Scalable File Service

User Guide (ME-Abu Dhabi Region)

Issue	03
Date	2025-06-27

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

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.

Contents

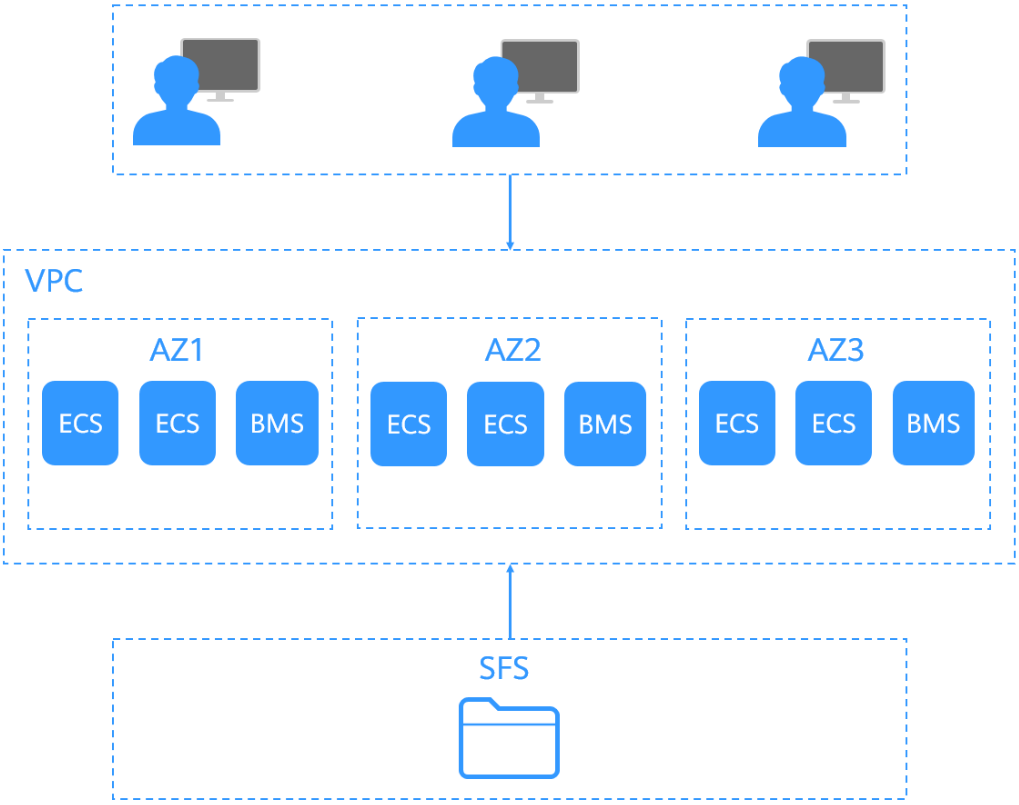
1 Introduction

1.1 What Is SFS?

Overview

Scalable File Service (SFS) provides scalable, high-performance (NAS) file storage. With SFS, you can enjoy shared file access spanning multiple Elastic Cloud Servers (ECSs), Bare Metal Servers (BMSs). See **Figure 1-1**.

Figure 1-1 Accessing SFS



Compared with traditional file sharing storage, SFS has the following advantages:

- File sharing

  Servers in multiple availability zones (AZs) of a same region can access the same file system concurrently and share files.

- Elastic scaling

  Storage can be scaled up or down on demand to dynamically adapt to service changes without interrupting applications. You can complete resizing with a few clicks.

- Superior performance and reliability

  SFS enables file system performance to increase as capacity grows, and it delivers a high data durability to support rapid service growth.

  The backend storage system supports both HDD and SSD storage media. It adopts a distributed architecture and uses full redundant design for modules, which eliminate single-node faults.

- Seamless integration

  SFS supports Network File System (NFS). With this standard protocol, a broad range of mainstream applications can read and write data in the file system.

- Easy operation

  In an intuitive graphical user interface (GUI), you can create and manage file systems with ease.

Accessing SFS

You can access SFS on the management console or via APIs by sending HTTPS requests.

- APIs

  Use APIs if you need to integrate SFS into a third-party system for secondary development. For detailed operations, see *Scalable File Service API Reference*.

- Management console

  Use the console if you prefer a web-based UI to perform operations.

1.2 Application Scenarios

SFS Turbo

Expandable to 320 TB, SFS Turbo provides fully hosted shared file storage. It features high availability and durability to support massive small files and applications requiring low latency and high IOPS. SFS Turbo is perfect to scenarios such as high-performance websites, log storage, compression and decompression, DevOps, enterprise offices, and container applications.

- High-performance websites

  For I/O-intensive website services, SFS Turbo can provide shared website source code directories for multiple web servers, enabling low-latency and high-IOPS concurrent share access.

- Log storage

  SFS Turbo can provide multiple service nodes for shared log output directories, facilitating log collection and management of distributed applications.

- DevOps

  The development directory can be shared to multiple VMs or containers, simplifying the configuration process and improving R&D experience.

- Enterprise offices

  Office documents of enterprises or organizations can be saved in an SFS Turbo file system for high-performance shared access.

1.3 File System Types

SFS Turbo provides two types of file systems: SFS Turbo Standard and SFS Turbo Performance.

The following table describes the features, advantages, and application scenarios of these file system types.

Table 1-1 Comparison of file system types

File System Type	Storage Class	Features	Highlights	Application Scenarios
SFS Turbo	Standard	● Maximum bandwidth: 150 MB/s; maximum IOPS: 5,000 ● Latency: 2 to 5 ms; maximum capacity: 32 TB ● Suitable for services with massive small files and services that require low latency.	Low latency and tenant exclusive	Workloads dealing with massive small files, such as code storage, log storage, web services, and virtual desktop
	Standard-Enhanced	● Maximum bandwidth: 1 GB/s; maximum IOPS: 15,000 ● Enhanced bandwidth, IOPS, and capacity	Low latency, high bandwidth, and tenant exclusive	Workloads dealing with massive small files and those requiring high bandwidth, such as code storage, file sharing, enterprise office automation (OA), and log storage

File System Type	Storage Class	Features	Highlights	Application Scenarios
	Performance	- Maximum bandwidth: 350 MB/s; maximum IOPS: 20,000 - Latency: 1 to 2 ms; maximum capacity: 32 TB - Delivers better performance and suitable for services with massive small files and services that require low latency.	Low latency, high IOPS, and tenant exclusive	Workloads dealing with massive small files, and random I/O-intensive and latency-sensitive services, such as high-performance websites and content management
	Performance - Enhanced	- Maximum bandwidth: 2 GB/s; maximum IOPS: 100,000 - Enhanced bandwidth, IOPS, and capacity	Low latency, high IOPS, high bandwidth, and tenant exclusive	Workloads dealing with massive small files, and latency-sensitive and bandwidth-demanding workloads, such as image rendering, AI training, and enterprise OA

1.4 File System Encryption

SFS provides you with the encryption function. You can encrypt data on the new file systems if needed.

Keys for encrypting file systems are provided by Key Management Service (KMS), which is secure and convenient. You do not need to establish and maintain key management infrastructure. If you want to use your own key material, use the key import function on the KMS console to create a custom key whose key material is empty and import the key material to the custom key. For details, see section "Importing Key Materials" in *Key Management Service User Guide*.

To use the file system encryption function, you can directly select the encryption function when creating an SFS Turbo file system without authorization.

Encryption Key

SFS Turbo file systems do not have default keys. You can use your existing key or create a key. For details, see section "Creating a Key" in the *Key Management Service User Guide*.

1.5 SFS and Other Services

Relationships Between SFS and Other Services

Table 1-2 Related services

Function	Related Service	Reference
A file system and the servers must belong to the same project so that they can mount the same file system for data sharing.	Elastic Cloud Server (ECS)	Mounting an NFS File System to ECSs (Linux) Mounting an NFS File System to ECSs (Windows)
VPC allows you to provision isolated virtual networks defined and managed by yourself. This improves the security of cloud resources and simplifies network deployment. A server cannot access file systems in a different VPC. Before using SFS, assign the file system and the servers to the same VPC.	Virtual Private Cloud (VPC)	Creating a File System
IAM is an enterprise-level self-help cloud resource management system. It provides user identity management and access control functions. When an enterprise needs to provide SFS for multiple users within the enterprise, the enterprise administrator can use IAM to create users and control these users' permissions on enterprise resources.	Identity and Access Management (IAM)	**User Permissions**
Once you have subscribed to SFS, you can monitor its performance, such as the read bandwidth, write bandwidth, and read and write bandwidth on Cloud Eye, which does not require any plug-ins.	Cloud Eye	**Monitoring**

Function	Related Service	Reference
Cloud Trace Service (CTS) allows you to collect, store, and query cloud resource operation records and use these records for security analysis, compliance auditing, resource tracking, and fault locating. With CTS, you can record operations associated with SFS for later query, audit, and backtrack operations.	Cloud Trace Service (CTS)	**Auditing**

1.6 Basic Concepts

1.6.1 SFS Basic Concepts

Before you start, understand the following concepts.

NFS

Network File System (NFS) is a distributed file system protocol that allows different computers and operating systems to share data over a network.

File System

A file system provides users with shared file storage service through NFS. It is used for accessing network files remotely. After a user creates a file system on the console, the file system can be mounted to multiple servers and is accessible through the standard POSIX.

POSIX

Portable Operating System Interface (POSIX) is a set of interrelated standards specified by Institute of Electrical and Electronics Engineers (IEEE) to define the application programming interface (API) for software compatible with variants of the UNIX operating system. POSIX is intended to achieve software portability at the source code level. That is, a program written for a POSIX compatible operating system may be compiled and executed on any other POSIX operating system.

DHCP

Dynamic Host Configuration Protocol (DHCP) is a LAN network protocol. The server controls an IP address range, and a client can automatically obtain the IP address and subnet mask allocated by the server when logging in to the server. By default, DHCP is not automatically installed as a service component of Windows Server. Manual installation and configuration are required.

1.6.2 Region and AZ

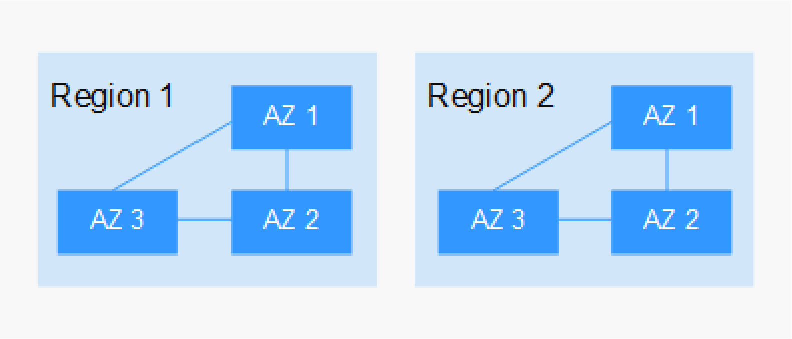
Concept

A region and availability zone (AZ) identify the location of a data center. You can create resources in a specific region and AZ.

- A region is a physical data center, which is completely isolated to improve fault tolerance and stability. The region that is selected during resource creation cannot be changed after the resource is created.
- An AZ is a physical location where resources use independent power supplies and networks. A region contains one or more AZs that are physically isolated but interconnected through internal networks. Because AZs are isolated from each other, any fault that occurs in one AZ will not affect others.

Figure 1-2 shows the relationship between regions and AZs.

Figure 1-2 Regions and AZs



Selecting a Region

You are advised to select a region close to you or your target users. This helps ensure low access latency.

Selecting an AZ

When deploying resources, consider your applications' requirements on disaster recovery (DR) and network latency.

- For high DR capability, deploy resources in different AZs within the same region.
- For lower network latency, deploy resources in the same AZ.

Regions and Endpoints

Before you use an API to call resources, specify its region and endpoint. For more details, see **Regions and Endpoints**.

1.7 Notes and Constraints

General

- To obtain better performance, you are advised to use the operating systems listed in **Supported Operating Systems**, which have passed the compatibility test.
- Currently, SFS does not support replication.
- Currently, SFS does not support cross-region access.

SFS Turbo

- Only the NFSv3 protocol is supported (NFSv4 is not supported).
- A maximum of 500 compute nodes can be mounted to and access a single file system at the same time.
- The maximum capacity of a single file system is 32 TB, and the maximum size of a single file allowed is 320 TB.
- Maximum number of files supported by a single file system = Capacity/16. For example, the maximum number of files supported by a 500 GB file system is 32,768,000 (500 GB/16 KB = 500 x 1024 x 1024/16).
- By default, a single directory can contain a maximum of 20 million files.

  NOTE

  If you need to execute the **ls**, **du**, **cp**, **chmod**, or **chown** command on a directory, you are advised to place no more than 500,000 files or subdirectories in that directory. Otherwise, requests may take long times as the NFS protocol sends a large number of requests to traverse directory files and requests are queuing up.
- The maximum full path is 4,096 bytes, and the maximum file name length is 255 bytes.
- The maximum soft link length is 1,024 bytes.
- The maximum number of hard links is 255.
- The maximum directory depth is 100 layers.

1.8 User Permissions

The system provides two types of user permissions by default: user management and resource management.

User management refers to the management of users, user groups, and user group rights.

Resource management refers to the control operations that can be performed by users on cloud service resources.

For details, see the *Permission Description*.

1.9 Permissions

If you need to assign different permissions to employees in your enterprise to access your SFS resources on the cloud, Identity and Access Management (IAM) is a good choice for fine-grained permissions management. IAM provides identity authentication, permissions management, and access control, helping you to securely access your cloud resources.

With IAM, you can use your cloud account to create IAM users, and assign permissions to the users to control their access to specific resources. For example, some software developers in your enterprise need to use SFS resources but should not be allowed to delete the resources or perform any other high-risk operations. In this scenario, you can create IAM users for the software developers and grant them only the permissions required for using SFS resources.

If your cloud account does not require individual IAM users for permissions management, skip this section.

IAM can be used free of charge. You pay only for the resources in your account. For more information about IAM, see *Identity and Access Management User Guide*.

SFS Permissions

By default, new IAM users do not have permissions assigned. You need to add a user to one or more groups, and attach permissions policies or roles to these groups. Users inherit permissions from the groups to which they are added and can perform specified operations on cloud services based on the permissions.

SFS is a project-level service deployed and accessed in specific physical regions. To assign SFS permissions to a user group, specify the scope as region-specific projects and select projects for the permissions to take effect. If **All projects** is selected, the permissions will take effect for the user group in all region-specific projects. When accessing SFS, the users need to switch to a region where they have been authorized to use this service.

You can grant users permissions by using roles and policies.

- Roles: A type of coarse-grained authorization mechanism that defines permissions related to user responsibilities. This mechanism provides only a limited number of service-level roles for authorization. When using roles to grant permissions, you need to also assign other roles on which the permissions depend to take effect. However, roles are not an ideal choice for fine-grained authorization and secure access control.
- Policies: A type of fine-grained authorization mechanism that defines permissions required to perform operations on specific cloud resources under certain conditions. This mechanism allows for more flexible policy-based authorization, meeting requirements for secure access control. For example, you can grant ECS users only the permissions for managing a certain type of ECSs. Most policies define permissions based on APIs. For the API actions supported by SFS, see section "Permissions Policies and Supported Actions" in the *Scalable File Service API Reference*.

Table 1-3 lists all the system-defined roles and policies supported by SFS Turbo.

Table 1-3 System-defined roles and policies supported by SFS Turbo

Role/Policy Name	Description	Type	Dependency
SFS Turbo FullAccess	Administrator permissions for SFS Turbo. Users granted these permissions can perform all operations on SFS Turbo file systems.	System-defined policy	None
SFS Turbo ReadOnlyAccess	Read-only permissions for SFS Turbo. Users granted these permissions can only view SFS Turbo file system data.	System-defined policy	None

1.10 Supported Operating Systems

Table 1-4 lists the operating systems that have passed the compatibility test.

Table 1-4 Supported operating systems

Type	Version	SFS Capacity-Oriented	SFS Turbo
CentOS	CentOS 5, 6, and 7 for x86	√	√
Debian	Debian GNU/Linux 6, 7, 8, and 9 for x86	√	√
Oracle	Oracle Enterprise Linux 5, 6, and 7 for x86	√	√
Red Hat	Red Hat Enterprise Linux 5, 6, and 7 for x86	√	√
SUSE	SUSE Linux Enterprise Server 10, 11, and 12 for x86	√	√
Ubuntu	Ubuntu 10, 11, 12, 13, 14, and 15 LTS for x86	√	√
EulerOS	EulerOS 2	√	√

Type	Version	SFS Capacity-Oriented	SFS Turbo
Fedora	Fedora 24 and 25	√	√
OpenSUSE	OpenSUSE 42	√	√
Windows	Windows Server 2008, 2008 r2, 2012, 2012 r2, and 2016 for x64 Windows 7, 8, and 10	√	×

2 Getting Started

2.1 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*.

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 2-1** describes the parameters.

Table 2-1 File system parameters

Parameter	Description	Remarks
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.

Parameter	Description	Remarks
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.
Storage Class	Mandatory Includes SFS Turbo Standard and SFS Turbo Performance. For more information, see **File System Types**.	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.
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: ● Standard: 500 GB to 32 TB ● Performance: 500 GB to 32 TB
Protocol Type	Mandatory SFS Turbo supports NFS for file system access.	The default value is **NFS**.

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*.	-

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.	-
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.

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

2.2 Mount a File System

2.2.1 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.

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 that is in the same VPC as the file system 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.

- **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
        ```

   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 2-2 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 **Mounting a File System Automatically**.

Table 2-2 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**.
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 2-3**. 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 2-3 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**.
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.

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.
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.

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

2.2.2 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.

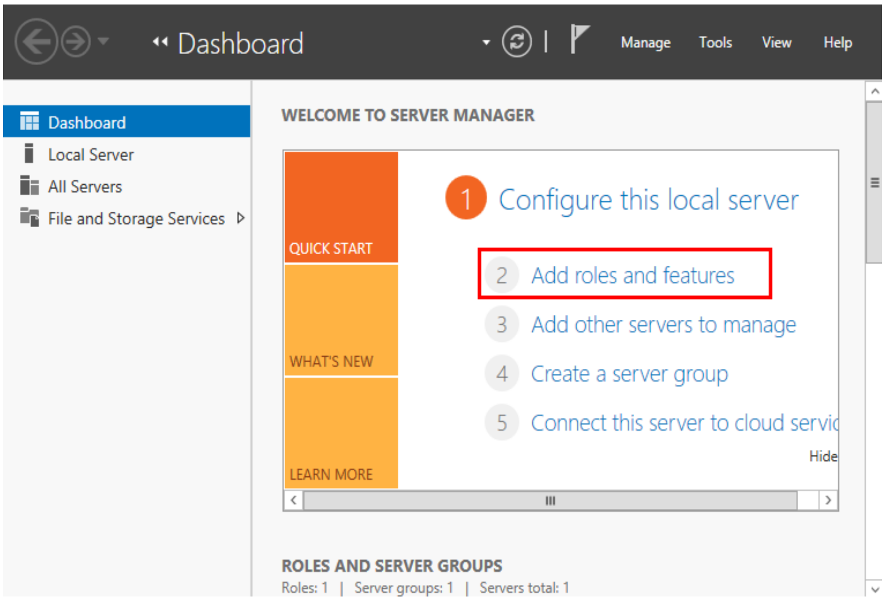
1. Log in to the management console and select a region and a project.
2. Choose **Compute** > **Elastic Cloud Server** to go to the ECS console.

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

Step 3 Install the NFS client.

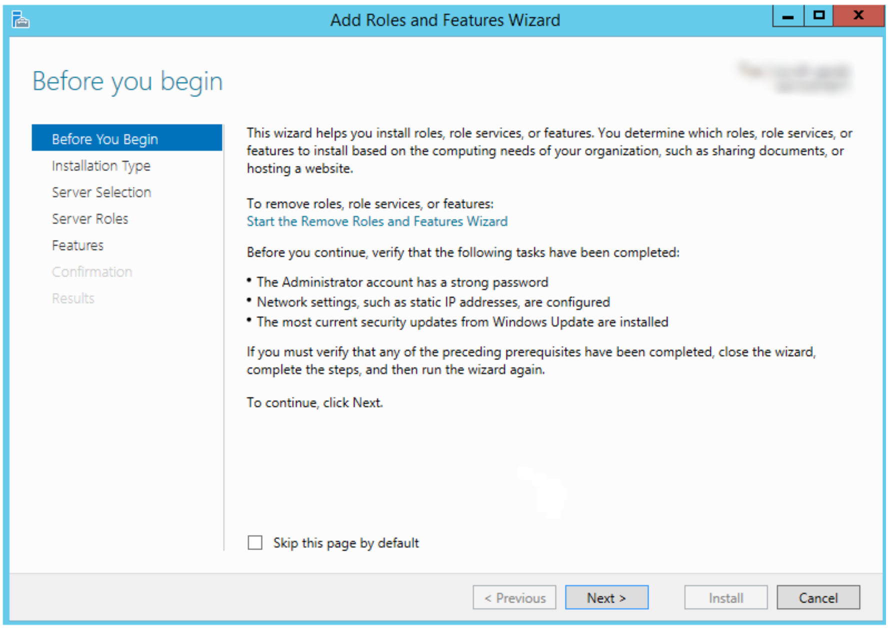
1. Click **Server Manager** in the lower left corner. The **Server Manager** window is displayed, as shown in **Figure 2-1**.

Figure 2-1 Server Manager


Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
File and Storage Services
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
1 Configure this local server
2 Add roles and features
3 Add other servers to manage
4 Create a server group
5 Connect this server to cloud servic
Hide
ROLES AND SERVER GROUPS
Roles: 1 | Server groups: 1 | Servers total: 1

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

Figure 2-2 Wizard for adding roles and features



This wizard helps you install roles, role services, or features. You determine which roles, role services, or features to install based on the computing needs of your organization, such as sharing documents, or hosting a website.

To remove roles, role services, or features:
Start the Remove Roles and Features Wizard

Before you continue, verify that the following tasks have been completed:

- The Administrator account has a strong password
- Network settings, such as static IP addresses, are configured
- The most current security updates from Windows Update are installed

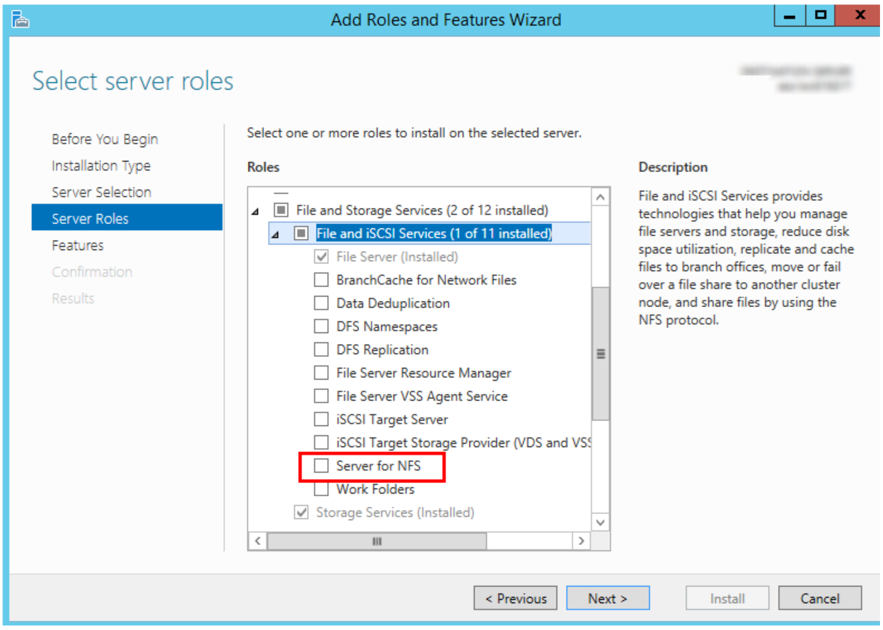
If you must verify that any of the preceding prerequisites have been completed, close the wizard, complete the steps, and then run the wizard again.

To continue, click Next.

□ Skip this page by default

3. Click **Next** as prompted. On the **Server Roles** page, select **Server for NFS**, as shown in **Figure 2-3**.

Figure 2-3 Selecting the server for NFS



Select one or more roles to install on the selected server.

Roles

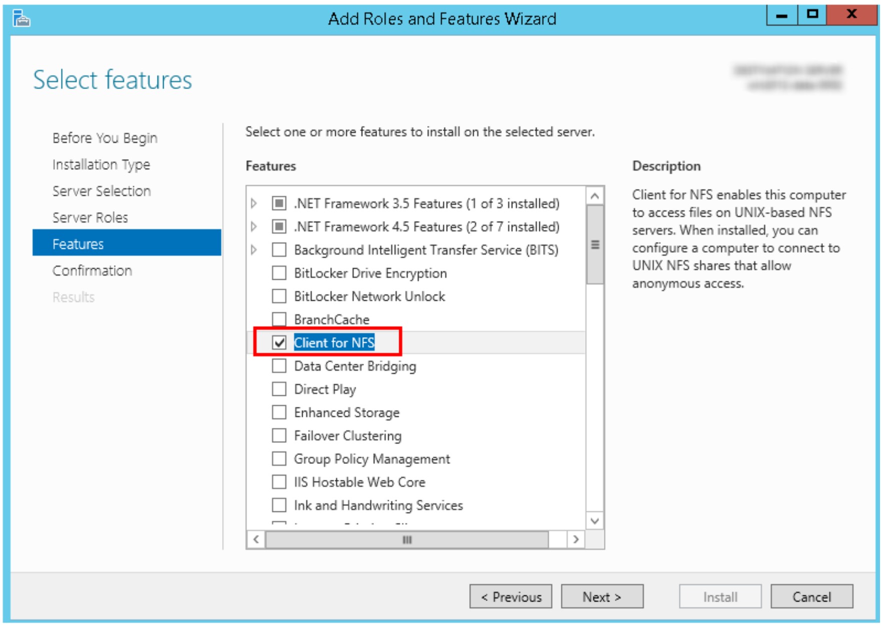
- File and Storage Services (2 of 12 installed)
  - File and iSCSI Services (1 of 11 installed)
    - ☑ File Server (Installed)
    - □ BranchCache for Network Files
    - □ Data Deduplication
    - □ DFS Namespaces
    - □ DFS Replication
    - □ File Server Resource Manager
    - □ File Server VSS Agent Service
    - □ iSCSI Target Server
    - □ iSCSI Target Storage Provider (VDS and VSS
    - □ Server for NFS
    - □ Work Folders
  - ☑ Storage Services (Installed)

Description

File and iSCSI Services provides technologies that help you manage file servers and storage, reduce disk space utilization, replicate and cache files to branch offices, move or fail over a file share to another cluster node, and share files by using the NFS protocol.

4. Click **Next**. In the **Features** page, select **Client for NFS** and click **Next**, as shown in **Figure 2-4**. 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 2-4 Selecting the NFS client



Select one or more features to install on the selected server.

Features

- ▣ .NET Framework 3.5 Features (1 of 3 installed)
- ▣ .NET Framework 4.5 Features (2 of 7 installed)
- □ Background Intelligent Transfer Service (BITS)
- □ BitLocker Drive Encryption
- □ BitLocker Network Unlock
- □ BranchCache
- ☑ Client for NFS
- □ Data Center Bridging
- □ Direct Play
- □ Enhanced Storage
- □ Failover Clustering
- □ Group Policy Management
- □ IIS Hostable Web Core
- □ Ink and Handwriting Services

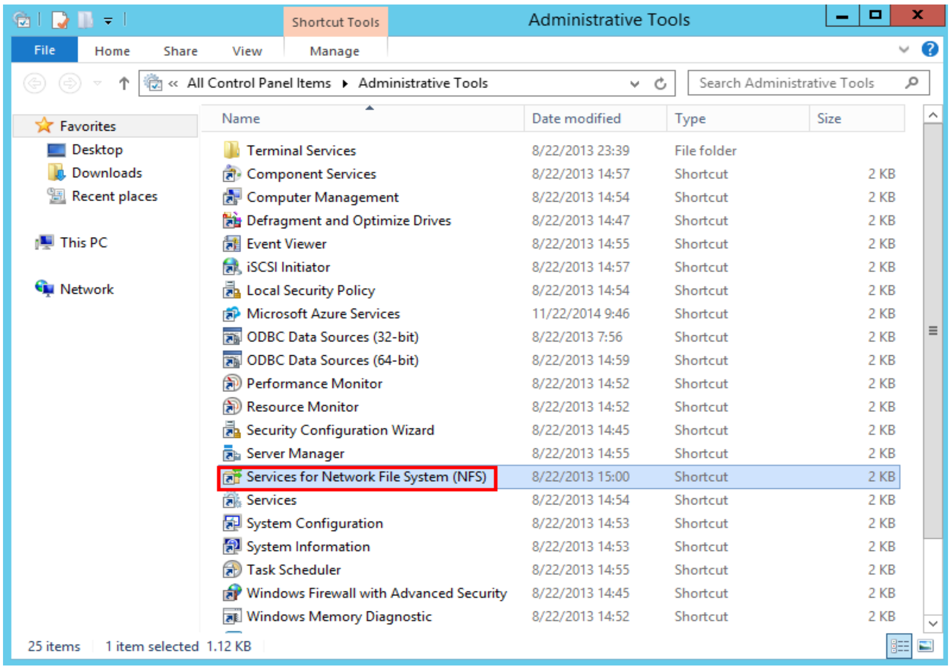
Description

Client for NFS enables this computer to access files on UNIX-based NFS servers. When installed, you can configure a computer to connect to UNIX NFS shares that allow anonymous access.

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 2-5**.

Figure 2-5 Administrative tools



Name	Date modified	Type	Size
Terminal Services	8/22/2013 23:39	File folder	
Component Services	8/22/2013 14:57	Shortcut	2 KB
Computer Management	8/22/2013 14:54	Shortcut	2 KB
Defragment and Optimize Drives	8/22/2013 14:47	Shortcut	2 KB
Event Viewer	8/22/2013 14:55	Shortcut	2 KB
iSCSI Initiator	8/22/2013 14:57	Shortcut	2 KB
Local Security Policy	8/22/2013 14:54	Shortcut	2 KB
Microsoft Azure Services	11/22/2014 9:46	Shortcut	2 KB
ODBC Data Sources (32-bit)	8/22/2013 7:56	Shortcut	2 KB
ODBC Data Sources (64-bit)	8/22/2013 14:59	Shortcut	2 KB
Performance Monitor	8/22/2013 14:52	Shortcut	2 KB
Resource Monitor	8/22/2013 14:52	Shortcut	2 KB
Security Configuration Wizard	8/22/2013 14:45	Shortcut	2 KB
Server Manager	8/22/2013 14:55	Shortcut	2 KB
Services for Network File System (NFS)	8/22/2013 15:00	Shortcut	2 KB
Services	8/22/2013 14:54	Shortcut	2 KB
System Configuration	8/22/2013 14:53	Shortcut	2 KB
System Information	8/22/2013 14:53	Shortcut	2 KB
Task Scheduler	8/22/2013 14:55	Shortcut	2 KB
Windows Firewall with Advanced Security	8/22/2013 14:45	Shortcut	2 KB
Windows Memory Diagnostic	8/22/2013 14:52	Shortcut	2 KB

25 items 1 item selected 1.12 KB

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

Figure 2-6 Services for NFS

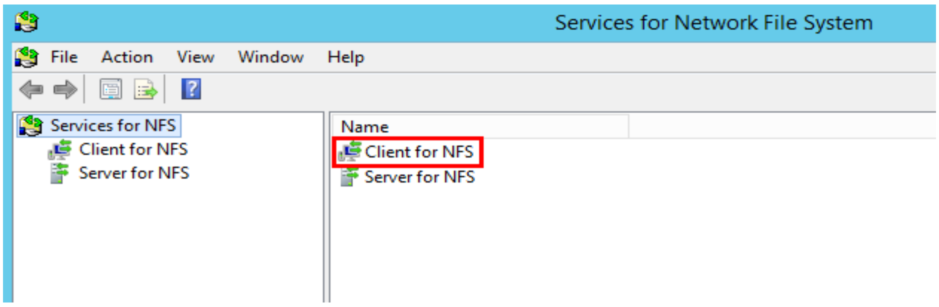
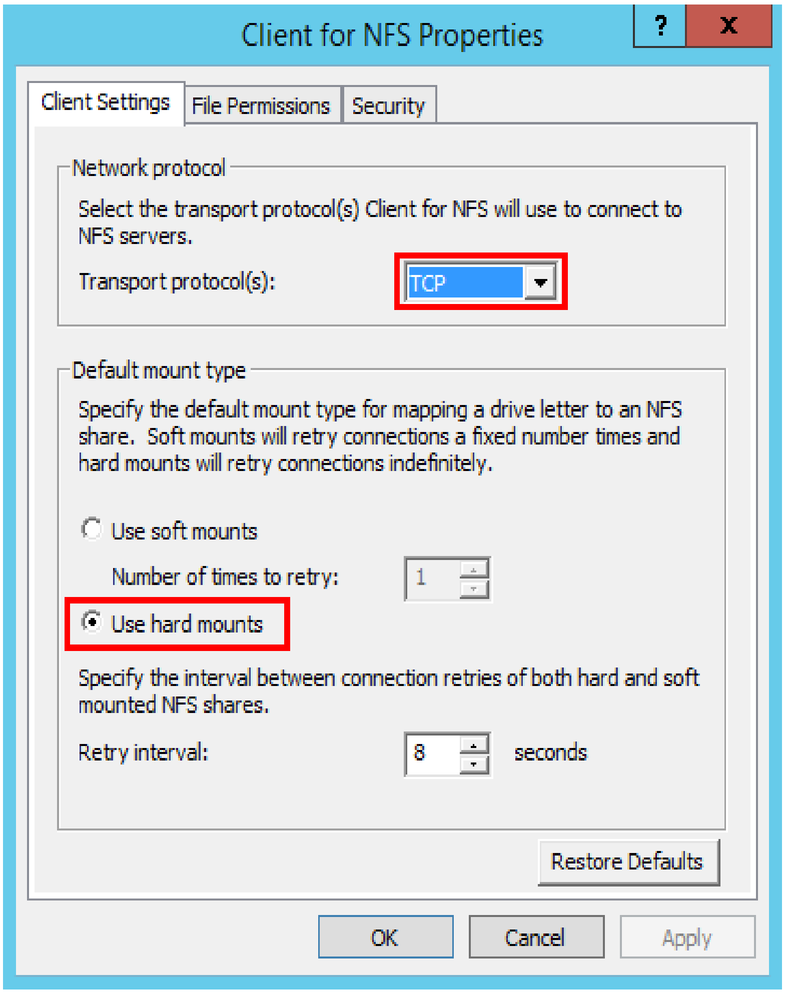


Figure 2-7 Client for NFS properties


Client for NFS Properties

Client Settings | File Permissions | Security

Network protocol

Select the transport protocol(s) Client for NFS will use to connect to NFS servers.

Transport protocol(s): TCP

Default mount type

Specify the default mount type for mapping a drive letter to an NFS share. Soft mounts will retry connections a fixed number times and hard mounts will retry connections indefinitely.

○ Use soft mounts

Number of times to retry: 1

● Use hard mounts

Specify the interval between connection retries of both hard and soft mounted NFS shares.

Retry interval: 8 seconds

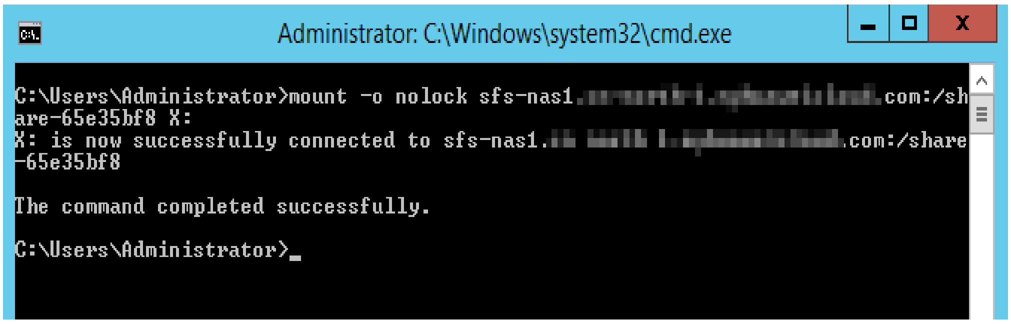
Step 5 Run the following command in the Command Prompt of the Windows Server 2012 (**X** is the drive letter of the free disk). Select the ECS that is in the same VPC as the file system to mount the file system.

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 2-8** is displayed, the mounting is successful.

Figure 2-8 Running the command

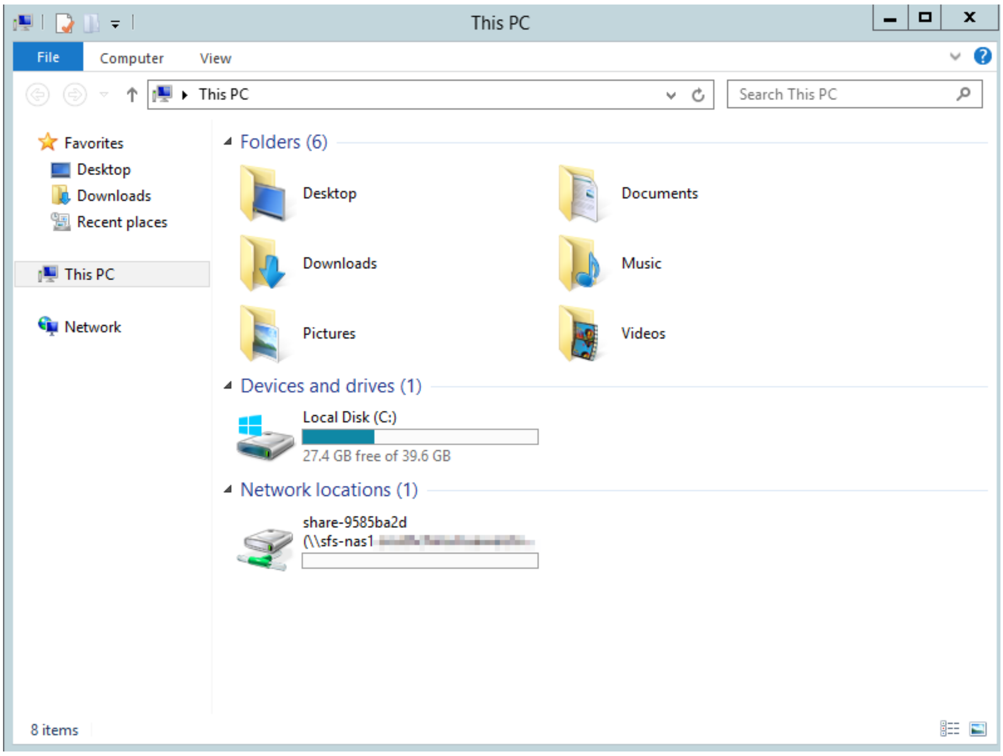


```
C:\Users\Administrator>mount -o nolock sfs-nas1.[redacted].com:/sh
are-65e35bf8 X:
X: is now successfully connected to sfs-nas1.[redacted].com:/share
-65e35bf8

The command completed successfully.

C:\Users\Administrator>_
```

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 2-9**.

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

Figure 2-9 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

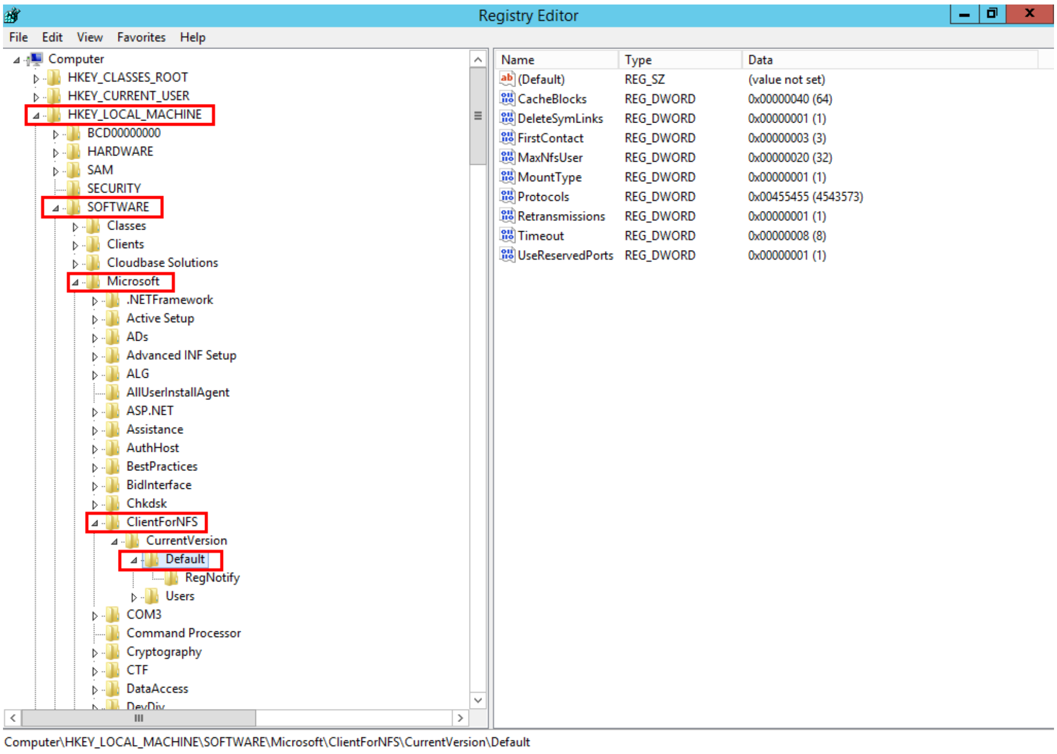
Troubleshooting

If a file system is mounted to a Linux ECS and a Windows ECS, on the Windows ECS, data cannot be written to the files created by the Linux ECS. To address this problem, modify the registry and change both UID and GID values to **0** for NFS accesses from Windows. This section uses Windows Server 2012 as an example. Do as follows:

Step 1 Choose **Start** > **Run** and enter **regedit** to open the registry.

Step 2 Enter the **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ClientForNFS\CurrentVersion\Default** directory. See **Figure 2-10**.

Figure 2-10 Entering the directory

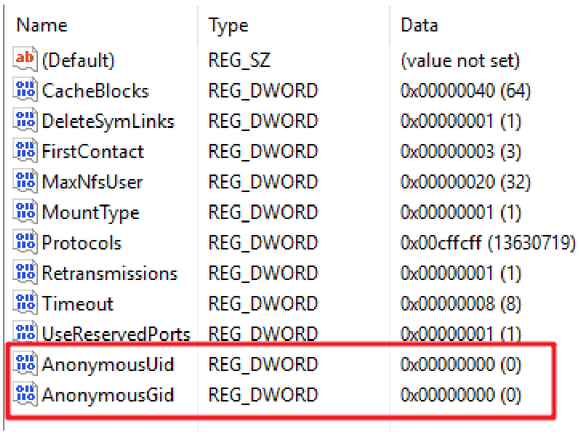


Name	Type	Data
(Default)	REG_SZ	(value not set)
CacheBlocks	REG_DWORD	0x00000040 (64)
DeleteSymLinks	REG_DWORD	0x00000001 (1)
FirstContact	REG_DWORD	0x00000003 (3)
MaxNfsUser	REG_DWORD	0x00000020 (32)
MountType	REG_DWORD	0x00000001 (1)
Protocols	REG_DWORD	0x00455455 (4543573)
Retransmissions	REG_DWORD	0x00000001 (1)
Timeout	REG_DWORD	0x00000008 (8)
UseReservedPorts	REG_DWORD	0x00000001 (1)

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ClientForNFS\CurrentVersion\Default

Step 3 Right-click the blank area and choose **New** > **DWORD Value** from the shortcut menu. Set **AnonymousUid** and **AnonymousGid** to **0**. **Figure 2-11** shows a successful operation.

Figure 2-11 Adding values



Name	Type	Data
(Default)	REG_SZ	(value not set)
CacheBlocks	REG_DWORD	0x00000040 (64)
DeleteSymLinks	REG_DWORD	0x00000001 (1)
FirstContact	REG_DWORD	0x00000003 (3)
MaxNfsUser	REG_DWORD	0x00000020 (32)
MountType	REG_DWORD	0x00000001 (1)
Protocols	REG_DWORD	0x00cffcff (13630719)
Retransmissions	REG_DWORD	0x00000001 (1)
Timeout	REG_DWORD	0x00000008 (8)
UseReservedPorts	REG_DWORD	0x00000001 (1)
AnonymousUid	REG_DWORD	0x00000000 (0)
AnonymousGid	REG_DWORD	0x00000000 (0)

Step 4 After modifying the registry, restart the server for the modification to take effect.

----End

2.2.3 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.
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 2-4 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 **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 **Mounting an NFS File System to ECSs (Linux)**.
nfs	The file system or partition mount type. Set it to **nfs**.
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.

Field	Description
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.

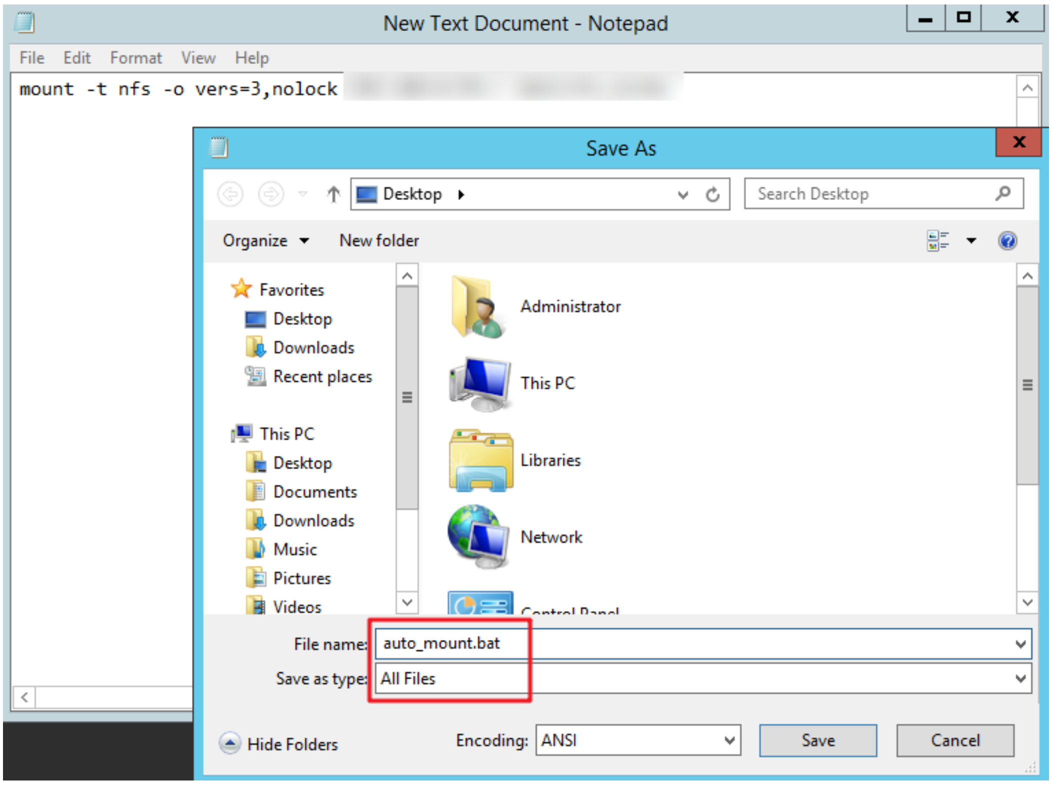
1. Log in to the management console and select a region and a project.
2. Choose **Compute** > **Elastic Cloud Server** to go to the ECS console.

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
```

Figure 2-12 Saving the script



```
mount -t nfs -o vers=3,nolock [redacted]
```

File name: auto_mount.bat

Save as type: All Files

Encoding: ANSI

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

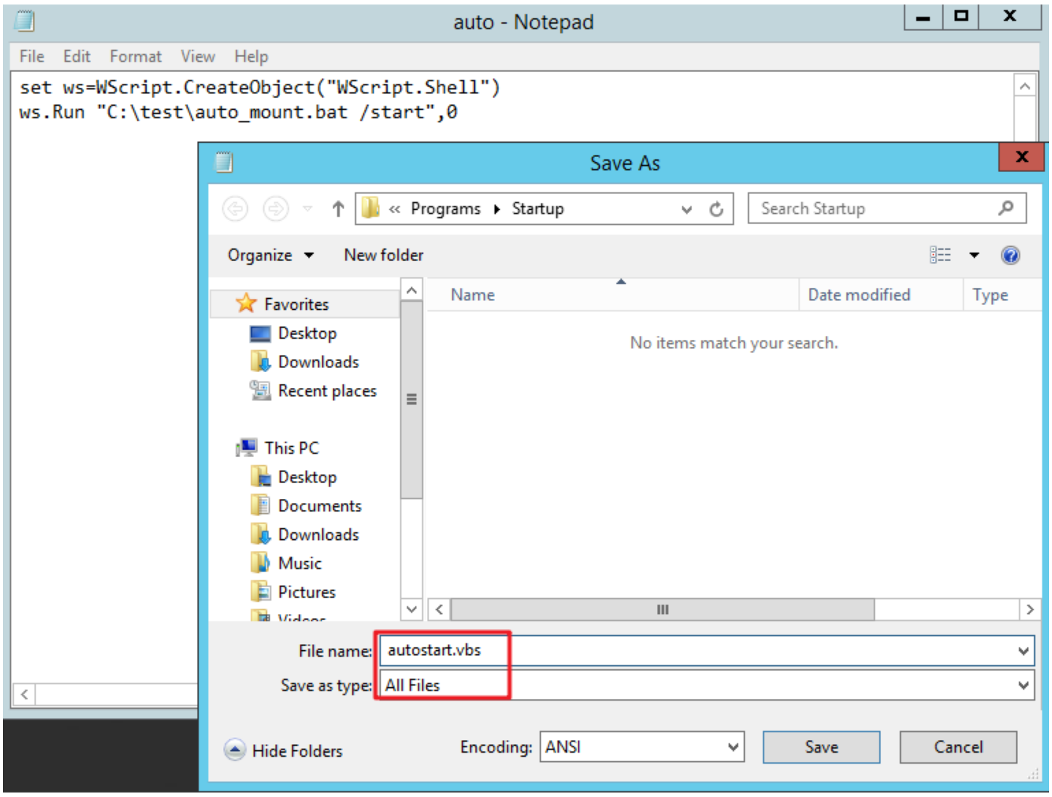
NOTE

- 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
```

Figure 2-13 Creating .vbs file



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

File name: autostart.vbs
Save as type: All Files
Encoding: ANSI

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

2.3 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

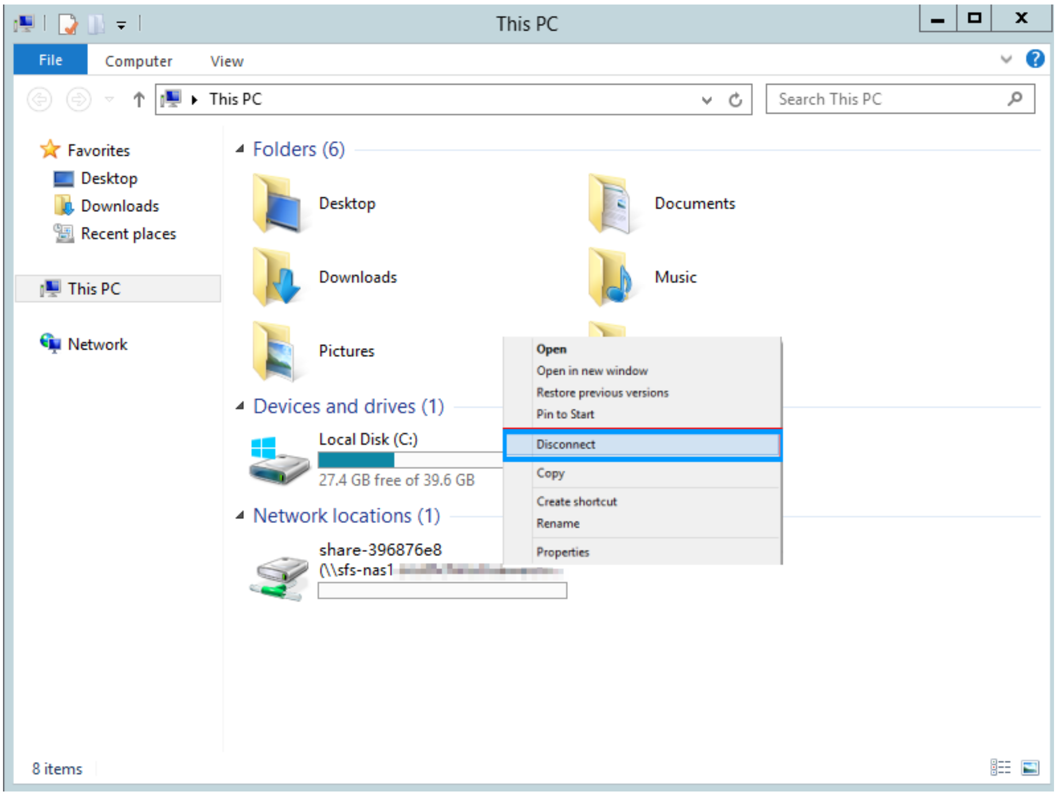
Step 1 Log in to the management console using a cloud account.

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**.

Figure 2-14 Unmounting



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

----End

3 Management

3.1 Permissions Management

3.1.1 Creating a User and Granting SFS Permissions

This chapter describes how to use IAM to implement fine-grained permissions control for your SFS resources. With IAM, you can:

- Create IAM users for employees based on your enterprise's organizational structure. Each IAM user will have their own security credentials for accessing SFS resources.
- Grant only the permissions required for users to perform a specific task.

If your cloud account does not require individual IAM users, skip this section.

This section describes the procedure for granting permissions (see **Figure 3-1**).

Prerequisites

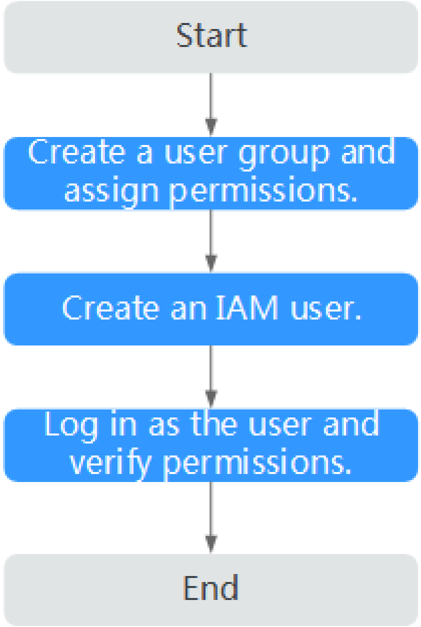
Learn about the permissions (see **Permissions**) supported by SFS and choose policies or roles according to your requirements.

Restrictions

- Both system-defined policies and custom policies are supported in SFS Turbo file systems.

Process Flow

Figure 3-1 Process for granting SFS permissions


Start
Create a user group and assign permissions.
Create an IAM user.
Log in as the user and verify permissions.
End

1. Create a user group and assign permissions to it.

   Create a user group on the IAM console, and attach the **SFS Turbo ReadOnlyAccess** policy to the group.

2. Create a user and add it to a user group.

   Create a user on the IAM console and add the user to the group created in **1**.

3. Log in and verify permissions.

   Log in to the SFS console using the created user, and verify that the user only has read permissions for SFS.

   - Choose **Scalable File Service**. Click **Create File System** on the SFS console. If a message appears indicating that you have insufficient permissions to perform the operation, the **SFS Turbo ReadOnlyAccess** policy has already taken effect.
   - Choose any other service. If a message appears indicating that you have insufficient permissions to access the service, the **SFS Turbo ReadOnlyAccess** policy has already taken effect.

3.2 File System Management

3.2.1 Viewing a File System

You can search for file systems by file system name keyword and view their basic information.

Procedure

Step 1 Log in to the SFS console.

Step 2 In the file system list, view the file systems you have created. **Table 3-1** describes the file system parameters.

Table 3-1 Parameter description

Parameter	Description
Name	Name of the created file system
Status	Possible values are **Available**, **Unavailable**, **Frozen**, **Creating**, **Deleting**.
Type	File system type
Protocol Type	File system protocol, which is **NFS**
Used Capacity (GB)	File system space already used for data storage **NOTE** This information is refreshed every 15 minutes.
Maximum Capacity (GB)	Maximum capacity of the file system
Mount Point	File system mount point, which is in the format of *File system IP address*:**/**
Operation	Valid operations include capacity expansion, monitoring metric viewing, and deletion.

Step 3 (Optional) Search for the specified file system by file system name.

----End

3.2.2 Deleting a File System

Data in a deleted file system cannot be restored. Ensure that files in a file system have been properly stored or backed up before you delete the file system.

Prerequisites

The file system to be deleted has been unmounted. For details about how to unmount the file system, see .

Procedure

Step 1 In the file system list, locate the file system you want to delete and click **Delete** in the **Operation** column.

Step 2 In the displayed dialog box file system, as shown in , confirm the information and click **OK**.

NOTE

Only file systems whose statuses are **Available** or **Creation failed** can be deleted.

Step 3 Check that the file system disappears from the file system list.

----End

3.3 Capacity Expansion

Scenarios

You can expand the capacity of a file system when needed.

Constraints

SFS Turbo file systems can only have their capacities expanded, not reduced. And only **In-use** file systems can be expanded.

Procedure

Step 1 Log in to the SFS console.

Step 2 In the file system list, click **Expand Capacity** in the row of the desired file system. The following dialog box is displayed

Step 3 Enter a new maximum capacity of the file system based on service requirements, and click **OK**. Table 3-2 describes the parameters.

Table 3-2 Capacity expansion parameters

Parameter	Description
Used Capacity (GB)	Used capacity of the current file system
Maximum Capacity (GB)	Maximum capacity of the current file system
New Maximum Capacity (GB)	Target maximum capacity of the file system after expanding The value ranges from **1 GB** to **512,000 GB**.

Step 4 In the displayed dialog box, confirm the information and click **OK**.

Step 5 In the file system list, check the capacity information after resizing.

----End

3.4 Quotas

What Is Quota?

Quotas can limit the number or amount of resources available to users, such as the maximum number of ECS or EVS disks that can be created.

If the existing resource quota cannot meet your service requirements, you can apply for a higher quota.

How Do I View My Quotas?

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the desired region and project.
3. In the upper right corner of the page, click 📊 .

   The **Quotas** page is displayed.
4. View the used and total quota of each type of resources on the displayed page.

   If a quota cannot meet service requirements, apply for a higher quota.

How Do I Apply for a Higher Quota?

1. Log in to the management console.
2. In the upper right corner of the page, choose **Resources** > **My Quotas**.

   The **Quotas** page is displayed.
3. Click **Increase Quota** in the upper right corner of the page.
4. On the **Create Service Ticket** page, configure parameters as required.

   In the **Problem Description** area, fill in the content and reason for adjustment.
5. After all necessary parameters are configured, select **I have read and agree to the Ticket Service Protocol and Privacy Statement** and click **Submit**.

3.5 Encryption

Creating an Encrypted File System

To use the file system encryption function, you can directly select the encryption function when creating an SFS Turbo file system. Authorization is not required. For details, see **File System Encryption**.

You can create an encrypted or non-encrypted file system, but you cannot change the encryption settings of an existing file system.

For details about how to create an encrypted file system, see **Create a File System**.

Unmounting an Encrypted File System

If the custom key used by the encrypted file system is disabled or scheduled for deletion, the file system can only be used within a certain period of time (30s by default). Exercise caution in this case.

For details about how to unmount a file system, see **Unmount a File System**

3.6 Backup

You can back up SFS Turbo file systems using CBR.

Scenarios

A backup is a complete copy of an SFS Turbo file system at a specific time and it records all configuration data and service data at that time.

For example, if a file system is faulty or encounters a logical error (for example, mis-deletion, hacker attacks, and virus infection), you can use data backups to restore data quickly.

Creating a File System Backup

Ensure that the target file system is available. Or, the backup task cannot start. This procedure describes how to manually create a file system backup.

NOTE

> If any modification is made to a file system during the backup, inconsistencies may occur. For example, there may be duplicate or deleted data, or data discrepancies. Such a modification includes a write, rename, move or delete. To ensure backup data consistency, you are advised to stop the applications or programs that use the file system during the backup, or schedule the backup at off-peak hours.

Step 1 In the navigation pane on the left, choose **SFS Turbo Backups**.

Step 2 Create a backup vault by referring to section "Creating an SFS Turbo Backup Vault" and then create a backup by referring to section "Creating an SFS Turbo Backup" in the *Cloud Backup and Recovery User Guide*.

Step 3 The system automatically backs up the file system.

You can view the backup creation status on the **Backups** tab page. When the **Status** of the backup changes to **Available**, the backup has been created.

Step 4 If the file system becomes faulty or an error occurred, you can restore the backup data to a new file system. For details, see **Using a Backup to Create a File System**.

----End

Using a Backup to Create a File System

In case of a virus attack, accidental deletion, or software or hardware fault, you can use an SFS Turbo file system backup to create a new file system. Data on the new file system is the same as that in the backup.

Step 1 Log in to CBR Console.

1. Log in to the management console.
2. Click 📍 in the upper left corner and select your desired region and project.
3. Choose **Storage** > **Cloud Backup and Recovery** > **SFS Turbo Backups**.

Step 2 Click the **Backups** tab and locate the desired backup.

Step 3 If the status of the target backup is **Available**, click **Create File System** in the **Operation** column of the backup.

Step 4 Set the file system parameters.

NOTE

- For detailed parameter descriptions, see table "Parameter description" under **Table 2-1**.

Step 5 Click **Next**.

Step 6 Go back to the file system list and check whether the file system is successfully created.

You will see the file system status change as follows: **Creating**, **Available**, **Restoring**, **Available**. You may not notice the **Restoring** status because Instant Restore is supported and the restoration speed is very fast. After the file system status has changed from **Creating** to **Available**, the file system is successfully created. After the status has changed from **Restoring** to **Available**, backup data has been successfully restored to the created file system.

----End

3.7 Encrypted Transmission

Overview

Encrypted transmission allows you to protect your data transmitted between clients and SFS Turbo file systems using the TLS protocol.

As data needs to be encrypted and decrypted, you may experience a slight decrease in performance when encrypted transmission is used.

Configuring Encrypted Transmission and Mounting the File System (Linux)

1. **Install stunnel.**

   Stunnel is an open-source proxy designed to add TLS encryption functionality to existing clients and servers without any changes in the programs' code. It listens to local ports, encrypts the received traffic, and forwards the encrypted traffic to SFS Turbo file systems. To use encrypted transmission, you need to install stunnel first.

   – Run the following commands to install stunnel in Ubuntu or Debian:

```
sudo apt update
sudo apt-get install stunnel
```

   – Run the following command to install stunnel in CentOS, EulerOS, or Huawei Cloud EulerOS:

```
sudo yum install stunnel
```

NOTE

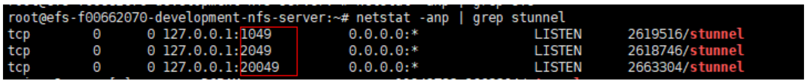
Stunnel 5.56 or later is recommended.

2. **Select an idle port as the local listening port.**

   Run the following command to view occupied local ports:

   ```
   netstat -anp | grep 127.0.0.1
   ```

   Figure 3-2 Viewing occupied local ports

   ```
   root@efs-f00662070-development-nfs-server:~# netstat -anp | grep stunnel
   tcp        0      0 127.0.0.1:1049          0.0.0.0:*               LISTEN      2619516/stunnel
   tcp        0      0 127.0.0.1:2049          0.0.0.0:*               LISTEN      2618746/stunnel
   tcp        0      0 127.0.0.1:20049         0.0.0.0:*               LISTEN      2663304/stunnel
   ```

   In this example, port 20049 has been used. Select an idle port ranging from 20050 to 21049.

3. **Configure the stunnel configuration file.**

   Create a **stunnel_*[Local listening port]*.conf** file in **/etc/stunnel** and add the following content to the file:

   ```
   client = yes
   sslVersion = TLSv1.2
   [nfs]
   ciphers = ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256
   accept = 127.0.0.1:[Local listening port]
   connect = [dns name]:2052
   ```

4. **Start the stunnel process.**

   ```
   stunnel /etc/stunnel/stunnel_[local listening port].conf
   ```

5. **Mount the file system.**

   ```
   mount -t nfs -o vers=3,nolock,tcp,port=[Local listening port],mountport=[Local listening port]
   127.0.0.1:/ [Mount point]
   ```

   All file operations on this mount point are the same as those in non-encrypted transmission scenarios.

   NOTE

   If the stunnel process exits abnormally, file operations will be suspended. You can use Linux functionalities such as crontab to ensure that the stunnel process can be automatically started after it exits.

Dependency Components

Stunnel and crontab

FAQ

- Why Can't the Stunnel Process Be Started?

  The stunnel process cannot be started if the port is occupied. If the following message is returned when stunnel is started, the port has been occupied:

  ```
  Binding service [nfs] to 127.0.0.1: (occupied port): Address already in use
  ```

3.8 Monitoring

3.8.1 SFS Turbo Metrics

Function

This section describes metrics reported by SFS Turbo to Cloud Eye as well as their namespaces and dimensions. You can use the console or APIs provided by Cloud Eye to query the metrics generated for SFS Turbo.

Namespace

SYS.EFS

Metrics

Table 3-3 SFS Turbo metrics

Metric ID	Metric Name	Description	Value Range	Unit	Conversion Rule	Monitored Object (Dimension)	Monitoring Period (Raw Data)
client_connections	File System Client Connections	Number of client connections **NOTE** Only active client connections are counted. A network connection is automatically disconnected when the client has no I/Os for a long time and is automatically re-established when there are I/Os.	≥ 0	count	N/A	SFS Turbo file system	1 minute
data_read_io_bytes	Read Bandwidth	Data read I/O load	≥ 0	bytes/s	1024 (IEC)	SFS Turbo file system	1 minute
data_write_io_bytes	Write Bandwidth	Data write I/O load	≥ 0	bytes/s	1024 (IEC)	SFS Turbo file system	1 minute

Metric ID	Metric Name	Description	Value Range	Unit	Conversion Rule	Monitored Object (Dimension)	Monitoring Period (Raw Data)
metadata_io_bytes	Metadata Read and Write Bandwidth	Metadata read and write I/O load	≥ 0	bytes/s	1024 (IEC)	SFS Turbo file system	1 minute
total_io_bytes	Total Bandwidth	Total I/O load	≥ 0	bytes/s	1024 (IEC)	SFS Turbo file system	1 minute
iops	IOPS	I/O operations per unit time	≥ 0	count	N/A	SFS Turbo file system	1 minute
used_capacity	Used Capacity	Used capacity of a file system	≥ 0	byte	1024 (IEC)	SFS Turbo file system	1 minute
used_capacity_percent	Capacity Usage	Percentage of used capacity in the total capacity	0 - 100	%	N/A	SFS Turbo file system	1 minute
used_inode	Used Inode	Number of inodes used in a file system	≥ 1	count	N/A	SFS Turbo file system	1 minute
used_inode_percent	Used Inode	Percentage of used inodes to total inodes in a file system	0 - 100	%	N/A	SFS Turbo file system	1 minute

Dimension

Key	Value
efs_instance_id	Instance

Viewing Monitoring Statistics

Step 1 Log in to the management console.

Step 2 View the monitoring graphs using either of the following methods.

- Method 1: Choose **Service List** > **Storage** > **Scalable File Service**. In the file system list, click **View Metric** in the **Operation** column of the target file system.
- Method 2: Choose > **Cloud Eye** > **Cloud Service Monitoring** > **SFS Turbo**. In the file system list, click **View Metric** in the **Operation** column of the desired file system.

Step 3 View the SFS Turbo file system monitoring data by metric or monitored duration.

For more information about Cloud Eye, see the *Cloud Eye User Guide*.

----End

3.9 Auditing

3.9.1 Supported SFS Operations

Scenarios

Cloud Trace Service (CTS) records operations of SFS resources, facilitating query, audit, and backtracking.

Prerequisites

You have enabled CTS and the tracker is normal. For details about how to enable CTS, see section "Enabling CTS" in the *Cloud Trace Service User Guide.*

Operations

Table 3-4 SFS Turbo operations traced by CTS

Operation	Resource Type	Trace
Creating a file system	sfs_turbo	createShare
Deleting a file system	sfs_turbo	deleteShare

Querying Traces

Step 1 Log in to the management console.

Step 2 Click 📍 in the upper left corner and select a region and project.

Step 3 Choose **Management & Deployment** > **Cloud Trace Service**.

The **Cloud Trace Service** page is displayed.

Step 4 In the navigation pane on the left, choose **Trace List**.

Step 5 On the trace list page, set **Trace Source**, **Resource Type**, and **Search By**, and click **Query** to query the specified traces.

For details about other operations, see section "Querying Real-Time Traces" in the *Cloud Trace Service User Guide*.

----End

Disabling or Enabling a Tracker

This section describes how to disable an existing tracker on the CTS console. After the tracker is disabled, the system will stop recording operations, but you can still view existing operation records.

Step 1 Log in to the management console.

Step 2 Choose **Management & Deployment** > **Cloud Trace Service**.

The **Cloud Trace Service** page is displayed.

Step 3 Click **Trackers** in the left pane.

Step 4 Click **Disable** on the right of the tracker information.

Step 5 Click **Yes**.

Step 6 After the tracker is disabled, the available operation changes from **Disable** to **Enable**. To enable the tracker again, click **Enable** and then click **Yes**. The system will start recording operations again.

----End

4 Typical Applications

4.1 Enterprise Website/App Background

Context

For I/O-intensive website services, SFS Turbo can provide shared website source code directories and storage for multiple web servers, enabling low-latency and high-IOPS concurrent share access. Features of such services are as follows:

- A large number of small files: Static website files need to be stored, including HTML files, JSON files, and static images.
- Read I/O intensive: Scope of data reading is large, and data writing is relatively small.
- Multiple web servers access an SFS Turbo background to achieve high availability of website services.

Configuration Process

1. Sort out the website files.
2. Log in to the SFS console. Create an SFS Turbo file system to store the website files.
3. Log in to the ECSs that function as compute nodes and mount the file system.
4. On the head node, upload the files to the file system.
5. Start the web server.

Prerequisites

- A VPC has been created.
- ECSs that function as head nodes and compute nodes have been created, and have been assigned to the VPC.
- SFS has been enabled.

Example Configuration

Step 1 Log in to the SFS console.

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

Step 3 On the **Create File System** page, set parameters as instructed.

Step 4 To mount a file system to Linux ECSs, see **Mounting an NFS File System to ECSs (Linux)**. To mount a file system to Windows ECSs, see **Mounting an NFS File System to ECSs (Windows)**.

Step 5 Log in to the head node and upload the files to the file system.

Step 6 Start the web server.

----End

4.2 Log Printing

Context

SFS Turbo can provide multiple service nodes for shared log output directories, facilitating log collection and management of distributed applications. Features of such services are as follows:

- A shared file system is mounted to multiple service hosts and logs are printed concurrently.
- Large file size and small I/O: The size of a single log file is large, but the I/O of each log writing is small.
- Write I/O intensive: Write I/O of small blocks is the major service.

Configuration Process

1. Log in to the SFS console. Create an SFS Turbo file system to store the log files.
2. Log in to the ECSs that function as compute nodes and mount the file system.
3. Configure the log directory to the shared file system. It is recommended that each host use different log files.
4. Start applications.

Prerequisites

- A VPC has been created.
- ECSs that function as head nodes and compute nodes have been created, and have been assigned to the VPC.
- SFS has been enabled.

Example Configuration

Step 1 Log in to the SFS console.

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

Step 3 On the **Create File System** page, set parameters as instructed.

Step 4 To mount a file system to Linux ECSs, see **Mounting an NFS File System to ECSs (Linux)**. To mount a file system to Windows ECSs, see **Mounting an NFS File System to ECSs (Windows)**.

Step 5 Configure the log directory to the shared file system. It is recommended that each host use different log files.

Step 6 Start applications.

----End

5 Troubleshooting

5.1 Mounting a File System Times Out

Symptom

When a file system is mounted to servers using the **mount** command, message **timed out** is displayed.

Possible Causes

- Cause 1: The network status is not stable.
- Cause 2: The network connection is abnormal.
- Cause 3: The server that mounts the file system runs Ubuntu18 or later.

Fault Diagnosis

After the network fault is excluded, run the **mount** command again.

Solution

- Cause 1 and Cause 2: The network status is not stable or the network connection is abnormal.

  Re-mount the file system after the network issue is addressed.

  - If the patch is uninstalled successfully, no further action is required.
  - If the problem persists, see the solution for cause 3.
- Cause 3: The server that mounts the file system runs Ubuntu18 or later.
  a. Check whether the server running Ubuntu18 or later was created from a private image.
     - If yes, go to **c**.
     - If no, go to **b**.

  b. Convert the public image server to a private image server.

   i. Create a private image based on the existing ECS. For details, see section "Creating an Image" in the Elastic Cloud Server User Guide.
   ii. Use the private image created in **b.i** to create an ECS or change the ECS OS to the private image created in **b.i**. For details, see section "Changing the OS" in the *Elastic Cloud Server User Guide*.

c. Log in to the server and mount the file system again.

5.2 Mounting a File System Fails

Symptom

When a file system is mounted to servers using the **mount** command, message **access denied** is displayed.

Possible Causes

- Cause 1: The file system has been deleted.
- Cause 2: The server and the mounted file system are not in the same VPC.
- Cause 3: The mount point in the **mount** command is incorrect.
- Cause 4: The IP address used for accessing SFS is a virtual IP address.

Fault Diagnosis

Take troubleshooting measures based on possible causes.

Solution

- Cause 1: The file system has been deleted.

  Log in to the management console and check whether the file system has been deleted.

  – If yes, create a file system or select an existing file system to mount. Ensure that the server and the file system reside in the same VPC.
  – If no, go to Cause 2.
- Cause 2: The server and the mounted file system are not in the same VPC.

  Log in to the management console and check whether the server and the file system are in the same VPC.

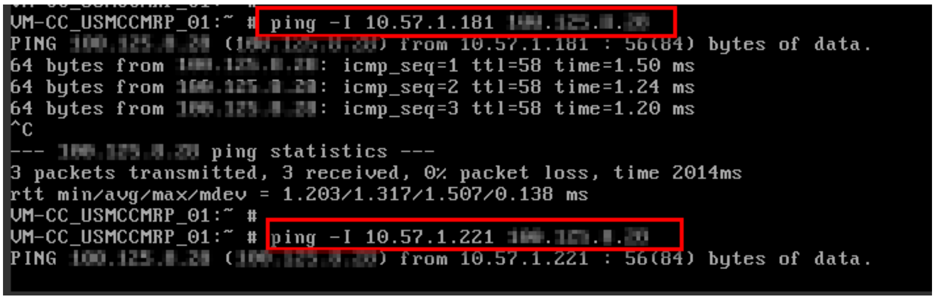
  – If yes, go to Cause 3.
  – If no, select a file system that is in the same VPC as the server.
- Cause 3: The mount point in the **mount** command is incorrect.

  a. Log in to the management console and check whether the mount point is the same as the one in the **mount** command.
  b. If the mount point in the **mount** command is incorrectly entered, correct it and run the command again.
- Cause 4: The IP address used for accessing SFS is a virtual IP address.

  Log in to the server and run the **ping** command and use the server IP address to access SFS. Check whether the service is reachable. See **Figure 5-1**.

- If yes, the network problem has been resolved. Check other possible causes.
- If no, the network is disconnected. Use the server's private IP address and the **ping** command to access SFS and check whether the service is reachable.

Figure 5-1 Running the ping command to access SFS



```
VM-CC_USMCCMRP_01:~ # ping -I 10.57.1.181 [redacted]
PING [redacted] ([redacted]) from 10.57.1.181 : 56(84) bytes of data.
64 bytes from [redacted]: icmp_seq=1 ttl=58 time=1.50 ms
64 bytes from [redacted]: icmp_seq=2 ttl=58 time=1.24 ms
64 bytes from [redacted]: icmp_seq=3 ttl=58 time=1.20 ms
^C
--- [redacted] ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2014ms
rtt min/avg/max/mdev = 1.203/1.317/1.507/0.138 ms
VM-CC_USMCCMRP_01:~ #
VM-CC_USMCCMRP_01:~ # ping -I 10.57.1.221 [redacted]
PING [redacted] ([redacted]) from 10.57.1.221 : 56(84) bytes of data.
```

5.3 Failed to Create an SFS Turbo File System

Symptom

An SFS Turbo file system fails to be created.

Fault Diagnosis

The following fault causes are sequenced based on their occurrence probability.

If the fault persists after you have ruled out one cause, move on to the next one in the list.

Figure 5-2 Fault diagnosis

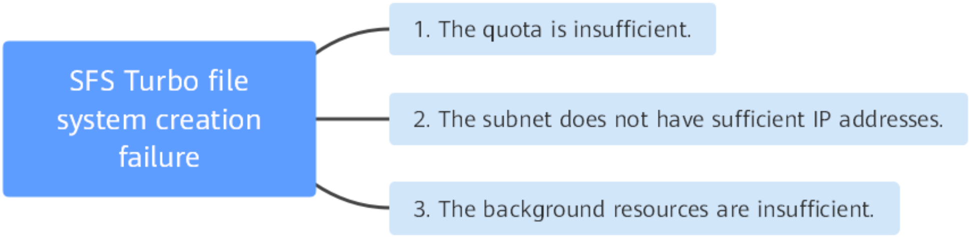

SFS Turbo file system creation failure
1. The quota is insufficient.
2. The subnet does not have sufficient IP addresses.
3. The background resources are insufficient.

Table 5-1 Fault diagnosis

Possible Cause	Solution
The quota is insufficient.	The number of created file systems has reached the upper limit. See **Quotas** to increase the quota.

Possible Cause	Solution
The subnet does not have sufficient IP addresses.	If the IP addresses in the subnet are insufficient, change the subnet or release IP addresses in the subnet.
The background resources are insufficient.	Background resources, such as compute and storage resources, have reached the upper limit. for technical consultation.

5.4 A File System Is Automatically Disconnected from the Server

Symptom

A file system is disconnected from the server and needs to be mounted again.

Possible Causes

Automatic mounting is not configured. The server is automatically disconnected from the file system after restart.

Solution

Configure auto mount on the server by referring to **Mounting a File System Automatically**.

5.5 A Server Fails to Access a File System

Symptom

Access from a server to a file system was denied. All services on the server were abnormal.

Possible Causes

- Cause 1: The file system is abnormal.
- Cause 2: After a forcible unmount operation on the server, mount fails.

Fault Diagnosis

Take troubleshooting measures based on possible causes.

Solution

- Cause 1: The file system is abnormal.

  Log in to the management console. On the **Scalable File System** page, check whether the file system is in the **Available** state.

  - If yes, go to Cause 2.
  - If no, see **The File System Is Abnormal** to restore the file system to the available state, and then access the file system again.
- Cause 2: After a forcible unmount operation on the server, mount fails.
  a. This problem is caused by a defect of servers. Restart the server to resolve this problem.
  b. Check whether the file system can be properly mounted and accessed.
     - If yes, no further action is required.
     - If no, contact technical support.

5.6 The File System Is Abnormal

Currently, the file system exceptions include reduction error, reduction failure deletion error, and expansion error. When the file system is in these statuses, refer to the following handling suggestions.

Table 5-2 Measures for handling file system abnormalities

Exception	Suggestion
Deletion error	When the file system is in the deletion error status, it can automatically recover to the available state. If the status cannot be restored to available, contact the administrator.
Expansion error	When the file system is in the expansion error status, it can automatically recover to the available state. If the status cannot be restored to available, contact the administrator.
Reduction error	When the file system is in the reduction error status, it takes approximately five minutes for the file system to restore to the available state.
Reduction failure	When the file system is in the reduction failure status, it takes approximately five minutes for the file system to restore to the available state.

5.7 Data Fails to Be Written into a File System Mounted to ECSs Running Different Types of Operating Systems

A file system can be mounted to a Linux ECS and a Windows ECS. However, data may fail to be written to the file system.

Symptom

If a file system is mounted to a Linux ECS and a Windows ECS, on the Windows ECS, data cannot be written to the files created by the Linux ECS.

Possible Causes

A shared NFS file system belongs to the root user and cannot be modified. The write permission is granted to a user only when both the values of UID and GID of the user are **0**. You can check your UID using Windows commands. If the value of UID is, for example, **-2**, you do not have the write permission.

Fault Diagnosis

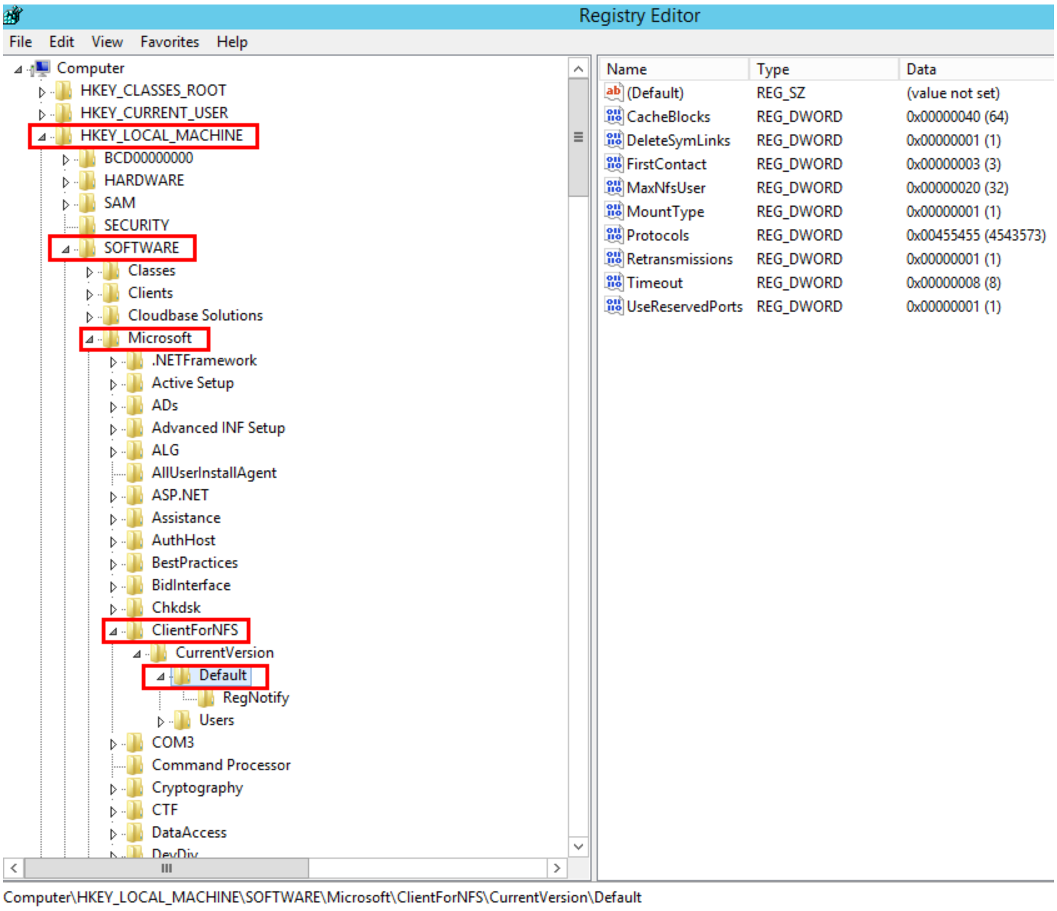
To address this problem, modify the registry and change both UID and GID values to **0** for NFS accesses from Windows.

Solution

Step 1 Choose **Start** > **Run** and enter **regedit** to open the registry.

Step 2 Enter the **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ClientForNFS\CurrentVersion\Default** directory. **Figure 5-3** shows an example of the directory.

Figure 5-3 Entering the directory

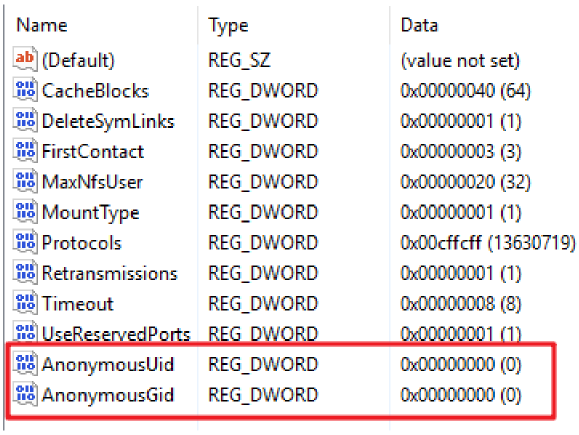


Name	Type	Data
(Default)	REG_SZ	(value not set)
CacheBlocks	REG_DWORD	0x00000040 (64)
DeleteSymLinks	REG_DWORD	0x00000001 (1)
FirstContact	REG_DWORD	0x00000003 (3)
MaxNfsUser	REG_DWORD	0x00000020 (32)
MountType	REG_DWORD	0x00000001 (1)
Protocols	REG_DWORD	0x00455455 (4543573)
Retransmissions	REG_DWORD	0x00000001 (1)
Timeout	REG_DWORD	0x00000008 (8)
UseReservedPorts	REG_DWORD	0x00000001 (1)

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ClientForNFS\CurrentVersion\Default

Step 3 Right-click the blank area and choose **New** > **DWORD Value** from the shortcut menu. Set **AnonymousUid** and **AnonymousGid** to **0**. **Figure 5-4** shows a successful operation.

Figure 5-4 Adding values



Name	Type	Data
(Default)	REG_SZ	(value not set)
CacheBlocks	REG_DWORD	0x00000040 (64)
DeleteSymLinks	REG_DWORD	0x00000001 (1)
FirstContact	REG_DWORD	0x00000003 (3)
MaxNfsUser	REG_DWORD	0x00000020 (32)
MountType	REG_DWORD	0x00000001 (1)
Protocols	REG_DWORD	0x00cffcff (13630719)
Retransmissions	REG_DWORD	0x00000001 (1)
Timeout	REG_DWORD	0x00000008 (8)
UseReservedPorts	REG_DWORD	0x00000001 (1)
AnonymousUid	REG_DWORD	0x00000000 (0)
AnonymousGid	REG_DWORD	0x00000000 (0)

Step 4 After modifying the registry, restart the server for the modification to take effect.

----End

5.8 Failed to Mount an NFS File System to a Windows IIS Server

Symptom

When an NFS file system is mounted to a Windows IIS server, an error message is displayed, indicating that the path format is not supported, and the mounting fails.

Possible Causes

The physical path of the IIS Web server is incorrect.

Fault Diagnosis

Take troubleshooting measures based on possible causes.

Solution

Step 1 Log in to the ECS. An ECS running Windows Server 2012 R2 is used in this example.

Step 2 Click **Server Manager** in the lower left corner.

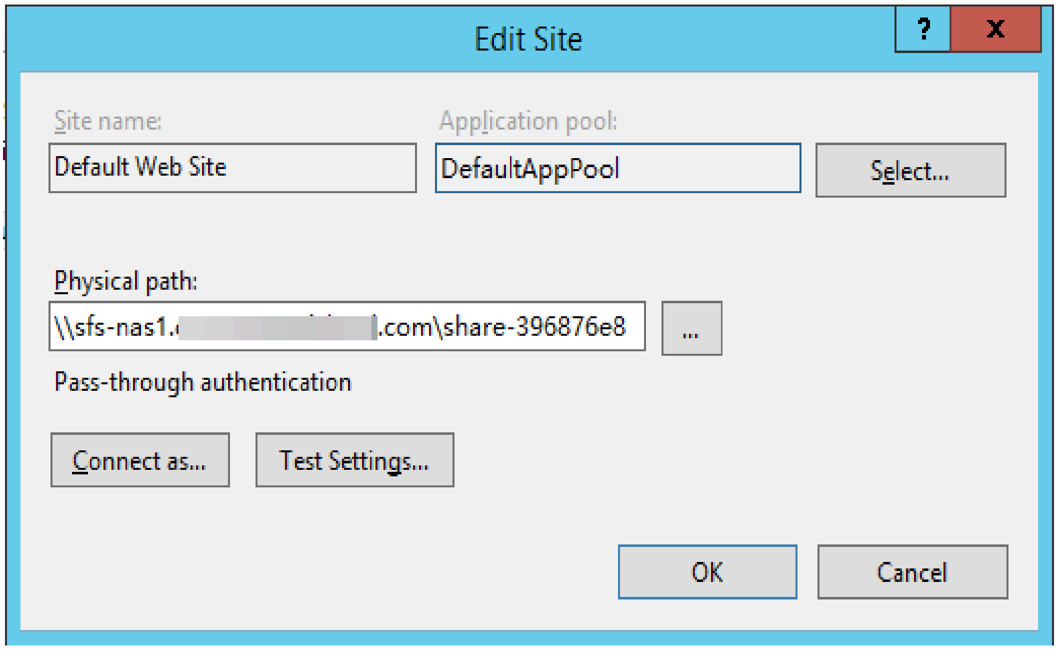
Step 3 Choose **Tools** > **Internet Information Services (IIS) Manager**, expand **Sites**, and select the target website.

Step 4 Click **Basic Settings** to check whether the **Physical path** is correct.

Step 5 The correct physical path is that of the mount point with the colon (:) deleted.

You need to enter the physical path **\\sfs-nas1.example.com\share-396876e8**, as shown in **Figure 5-5**.

Figure 5-5 Physical path



Site name: Default Web Site

Application pool: DefaultAppPool

Physical path: \\sfs-nas1.[redacted].com\share-396876e8

Pass-through authentication

----End

5.9 Writing to a File System Fails

Symptom

Data fails to be written to the file system mounted to ECSs running the same type of operating system.

Possible Causes

The ECS security group configuration is incorrect. The port used to communicate with the file system is not enabled.

Fault Diagnosis

Check whether the port of the target server is enabled and correctly configure the port on the security group console.

Solution

Step 1 Log in to the ECS console.

1. Log in to the management console.
2. Click 📍 in the upper left corner and select your desired region and project.
3. Under **Compute**, choose **Elastic Cloud Server**.

Step 2 In the navigation pane on the left, choose **Elastic Cloud Server**. On the page displayed, select the target server. Go to the server details page.

Step 3 Click the **Security Groups** tab and select the target security group. Click **Manage Rule** to go to the security group console.

Step 4 On the displayed page, click the **Inbound Rules** tab and click **Add Rule**. The **Add Inbound Rule** page is displayed. Add rules as follows:

After an SFS Turbo file system is created, the system automatically enables the security group port required by the NFS protocol. This ensures that the SFS Turbo file system can be accessed by your servers 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.

You are advised to use an independent security group for an SFS Turbo file system to isolate it from service nodes.

Step 5 Click **OK**. Access the file system again for verification.

----End

5.10 Error Message "wrong fs type, bad option" Is Displayed During File System Mounting

Symptom

The message "wrong fs type, bad option" is displayed when you run the **mount** command to mount a file system to an ECS running Linux.

Possible Causes

An NFS client is not installed on the Linux ECS. That is, the **nfs-utils** software package is not installed before you execute the **mount** command.

Fault Diagnosis

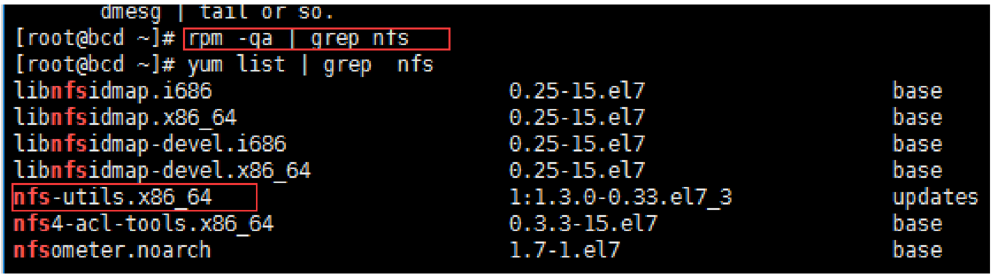
Install the required **nfs-utils** software package.

Solution

Step 1 Log in to the ECS and check whether the **nfs-utils** package is installed. Run the following command. If no command output is displayed, the package is not installed.

```
rpm -qa|grep nfs
```

Figure 5-6 Checking whether the software package has been installed

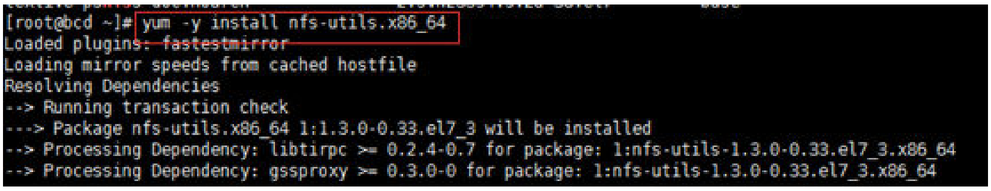


```
       dmesg | tail or so.
[root@bcd ~]# rpm -qa | grep nfs
[root@bcd ~]# yum list | grep  nfs
libnfsidmap.i686                        0.25-15.el7                   base
libnfsidmap.x86_64                      0.25-15.el7                   base
libnfsidmap-devel.i686                  0.25-15.el7                   base
libnfsidmap-devel.x86_64                0.25-15.el7                   base
nfs-utils.x86_64                        1:1.3.0-0.33.el7_3            updates
nfs4-acl-tools.x86_64                   0.3.3-15.el7                  base
nfsometer.noarch                        1.7-1.el7                     base
```

Step 2 Run the following command to install the nfs-utils software package:

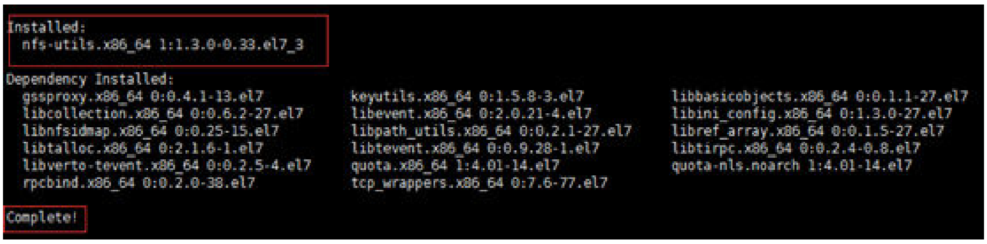
```
yum -y install nfs-utils
```

Figure 5-7 Executing the installation command



```
[root@bcd ~]# yum -y install nfs-utils.x86_64
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
Resolving Dependencies
--> Running transaction check
---> Package nfs-utils.x86_64 1:1.3.0-0.33.el7_3 will be installed
--> Processing Dependency: libtirpc >= 0.2.4-0.7 for package: 1:nfs-utils-1.3.0-0.33.el7_3.x86_64
--> Processing Dependency: gssproxy >= 0.3.0-0 for package: 1:nfs-utils-1.3.0-0.33.el7_3.x86_64
```

Figure 5-8 Successful installation



```
Installed:
  nfs-utils.x86_64 1:1.3.0-0.33.el7_3

Dependency Installed:
  gssproxy.x86_64 0:0.4.1-13.el7          keyutils.x86_64 0:1.5.8-3.el7           libbasicobjects.x86_64 0:0.1.1-27.el7
  libcollection.x86_64 0:0.6.2-27.el7     libevent.x86_64 0:2.0.21-4.el7          libini_config.x86_64 0:1.3.0-27.el7
  libnfsidmap.x86_64 0:0.25-15.el7        libpath_utils.x86_64 0:0.2.1-27.el7     libref_array.x86_64 0:0.1.5-27.el7
  libtalloc.x86_64 0:2.1.6-1.el7          libtevent.x86_64 0:0.9.28-1.el7         libtirpc.x86_64 0:0.2.4-0.8.el7
  libverto-tevent.x86_64 0:0.2.5-4.el7    quota.x86_64 1:4.01-14.el7              quota-nls.noarch 1:4.01-14.el7
  rpcbind.x86_64 0:0.2.0-38.el7           tcp_wrappers.x86_64 0:7.6-77.el7

Complete!
```

Step 3 Run the **mount** command again to mount the file system to the ECS.

```
mount -t nfs -o vers=3,timeo=600,noresvport,nolock Mount point Local path
```

Step 4 Run the following command to view the mounted file system:

mount -l

If the command output contains the following information, the file system is mounted successfully.

```
example.com:/share-xxx on /local_path type nfs (rw,vers=3,timeo=600,nolock,addr=)
```

----End

5.11 Failed to Access the Shared Folder in Windows

Symptom

When you mount a file system to an ECS running Windows, the system displays a message "You cannot access this shared folder because your organization's security policies block unauthenticated guest access. These policies help to protect you PC from unsafe or malicious devices on the network."

Possible Causes

Guest access to CIFS file systems is blocked or disabled.

Fault Diagnosis

Solution 1: Manually enable guest access.

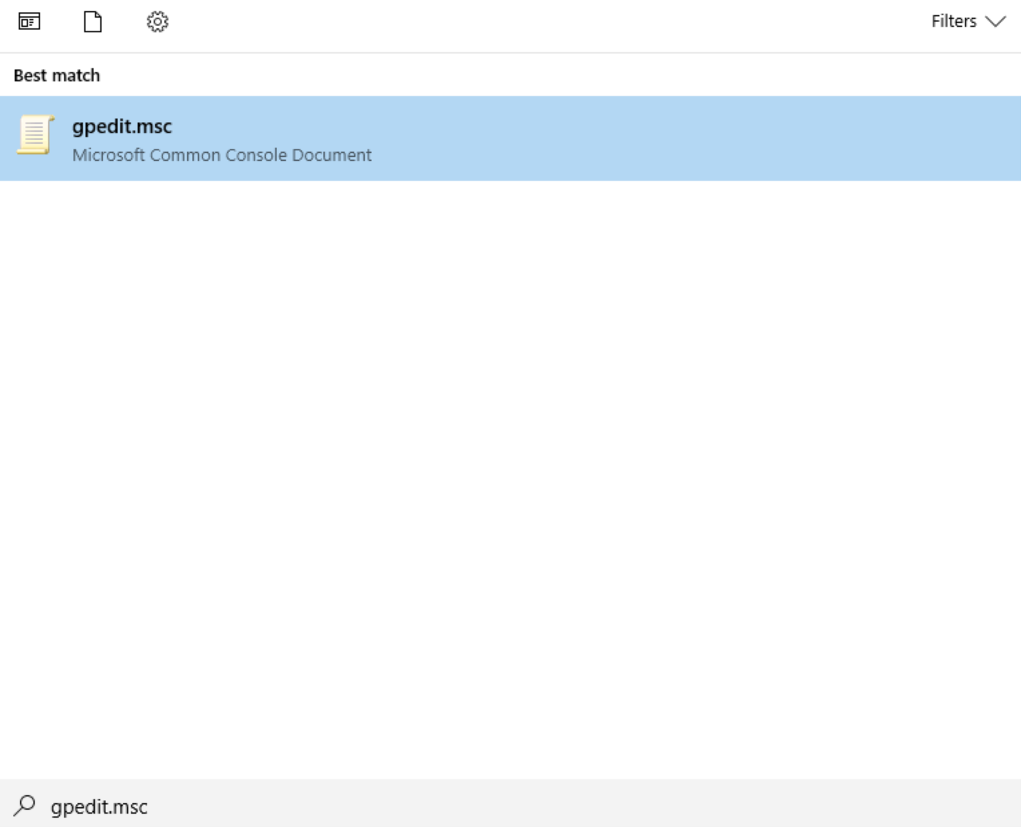
Solution 2: Modify the registry to allow guest access (suitable for versions later than Windows Server 2016).

Solution

Solution 1: Manually enable guest access.

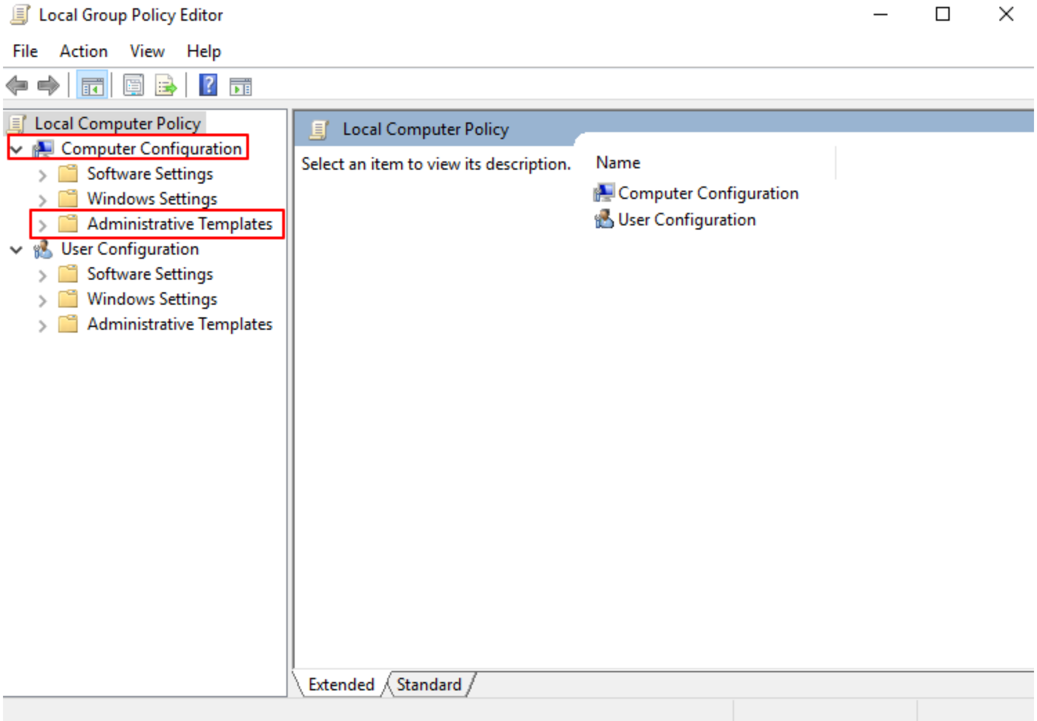
Step 1 Open **Run** command box, enter **gpedit.msc**, and press **Enter** to start **Local Group Policy Editor**.

Figure 5-9 Entering gpedit.msc



Step 2 On the **Local Group Policy Editor** page, choose **Computer Configuration** > **Administrative Templates**.

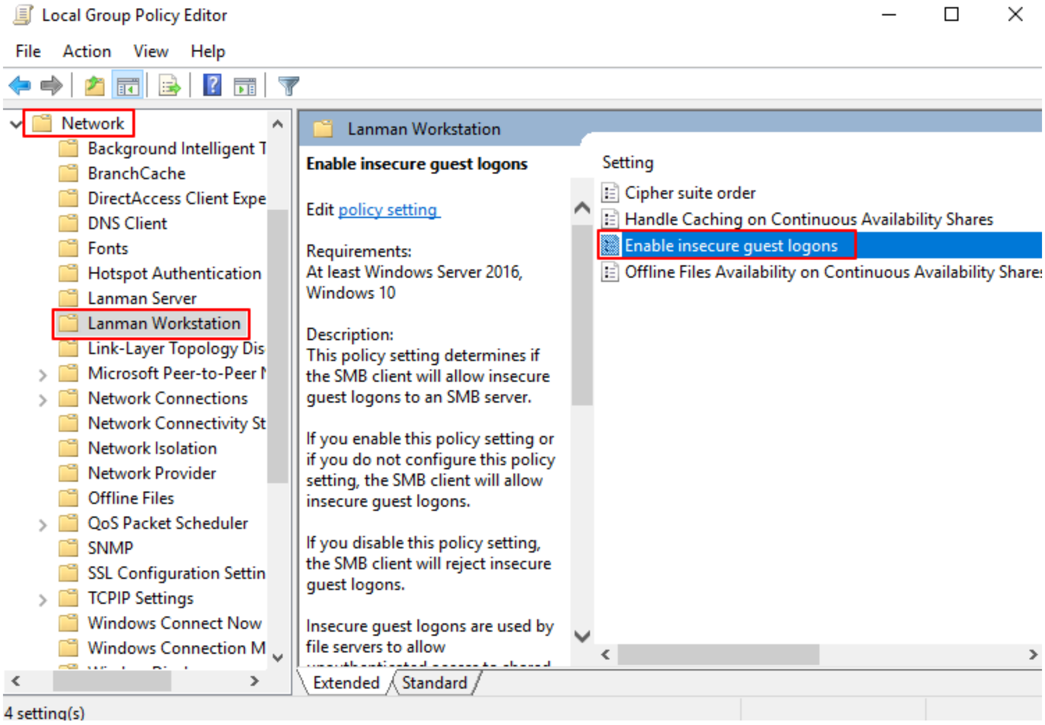
Figure 5-10 Local Group Policy Editor



Select an item to view its description.

Step 3 Under **Administrative Templates**, choose **Network** > **Lanman Workstation** and find the option of **Enable insecure guest logons**.

Figure 5-11 Locating the option



Enable insecure guest logons

Edit policy setting

Requirements:
At least Windows Server 2016, Windows 10

Description:
This policy setting determines if the SMB client will allow insecure guest logons to an SMB server.

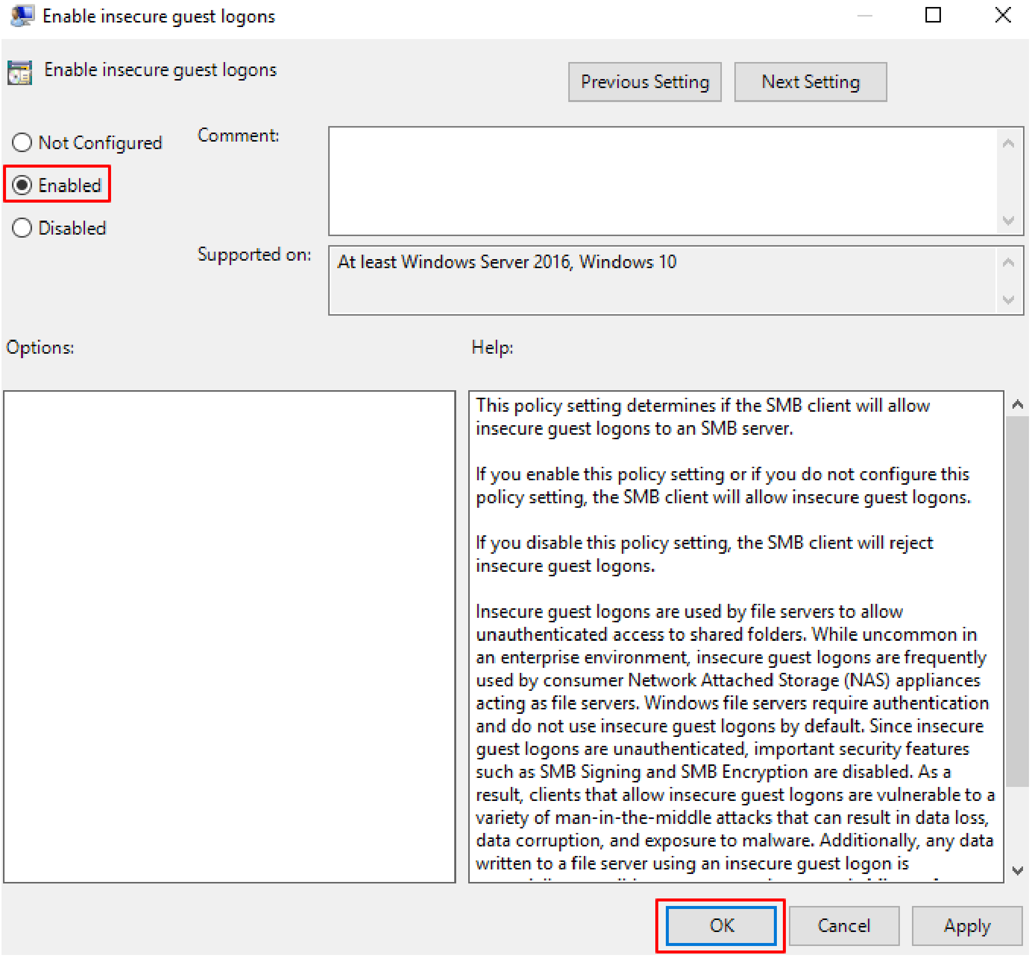
If you enable this policy setting or if you do not configure this policy setting, the SMB client will allow insecure guest logons.

If you disable this policy setting, the SMB client will reject insecure guest logons.

Insecure guest logons are used by file servers to allow

Step 4 Double-click **Enable insecure guest logons**. Select **Enabled** and click **OK**.

Figure 5-12 Enabling insecure guest logons



Enable insecure guest logons

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Windows Server 2016, Windows 10

Options:

Help:

This policy setting determines if the SMB client will allow insecure guest logons to an SMB server.

If you enable this policy setting or if you do not configure this policy setting, the SMB client will allow insecure guest logons.

If you disable this policy setting, the SMB client will reject insecure guest logons.

Insecure guest logons are used by file servers to allow unauthenticated access to shared folders. While uncommon in an enterprise environment, insecure guest logons are frequently used by consumer Network Attached Storage (NAS) appliances acting as file servers. Windows file servers require authentication and do not use insecure guest logons by default. Since insecure guest logons are unauthenticated, important security features such as SMB Signing and SMB Encryption are disabled. As a result, clients that allow insecure guest logons are vulnerable to a variety of man-in-the-middle attacks that can result in data loss, data corruption, and exposure to malware. Additionally, any data written to a file server using an insecure guest logon is

Step 5 After the access is enabled, mount the file system again. If the fault persists, contact technical support.

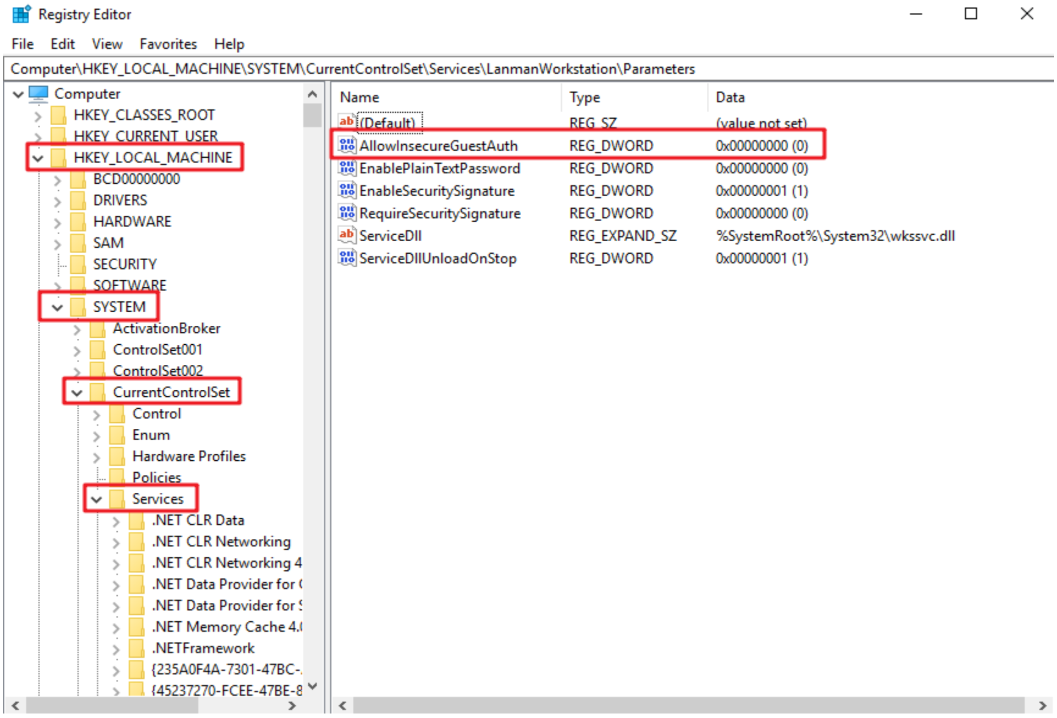
----End

Solution 2: Modify the registry to allow guest access (suitable for versions later than Windows Server 2016).

Step 1 Choose **Start** > **Run** and enter **regedit** to open the registry.

Step 2 Go to the **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters** directory.

Figure 5-13 Entering the registry

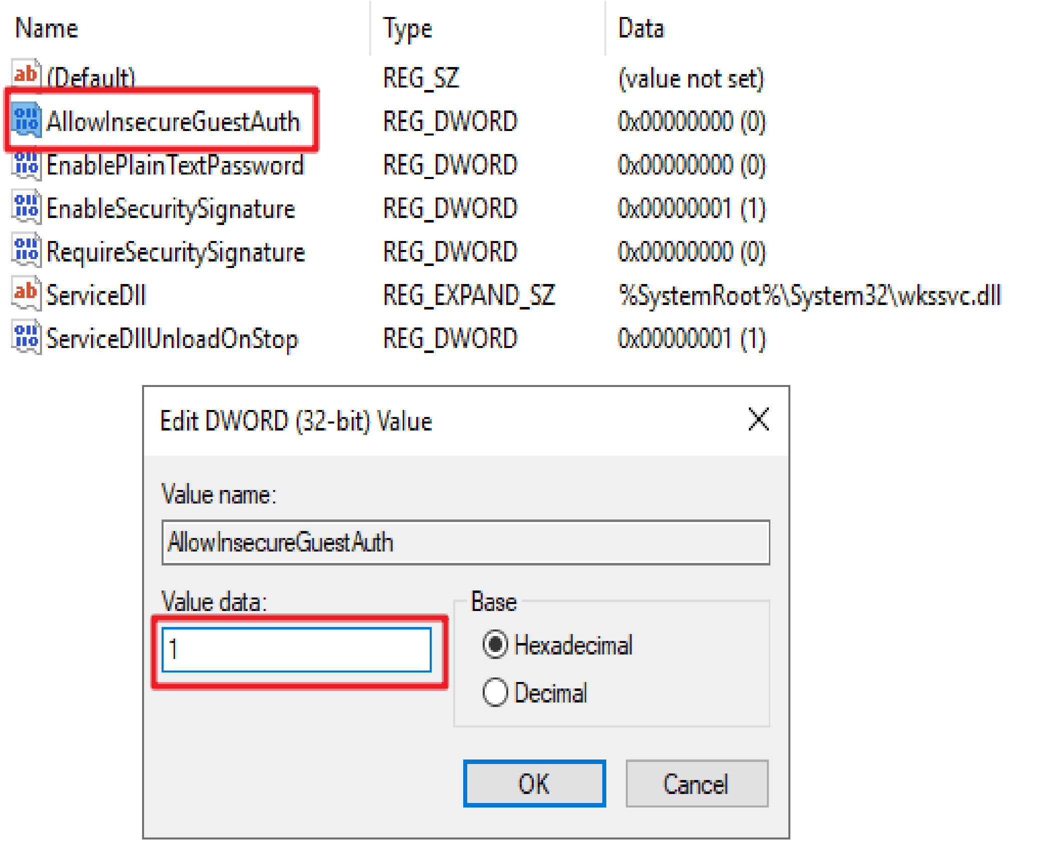


Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters

Name	Type	Data
(Default)	REG_SZ	(value not set)
AllowInsecureGuestAuth	REG_DWORD	0x00000000 (0)
EnablePlainTextPassword	REG_DWORD	0x00000000 (0)
EnableSecuritySignature	REG_DWORD	0x00000001 (1)
RequireSecuritySignature	REG_DWORD	0x00000000 (0)
ServiceDll	REG_EXPAND_SZ	%SystemRoot%\System32\wkssvc.dll
ServiceDllUnloadOnStop	REG_DWORD	0x00000001 (1)

Step 3 Right-click **AllowInsecureGuestAuth** and choose **Modify** from the shortcut menu. In the pop-up window, change the value to **1**.

Figure 5-14 Changing the value



Name	Type	Data
ab (Default)	REG_SZ	(value not set)
AllowInsecureGuestAuth	REG_DWORD	0x00000000 (0)
EnablePlainTextPassword	REG_DWORD	0x00000000 (0)
EnableSecuritySignature	REG_DWORD	0x00000001 (1)
RequireSecuritySignature	REG_DWORD	0x00000000 (0)
ab ServiceDll	REG_EXPAND_SZ	%SystemRoot%\System32\wkssvc.dll
ServiceDllUnloadOnStop	REG_DWORD	0x00000001 (1)

Edit DWORD (32-bit) Value

Value name:

AllowInsecureGuestAuth

Value data:

1

Base

● Hexadecimal

○ Decimal

----End

6 FAQs

6.1 Concepts

6.1.1 What Is SFS?

Scalable File Service (SFS) provides scalable, high-performance file storage. With SFS, you can enjoy shared file access spanning multiple ECSs. SFS supports the Network File System (NFS) protocol. You can seamlessly integrate existing applications and tools with the service.

SFS provides an easy-to-use graphical user interface (GUI). On the GUI, users can create and configure file systems, saving effort in deploying, resizing, and optimizing file systems.

In addition, SFS features high availability. It can be elastically expanded, and it performs better as its capacity grows. The service is suitable for a wide range of scenarios, including enterprise office, high-performance websites, and software development.

6.1.2 What Is SFS Turbo?

SFS Turbo provides high-performance file storage that can be expanded on demand. With SFS Turbo, you can enjoy shared file access spanning multiple ECSs. SFS Turbo supports the Network File System (NFS) protocol (only NFSv3). You can seamlessly integrate existing applications and tools with the service.

SFS Turbo provides an easy-to-use graphical user interface (GUI). On the GUI, users can create and configure file systems, saving effort in deploying, resizing, and optimizing file systems.

In addition, SFS Turbo features high reliability and availability. It can be elastically expanded, and it performs better as its capacity grows. The service is suitable for a wide range of scenarios, including enterprise office, high-performance websites, and software development. For details about SFS Turbo file system types, see **File System Types**.

6.2 Specifications

6.2.1 What Is the Maximum Size of a File That Can Be Stored in a File System?

For SFS Turbo file systems, the maximum supported size of a file is 16 TB.

6.2.2 What Access Protocols Are Supported by SFS?

SFS supports the standard network file protocol NFSv3.

6.2.3 How Many File Systems Can Be Created by Each Account?

Each account can create a maximum of 10 SFS Turbo file systems.

6.2.4 How Many Servers Can I Mount a File System To?

You can mount an SFS Turbo file system to a maximum of 3,000 servers.

6.3 Restrictions

6.3.1 Can the Capacity of a File System Be Expanded?

SFS Turbo file systems: support online capacity expansion. During the capacity expansion, mounting a file system may fail and the connection being used for mounting will experience about a 30-second (max. 3 minutes) I/O delay.

6.4 Networks

6.4.1 Can a File System Be Accessed Across VPCs?

Yes. An SFS Turbo file system allows two or more VPCs in the same region to interconnect with each other through VPC peering connection. In this case, different VPCs are in the same network, and ECSs in these VPCs can share the same file system. For more information about VPC peering connection, see "VPC Peering Connection" in *Virtual Private Cloud User Guide*.

6.4.2 Does the Security Group of a VPC Affect SFS?

A security group is a collection of access control rules for servers that have the same security protection requirements and are mutually trusted in a VPC. After a security group is created, you can create different access rules for the security group to protect the servers that are added to this security group. The default security group rule allows all outgoing data packets. Servers in a security group can access each other without the need to add rules. The system creates a security group for each cloud account by default. Users can also create custom security groups by themselves.

After an SFS Turbo file system is created, the system automatically enables the security group port required by the NFS protocol. This ensures that the SFS Turbo file system can be accessed by your servers 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.

You are advised to use an independent security group for an SFS Turbo file system to isolate it from service nodes.

Example Value

- Inbound rule

Direction	Protocol	Port Range	Source IP Address		Description
Inbound	TCP and UDP	111	IP Address	0.0.0.0/0 (All IP addresses are allowed. It can be modified.)	One port corresponds to one access rule. You need to add information to the ports one by one.

- Outbound rule

Direction	Protocol	Port Range	Source IP Address		Description
Outbound	TCP and UDP	111	IP Address	0.0.0.0/0 (All IP addresses are allowed. It can be modified.)	One port corresponds to one access rule. You need to add information to the ports one by one.

NOTE

Enter an IP address range using a mask. For example, enter **192.168.1.0/24**, and do not enter **192.168.1.0-192.168.1.255**. If the source IP address is 0.0.0.0/0, all IP addresses are allowed.

The bidirectional access rule must be configured for port 111. The inbound rule can be set to the front-end service IP range of SFS. You can obtain it by running the following command: **ping** *File system domain name or IP address* or **dig** *File system domain name or IP address*.

For ports 2049, 2050, 2051, and 2052, only the outbound rule needs to be added, which is the same as the outbound rule of port 111.

For the NFS protocol, add an inbound rule to open the TCP&UDP port 111, TCP ports 2049, 2051, and 2052, and UDP&TCP port 20048.

For the NFS protocol with UDP port 20048 not opened, the time required for mounting may become longer. In this case, you can use the **-o tcp** option in **mount** to avoid this issue.

6.5 Others

6.5.1 How Do I Access a File System from a Server?

To access your file system, install the NFS client on a Linux server and run the **mount** command to mount the file system. For a Windows server, install the NFS client, modify the NFS transfer protocol, and run the **mount** command to mount the file system. Then, you can share the files and directories of the file system.

6.5.2 How Do I Check Whether a File System on a Linux Server Is Available?

Log in to the server as the **root** user. Run the following command to list all available file systems with the specified domain name or IP address:

showmount -e *File system domain name or IP address*

6.5.3 What Resources Does SFS Occupy?

To ensure that file systems can be used properly, the service occupies the following resources:

- For SFS Turbo file systems:
  - When an SFS Turbo file system is created, two private IP addresses and one virtual IP address are created in the subnet entered by the user.
  - When an SFS Turbo file system is created, the inbound rules of ports 111, 445, 2049, 2051, 2052, and 20048 are enabled in the security group selected by the user. The default source IP address is 0.0.0.0/0. You can change the IP address as required.

When data is written to the folders of a file system, the running memory of the server is occupied, but the storage space of the server disk is not occupied. The file system uses independent space.

6.5.4 How Can I Migrate Data Between SFS and EVS?

Mount a file system and an EVS disk to the same ECS, and then manually replicate data between the file system and EVS disk.

6.5.5 Can I Directly Access SFS from On-premises Devices?

SFS Turbo supports on-premises access via Direct Connect or other methods. After network communication is established, you can access an SFS Turbo file system from your on-premises devices.

6.5.6 How Do I Delete .nfs Files?

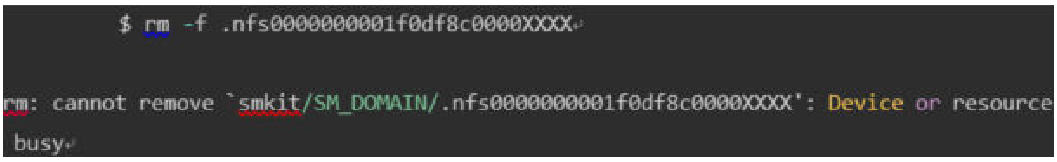
NFS .nfs Files

The .nfs files are temporary files in NFS. If you try to delete a file, and the file is still open, an .nfs file will appear. The .nfs files are used by NFS clients to manage the deletion of open files in the file system. If one process deletes a file while another process still has it open, the client will rename the file to .nfsxxx. If the last open to this file is closed, the client will automatically delete the file. If the client crashes before the file is cleared, the file will be left in the file system.

Clearing .nfs Files

The .nfs files need to be cleared. You can run the **rm -f** command to delete them. The file system will not be affected by the deletion. If an error is reported when you delete an .nfs file, do as follows:

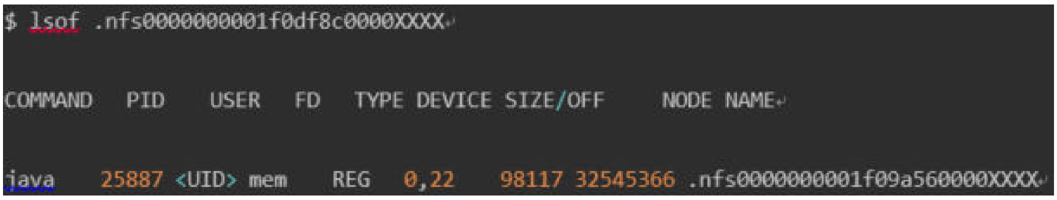
Figure 6-1 Deletion error



```
         $ rm -f .nfs0000000001f0df8c0000XXXX

rm: cannot remove `smkit/SM_DOMAIN/.nfs0000000001f0df8c0000XXXX': Device or resource
 busy
```

Run the **lsof** command to obtain the ID of the process that has the file open.

Figure 6-2 Viewing the process ID



```
$ lsof .nfs0000000001f0df8c0000XXXX

COMMAND   PID    USER   FD   TYPE DEVICE SIZE/OFF     NODE NAME

java    25887 <UID> mem    REG   0,22    98117 32545366 .nfs0000000001f09a560000XXXX
```

If the process can be stopped, run the **kill -9** *Process ID* command to stop the process and then delete the file.

6.5.7 How Can I Improve the Copy and Delete Efficiency with an SFS Turbo File System?

Common Linux commands, such as **cp**, **rm**, and **tar**, are executed sequentially. To take the concurrency advantage of cloud file systems, run commands concurrently to improve efficiency.

6.5.8 How Do Second- and Third-level Directory Permissions of an SFS Turbo File System Be Inherited?

Subdirectories in SFS Turbo file systems cannot inherit permissions of their parent directories.

7 Other Operations

7.1 Mounting a File System to a Linux ECS as a Non-root User

Scenarios

By default, a Linux ECS allows only the **root** user to use the **mount** command to mount file systems, but you can grant the permissions of user **root** to other users. Then, such users can use the **mount** command to mount the file systems. The following describes how to mount a file system to a Linux ECS as a common user. EulerOS is used in this example.

Prerequisites

- A non-**root** user has been created on the ECS.
- A file system has been created and can be mounted to the ECS as **root**.
- The mount point of the file system has been obtained.

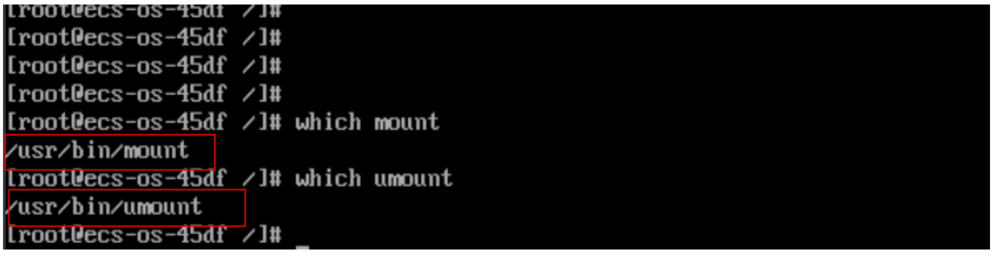
Procedure

Step 1 Log in to the ECS as user **root**.

Step 2 Assign the permissions of user **root** to the non-**root** user.

1. Run the **chmod 777 /etc/sudoers** command to change the **sudoers** file to be editable.
2. Use the **which** command to view the **mount** and **umount** command paths.

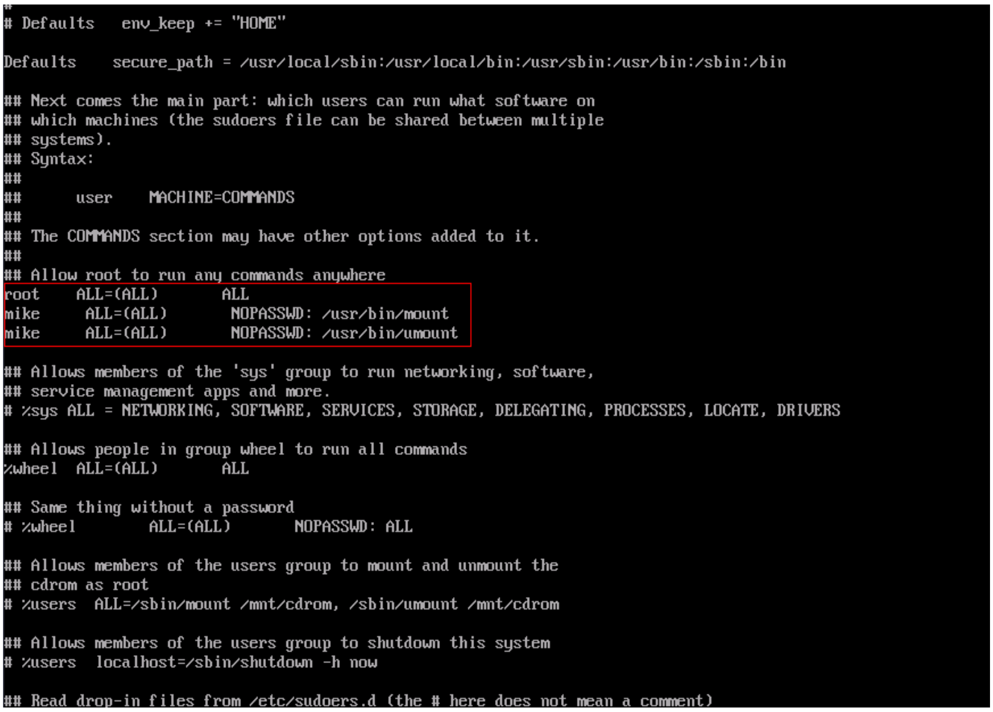
Figure 7-1 Viewing command paths



```
[root@ecs-os-45df /]#
[root@ecs-os-45df /]#
[root@ecs-os-45df /]#
[root@ecs-os-45df /]#
[root@ecs-os-45df /]# which mount
/usr/bin/mount
[root@ecs-os-45df /]# which umount
/usr/bin/umount
[root@ecs-os-45df /]# _
```

3. Run the **vi /etc/sudoers** command to edit the **sudoers** file.
4. Add a common user under the **root** account. In this example, user **Mike** is added.

Figure 7-2 Adding a user



```
#
# Defaults   env_keep += "HOME"

Defaults    secure_path = /usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin

## Next comes the main part: which users can run what software on
## which machines (the sudoers file can be shared between multiple
## systems).
## Syntax:
##
##      user    MACHINE=COMMANDS
##
## The COMMANDS section may have other options added to it.
##
## Allow root to run any commands anywhere
root    ALL=(ALL)       ALL
mike     ALL=(ALL)       NOPASSWD: /usr/bin/mount
mike     ALL=(ALL)       NOPASSWD: /usr/bin/umount

## Allows members of the 'sys' group to run networking, software,
## service management apps and more.
# %sys ALL = NETWORKING, SOFTWARE, SERVICES, STORAGE, DELEGATING, PROCESSES, LOCATE, DRIVERS

## Allows people in group wheel to run all commands
%wheel  ALL=(ALL)       ALL

## Same thing without a password
# %wheel        ALL=(ALL)       NOPASSWD: ALL

## Allows members of the users group to mount and unmount the
## cdrom as root
# %users  ALL=/sbin/mount /mnt/cdrom, /sbin/umount /mnt/cdrom

## Allows members of the users group to shutdown this system
# %users  localhost=/sbin/shutdown -h now

## Read drop-in files from /etc/sudoers.d (the # here does not mean a comment)
```

5. Press **Esc**, input **:wq**, and press **Enter** to save and exit.
6. Run the **chmod 440 /etc/sudoers** command to change the **sudoers** file to be read-only.

Step 3 Log in to the ECS as user **Mike**.

Step 4 Run the following command to mount the file system. For details about the mounting parameters, see **Table 7-1**.

sudo mount -t nfs -o vers=3,timeo=600,noresvport,nolock *Mount point Local path*

Table 7-1 Parameter description

Parameter	Description
Mount Point	**NOTE** *x* is a digit or letter. If the mount point is too long to display completely, you can adjust the column width.
Local path	A local directory on the ECS used to mount the file system, for example, **/local_path**.

Step 5 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.

```
example.com:/share-xxx on /local_path type nfs (rw,vers=3,timeo=600,nolock,addr=)
```

----End

A Change History

Released On	Description
2025-06-27	This issue is the third official release, which incorporates the following change: Added section "Encrypted Transmission."
2023-03-07	This issue is the second official release, which incorporates the following change: Added section "Encryption" and several troubleshooting cases and FAQs.
2020-11-06	This issue is the first official release.