount point/ local_path
```

----End

Field Description

Table 1 describes the mount fields.

Table 4-8 Field description

Field	Description
Mount point	The mount point of the file system to be mounted. Set it to the mount point in the **mount** command in **4.1 Mounting an NFS File System to ECSs (Linux)**.
/local_path	A directory created on the ECS used to mount the file system. Set it to the local path in the **mount** command in **4.1 Mounting an NFS File System to ECSs (Linux)**.
nfs	The file system or partition mount type. Set it to **nfs**.

 Copyright © Huawei Technologies Co., Ltd.

Field	Description
vers=3,timeo=600,nolock	Mount options, used to set mount parameters. Use commas (,) to separate between multiple options. • **vers**: file system version. The value **3** indicates NFSv3. • **timeo**: waiting time before the NFS client retransmits a request. The unit is 0.1 second. The recommended value is **600**. • **nolock**: specifies whether to lock files on the server using the NLM protocol.
0	Choose whether to back up file systems using the dump command. • **0**: not to back up file systems • An integer larger than 0: to back up file systems. A file system with a smaller integer is checked earlier than that with a larger integer.
0	Choose whether to check file systems using the fsck command when the ECS is starting and specify the sequence for checking file systems. • **0**: to check file systems • By default, this field is set to **1** for the root directory partition. Other partitions start from **2**, and a partition with a smaller integer is checked earlier than that with a larger integer.

Procedure (Windows)

Ensure that an NFS client has been installed on the target server before mounting. This section uses Windows Server 2012 as an example to describe how to mount a file system.

Step 1 Log in to the management console using a cloud account.

1. Log in to the management console and select a region and a project.
2. Choose **Compute** > **Elastic Cloud Server** to go to the ECS console.

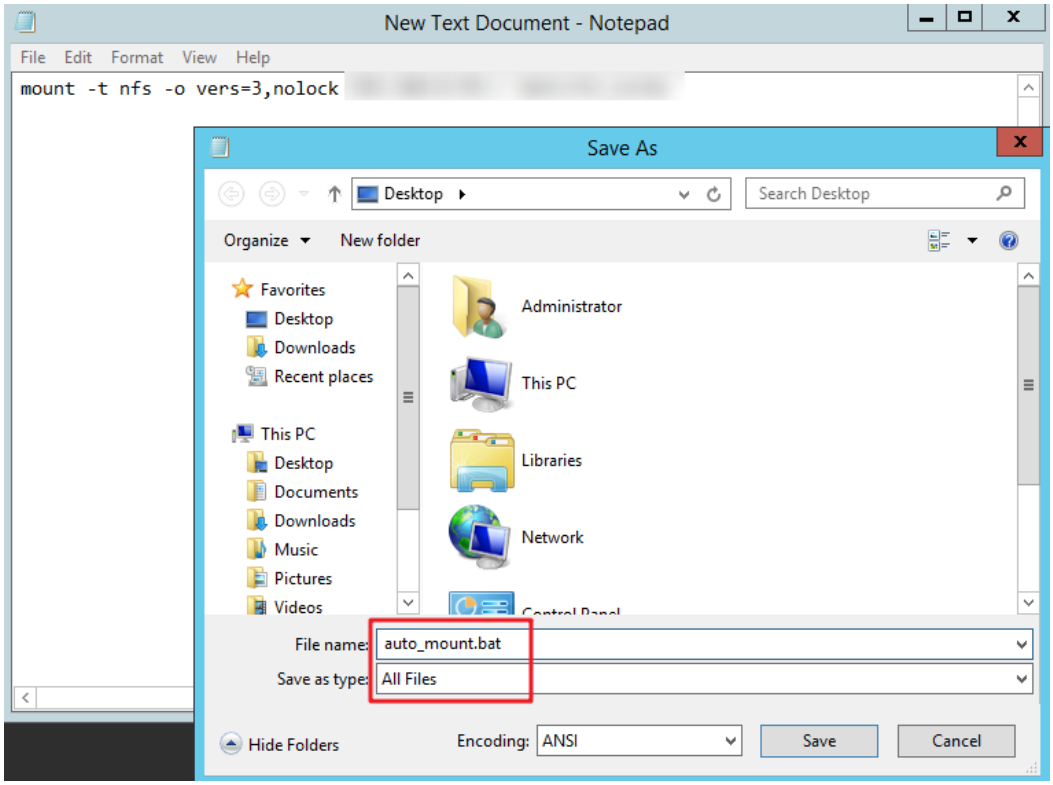
Step 2 Log in to the ECS.

Step 3 Before mounting the file system, create a script named **auto_mount.bat**, save the script to a local host, and record the save path. The script contains the following content:

```
mount -o nolock mount point corresponding drive letter
```

 Copyright © Huawei Technologies Co., Ltd.

Figure 4-50 Saving the script



For example, the **auto_mount.bat** script of a file system contains the following content:

NOTE

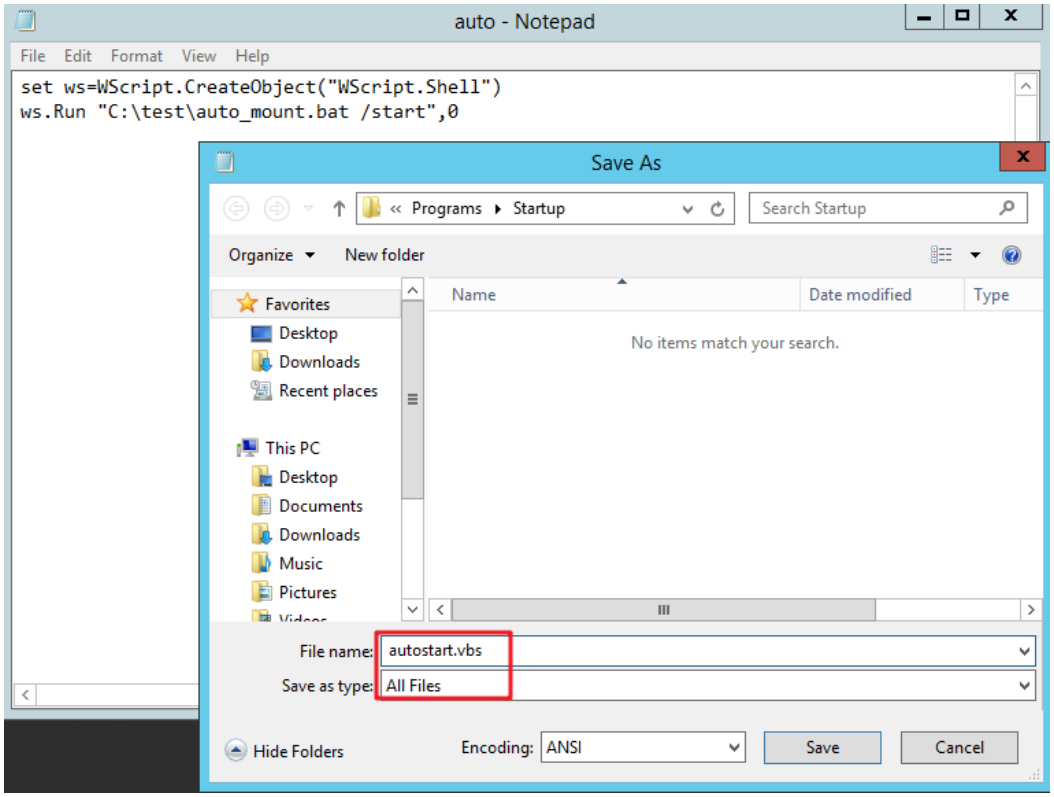
- You can copy the mount command of the file system from the console.
- After the script is created, manually run the script in the Command Prompt to ensure that the script can be executed successfully. If you can view the file system in **This PC** after the script execution, the script can be executed properly.
- This .bat script cannot be stored in the same path in **Step 4** that stores the .vbs file. In this example, the .bat script is stored in **C:\test**.

Step 4 Create a .txt file whose name is *XXX*.**vbs** and save the file to the directory **C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup**. The file contains the following content:

```
set ws=WScript.CreateObject("WScript.Shell")
ws.Run "Local path and script name of the auto_mount.bat script /start", 0
```

 Copyright © Huawei Technologies Co., Ltd.

Figure 4-51 Creating .vbs file



NOTE

In this example, the local path of the **auto_mount.bat** script is **C:\test**. Therefore, the content in the .vbs file is as follows:

```
set ws=WScript.CreateObject("WScript.Shell")
ws.Run "C:\test\auto_mount.bat /start",0
```

Step 5 After the task is created, you can restart the ECS and check whether the configuration is successful. After the configuration is successful, the file system automatically appears in **This PC**.

----End

 Copyright © Huawei Technologies Co., Ltd.

5 Unmount a File System

If a file system is no longer used and needs to be deleted, you are advised to unmount the file system and then delete it.

Prerequisites

Before unmounting a file system, stop the process and read/write operations.

Linux OS

Step 1 Log in to the management console using a cloud account.

1. Log in to the management console and select a region and a project.
2. Choose **Compute** > **Elastic Cloud Server** to go to the ECS console.

Step 2 Log in to the ECS.

Step 3 Run the following command:

umount *Local path*

Local path: An ECS local directory where the file system is mounted, for example, **/local_path**.

NOTE

Before running the **umount** command, stop all read and write operations related to the file system and exit from the local path. Or, the unmounting will fail.

----End

Windows OS

Step 1 Log in to the management console using a cloud account.

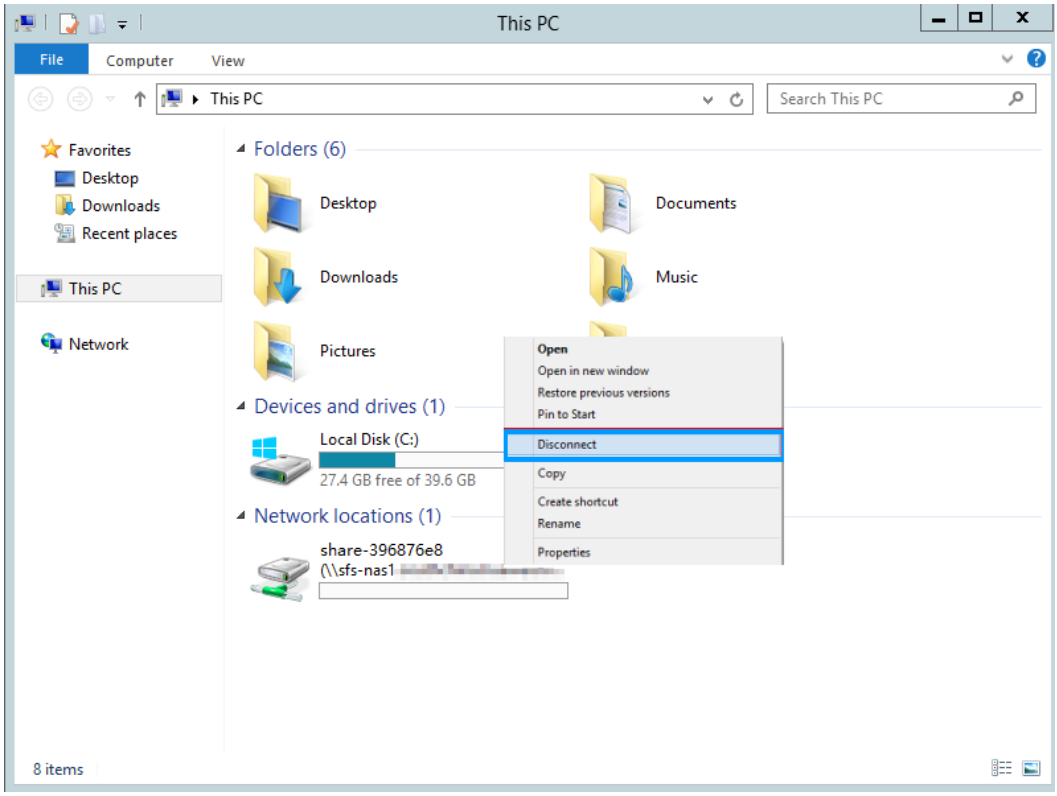
1. Log in to the management console and select a region and a project.
2. Under **Computing**, click **Elastic Cloud Server** to go to the ECS console.

Step 2 Log in to the ECS.

Step 3 Right-click the file system to be unmounted and choose **Disconnect**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 5-1 Unmounting



Step 4 If the file system disappears from the network location, it has been unmounted.

----End

 Copyright © Huawei Technologies Co., Ltd.