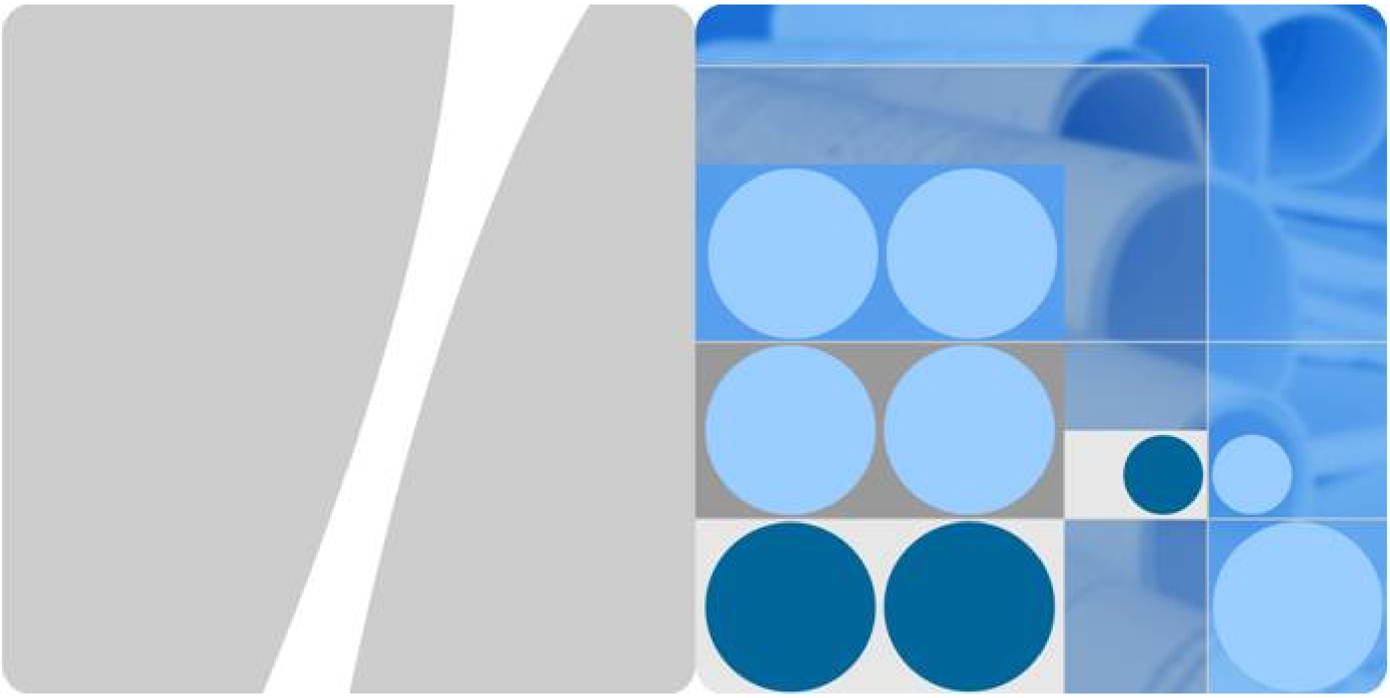


OceanStor V3 Series

V300R006

Basic Storage Service Configuration Guide for File

Issue	**05**
Date	**2018-01-30**

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.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: http://e.huawei.com

About This Document

Purpose

This document describes the basic storage services and explains how to configure and manage basic storage services.

The following table lists the product models applicable to this document.

Product Series	Product Model
OceanStor 2000 V3 series	OceanStor 2200 V3 (16 GB memory) and 2600 V3
OceanStor 5000 V3 series	OceanStor 5300 V3, 5500 V3, 5600 V3, and 5800 V3
OceanStor 6000 V3 series	OceanStor 6800 V3
OceanStor 18000 V3 series	OceanStor 18500 V3 and 18800 V3

Intended Audience

This document is intended for:

- Technical support engineers
- Maintenance engineers

Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
⚠ DANGER	Indicates an imminently hazardous situation which, if not avoided, will result in death or serious injury.

Symbol	Description
⚠ WARNING	Indicates a potentially hazardous situation which, if not avoided, could result in death or serious injury.
⚠ CAUTION	Indicates a potentially hazardous situation which, if not avoided, may result in minor or moderate injury.
⚠ NOTICE	Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance deterioration, or unanticipated results. NOTICE is used to address practices not related to personal injury.
🕮 NOTE	Calls attention to important information, best practices and tips. NOTE is used to address information not related to personal injury, equipment damage, and environment deterioration.

Change History

Changes between document issues are cumulative. The latest document issue contains all the changes made in earlier issues.

Issue 05 (2018-01-30)

This issue is the fifth official release. The updates are as follows:

Optimized descriptions about the chapter **Configuration Process**.

Issue 04 (2017-11-30)

This issue is the fourth official release. The updates are as follows:

- Optimized descriptions about some operation steps.
- Added information about global name space (GNS).
- Added information about CIFS Homedir share.

Issue 03 (2017-08-30)

This issue is the third official release. The updates are as follows:

- Optimized descriptions about some operation steps.
- Added descriptions in **Configuring a Storage System to Add It to an AD Domain**.

Issue 02 (2017-06-01)

This issue is the second official release. The updates are as follows:

- Added description about **Obtaining and Configuring Manila Driver**.
- Optimized descriptions about some operation steps.
- Synchronizes some software interface changes.

Issue 01 (2017-02-28)

This is the first official release.

Contents

1 Basic Storage Service Description

About This Chapter

You can configure basic storage services of a file system to enable application servers to access shared file-level data.

1.1 Introduction

This section focuses on the main features of storage systems, file access protocols and authentication specifications for file access.

The storage systems use the block virtualization technology to manage disks, which helps automatically and properly allocate storage resources and provide available storage space for application servers. Block virtualization is a new redundant array of independent disks (RAID) technology that divides disks into block-level chunks and organizes the chunks into multiple RAID groups. When a hard disk fails, source disks of storage pools in the storage system participate in the reconstruction. This smashes the performance bottleneck in the reconstruction of traditional RAID groups and greatly improves the data reconstruction speed. You can create file systems on the storage system and share files, enabling application servers to simply and conveniently access shared files.

The storage system supports:

- Multi-protocol access

  The storage system allows application servers to access shared files using different protocols, such as Common Internet File System (CIFS), Network File System (NFS), FTP (File Transfer Protocol) and (Hypertext transfer protocol).

- Quota configuration

  The user can restrict the storage space size and file quantity under shared directories for optimal storage space allocation and utilization.

- Permission control

  The file system can control access and read and write permissions of all share users for easy user management and maintenance, ensuring data security and reliability.

The storage system supports two file access protocol management modes: graphical user interface (GUI) and command-line interface (CLI). This document explains how to manage file access protocols using GUI. For details about how to manage file access protocols using CLI, see the *Command Reference* of the corresponding product model.

File Access Protocol Introduction

- NFS

  NFS is a protocol developed by Sun. Internet Engineering Task Force (IETF) is in charge of developing its new versions. This protocol is designed for file sharing among Linux, UNIX, Mac OS, and VMware operating systems.

- CIFS

  CIFS is a file system share protocol developed by Microsoft and primarily used in Windows environments.

- FTP

  File Transfer Protocol (FTP) is a universal protocol for transferring files between two computers over a TCP/IP network and primarily used in Internet.

- HTTP

  Hypertext Transfer Protocol (HTTP) is a protocol for transferring hypertext from web servers to local clients and primarily used in Internet.

Protocol Comparison

Table 1-1 compares the protocols.

Table 1-1 Protocol comparison

Type	Application Scenario	Transmission Protocol	Working Principle
NFS	Linux and UNIX environments, including the non-domain environment, Lightweight Directory Access Protocol (LDAP)[a] domain environment, and network information service (NIS)[b] domain environment.	Transmission Control Protocol (TCP) or User Datagram Protocol (UDP)	Client/Server architecture, requiring client software
CIFS	● Windows environments, including the non-domain environment and active directory (AD)[c] domain environment. ● Linux environment in which the SMB client is installed.	TCP	Client/Server architecture, with client software being integrated into operating systems
FTP	No restrictions on operating systems.	TCP	Client/Server architecture, with client software being integrated into operating systems
HTTP	No restrictions on operating systems.	TCP	Browser/Server architecture

a: LDAP is a domain environment in Linux and used to construct a user authentication system based on directories.

b: NIS is a domain environment in Linux and can centrally manage the directory service of system databases.

c: AD is a domain environment in Windows and can centrally manage computers, servers, and users.

Authentication Specifications for File Access

Table 1-2 describes the authentication specifications supported by the storage system.

Table 1-2 Authentication specifications

Authentication Mode	Kerberos[a]	NTLM[b]	User/User Group Management	Network Group
Local authentication	×[c]	√[c]	√	×
AD domain server authentication	● Access using **node name. AD domain name**: √ ● Access using another method: ×	√	×	×
LDAP domain server authentication	×	×	×	√
NIS domain server authentication	×	×	×	√

a: Kerberos is a computer network authentication protocol. This protocol is used to authenticate user identity in an open network environment and automate user authentication every time a user who has logged in accesses resources on networks. By default, the Kerberos authentication is used in Microsoft Windows 2000 and later.

b: NT LAN Manager (NTLM) is a security protocol proposed in Microsoft Windows NT. This protocol is used to protect user names and passwords during authentication.

c: √ Supported × Not supported or N/A.

NOTE

- Storage system can be added into an AD domain, LDAP domain, or NIS domain. However, each domain can have only one such storage system.
- NFS shares support LDAP/NIS domain authentication but do not support Kerberos authentication.
- For FTP shares and HTTP shares, the storage system employs **User/User Group Management** for local authentication.

About This Document

This document describes basic storage service (file services) configurations in non-tenant scenarios. For details about basic storage service (file services) configurations in tenant scenarios, see *OceanStor V3 Series V300R006 SmartMulti-Tenant Feature Guide for File*.

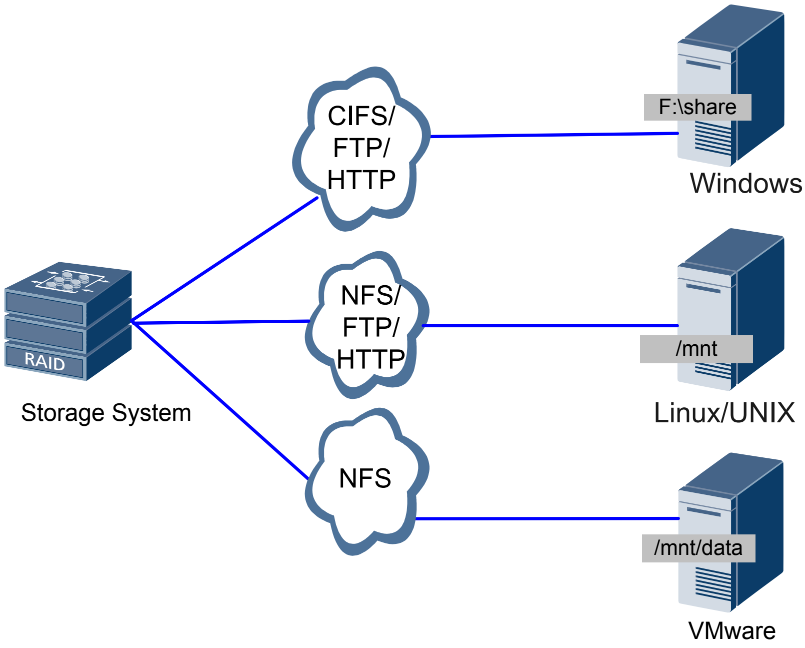
1.2 Application Scenarios

This section describes scenarios where application servers access a storage system.

Storage system enables application servers to access shared files using NFS, CIFS, FTP, or HTTP. Application servers can run different operating systems, including Windows, Linux, UNIX (Solaris, AIX, and HP-UX), and VMware.

Figure 1-1 shows a scenario where application servers access a storage system.

Figure 1-1 Scenario where application servers access a storage system



1.3 Basic Storage Principles

Storage systems provide storage space for application servers. This section mainly introduces the basic concepts, working principle and file system data writing process related to the storage system.

1.3.1 Basic Concepts

Get yourself started with the following basic concepts.

- **Disk domain**: consisting of the same type or different types of disks. Disk domains are isolated from each other. Therefore, services carried by different disk domains do not affect each other in terms of performance and faults.
- **Storage pool**: container of storage resources, which is created under a disk domain. The storage resources used by application servers are all from storage pools. Based on the storage media, a storage pool can have three storage tiers, including the high performance tier, performance tier, and capacity tier.
- **Storage tier**: a set of storage media providing the same performance in a storage pool. Storage tiers are used to manage storage media with different performance and provide appropriate storage space for applications having different performance requirements.
- **CHUNK**: CK for short, consecutive physical spaces of a fixed size on a disk.

- **CHUNK Group**: CKG for short, a logical set of CHUNKs on different disks. A CHUNK Group has the properties of a RAID group.
- **Block virtualization**: a new type of redundant array of independent disks (RAID) technology. Block virtualization divides disks into multiple CHUNKs of a fixed size and organizes them into multiple CHUNK groups. When a disk fails, all the disks on which the other CHUNKs in the same CHUNK group as the CHUNKs on the failed disk are located participate in the reconstruction. This significantly increases the disks involved in the reconstruction, eliminating the performance bottleneck in the reconstruction of traditional RAID groups and improving the data reconstruction speed. In addition, block virtualization distributes data to all the disks in a storage system and leverage the I/O processing capability of the storage system.
- **Extent**: An extent is a logical storage space with a fixed size divided from a CKG. The size ranges from 512 KB to 64 MB. The default size is 4 MB. Extent is the smallest unit (granularity) for data migration and hotspot data statistics collection. It is also the smallest unit for space application and release in a storage pool.
- **Grain**: In file system mode, extents are further divided into grains. The default size of a grain is 64 KB. Grains are basic units that constitute a file system.
- **Hot spare space**: the space used for faulty block data reconstruction in block virtualization. When a CHUNK is faulty, the system lets a CHUNK of the hot spare space take over and instructs the other CHUNKs in the CHUNK group to perform data reconstruction using the hot spare space. This ensures data integrity and read/write performance.
- **Reconstruction**: Reconstruction is the process of restoring the data saved on a faulty disk to hot spare chunks and replacing the chunks on the faulty disk with the hot spare chunks. During data reconstruction, valid data and parity data must be read and processed to restore the data saved on a faulty disk to hot spare space, thereby ensuring data security and reliability. Traditional reconstruction technologies enable only all disks in the same RAID group as the faulty disk to participate in reconstruction. RAID 2.0+ technology enables all disks in the same disk domain as the faulty disk to participate in reconstruction, boosting data reconstruction speed and shortening data recovery duration.

⚠ **NOTICE**

Data on other disks is read for reconstruction. To prevent reconstruction failures, service interruption, and data loss, do not remove other disks in the disk domain where the faulty disk resides.

- **Quota**: An administrator can set the number of files and space size for different directories. The quota management feature developed by Huawei is called SmartQuota.
- **Quota tree**: A quota tree is the root directory of a file system. File quantity or storage space under a quota tree can be managed.
- **Thin file system**: A thin file system is logical space accessible to a host, which is configured with an initial capacity when being created and dynamically allocated required storage resources when its available capacity is insufficient.
- **Thick file system**: A thick file system is logical space accessible to a host, which is allocated a fixed capacity of storage resources according to the capacity specified when being created using the thin provisioning technology.

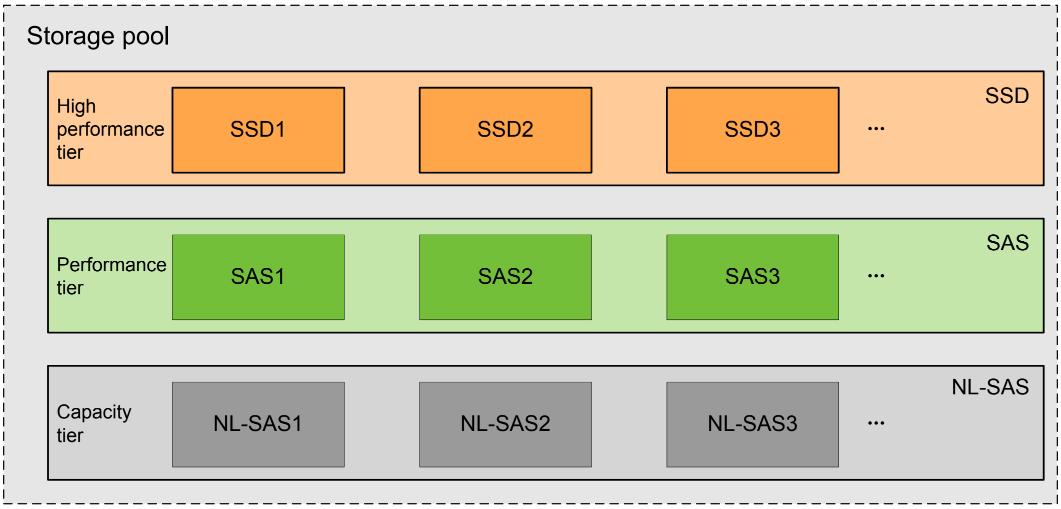
1.3.2 Operating Principles in a Storage System

Storage systems provide storage space for application servers. The storage systems use the block virtualization technology to support dynamic allocation and expansion of storage resources in storage pools. This shortens the response time for data reads/writes in the storage pools and the reconstruction time after a disk fails.

Storage Pool Structure

Figure 1-2 shows the structure of a storage pool.

Figure 1-2 Structure of a storage pool



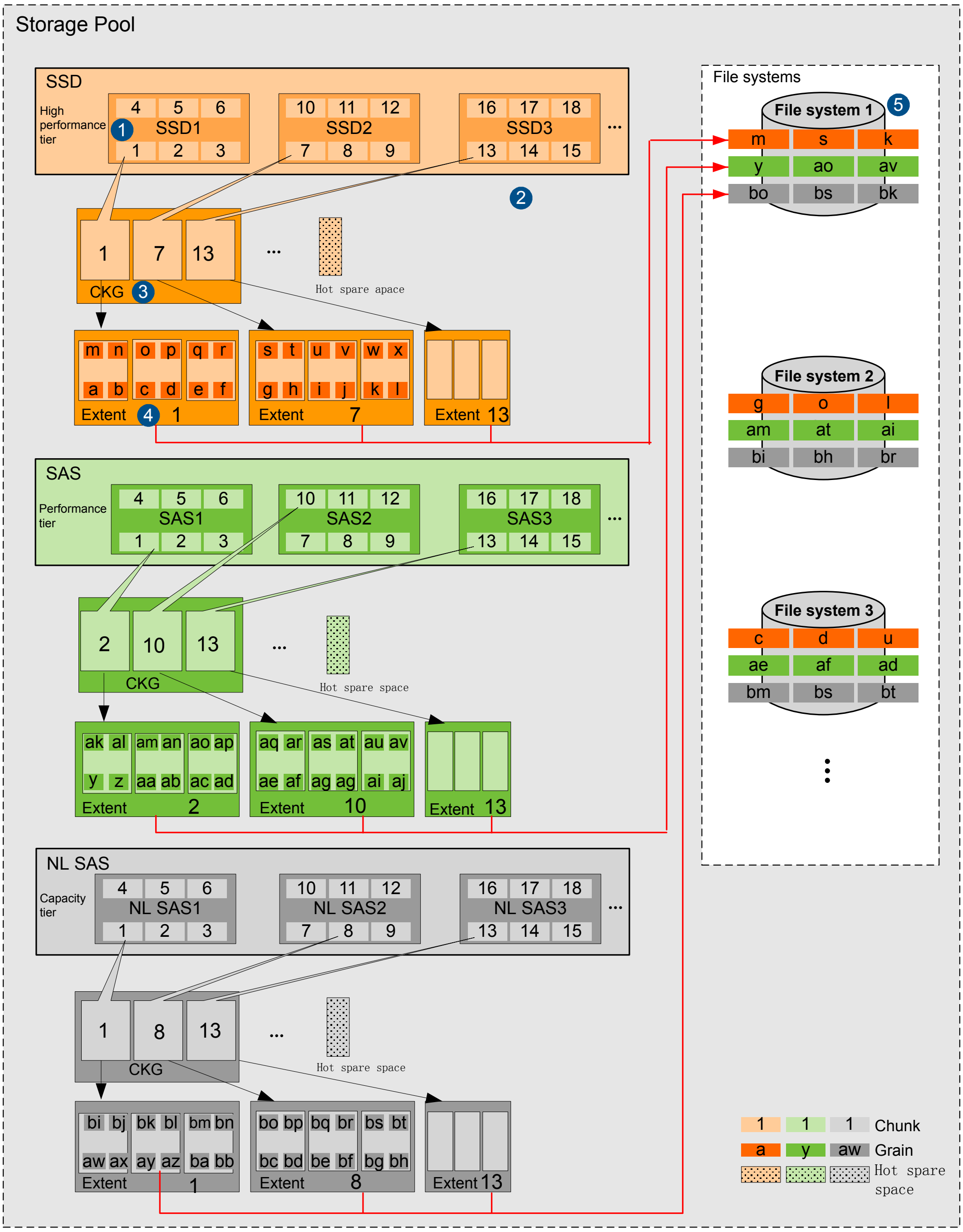
A storage pool consists of three storage tiers at most. Each storage tier is constructed by the same type of storage media.

- High performance tier is composed of solid-state drives (SSDs). High performance tier provides the highest performance at a high cost. It is used to store frequently accessed data.
- Performance tier is composed of serial attached SCSI (SAS) disks. Performance tier provides high performance at a moderate cost. It is used to store less frequently accessed data.
- Capacity tier is composed of Near Line SAS (NL-SAS) disks. Capacity tier provides moderate performance and a large capacity per disk at a low cost. It is used to store a large amount of data and seldom-accessed data.

Block Virtualization Process

Figure 1-3 shows the block virtualization process.

Figure 1-3 Block virtualization process



1. The storage system divides the storage media in disk domains into CHUNKs. Each CHUNK has a fixed size, which cannot be changed.

2. CHUNKs in each storage tier are configured into CHUNK groups and hot spare CHUNKs based on the **RAID policy** and **Hot spare policy** specified on the DeviceManager. You can set **RAID policy** and **Hot spare policy** for each storage tier.

   – **RAID policy** specifies the RAID level and the number of data blocks and parity blocks in a RAID group.

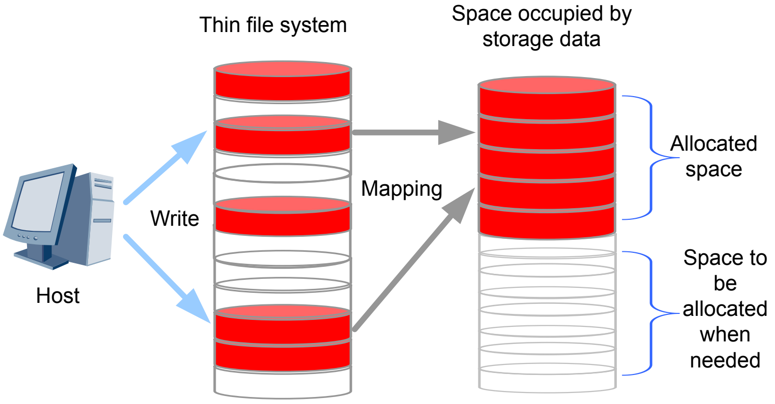
- Possible values of **Hot spare policy** are **High**, **Low** and **None**. Based on the specified value, the storage system sets the corresponding number of CHUNKs to be the hot spare space.

3. The storage system divides CKGs into extents based on the data migration granularity configured on the DeviceManager. The extent is the smallest unit of a file system. The extents may vary according to storage pools but must be the same in one storage pool. The file systems used by application servers are composed of extents. Space application, space release, and data relocation of file systems are based on extents.
4. Extents are further divided into grains. The default size of a grain is 64 KB.
5. The file systems used by application servers are composed of grains. When creating a file system, you can specify that the capacity of the file system comes from a storage tier. In this case, the file system is composed of the Grains in the storage tier. otherwise, data on the file system is distributed by Grains to the storage tiers in the storage pool.

Working Principle of SmartThin

Understanding the working principle of SmartThin can help you fully utilize storage system space. SmartThin provides a storage management mode that supports on-demand allocation. **Figure 1-4** shows storage space occupation when SmartThin is used.

Figure 1-4 Storage space occupation when SmartThin is used


Thin file system
Space occupied by storage data
Host
Write
Mapping
Allocated space
Space to be allocated when needed

SmartThin applies to the following scenarios:

- Core system services that have high requirements for service continuity use SmartThin for online expansion, ensuring ongoing services. For example, SmartThin applies to financial systems.
- For services whose data growth is hard to predict, use SmartThin to allocate physical storage space based on requirements, avoiding wasting storage space. For example, SmartThin applies to email and web disk services.
- Mixed services that have diverse storage requirements use SmartThin to contend for physical storage space and achieve optimal configuration of physical storage space. For example, SmartThin applies to carriers' services.

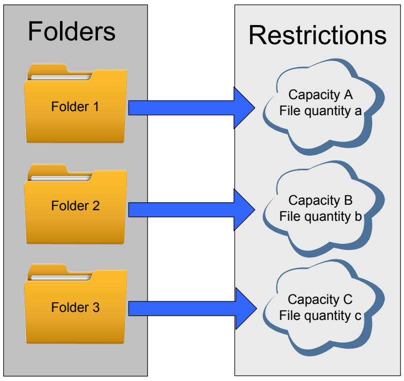
1.3.3 Working Principle of Quota

This section describes the working principle of quotas.

Quota Configuration

You can configure different space sizes and quantities for different directories for efficient storage resource utilization. **Figure 1-5** shows how to configure a quota.

Figure 1-5 Configuring quota



Working Principle of SmartQuota: A storage system employs hard quotas (including hard quotas of capacity and files) to restrict the maximum number of resources available to each user. The process is as follows: In each write I/O operation, check whether the accumulated quota (Quotas of the used capacity and file quantity + Quotas of the increased capacity and file quantity in this operation) exceeds the preset hard quota. If the accumulated quota does not exceed the preset hard quota, the follow-up operations can be performed. Otherwise, the write I/O operation fails. After the write I/O operation is allowed, add the incremental capacity and file quantity to the previously used capacity and file quantity. Then, update the quota (Latest capacity + Latest file quantity) and enable the quota and I/O data to be written into the file system. The I/O operation and quota update succeed or fail at the same time, ensuring that the used capacity is correct in each I/O check.

If a directory quota, user quota, and group quota are concurrently configured in a shared directory in which you are performing operations, each write I/O operation will be restricted by the three quotas. You must check each type of quota. If the hard quota of one type of quota does not pass the check, the I/O will be rejected.

1.3.4 Working Principle of Global Name Space (Applicable to V300R006C10 and Later Versions)

This section introduces working principle of global name space.

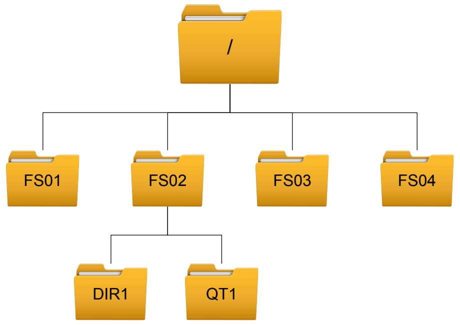
Challenges of File Management

With rapid development of enterprise services, file access and management are becoming more complicated. File virtualization technology based on global name space (GNS) is used to solve problems encountered by file management.

What Is GNS?

GNS converges file systems scattered on different storage systems to a virtual root directory /, providing a unified logical view and simplifying file access and management. **Figure 1-6** shows the logical structure of GNS. On the top of the structure is a virtual root directory /.

Figure 1-6 Logical structure of GNS



What Are the Benefits of GNS?

GNS is core of the file virtualization technology. With Domain Name System (DNS), you can visit Web sites without memorizing IP addresses. Similarly, GNS enables clients to directly access files without knowing locations of scattered files. GNS adopts a unified logical interface for file management. Users can create their own file folders or access authorized file folders.

GNS provides a platform to carry critical storage management solutions, covering file sharing, disaster recovery, data migration, load balance, server integration, and storage optimization.

NFS GNS Management

- The share path of GNS is root directory / by default.
- Each vStore can only create one GNS and the share name must be /.
- You must add an independent share for the file system. After the share is added, this file system will not be displayed if a host is only authorized to access / but not the file system.
- GNS root directory / only has read permissions. You cannot create, modify, delete directories or files under /, or modify directory attributes of /. Permission will change to the share permission of a file system once the directory of the file system is entered.
- If GNS is not created, root directory / cannot be mounted to NFSv3. Only shared file systems can be viewed when NFSv4 is mounted with root directory /.
- If GNS is created in the primary vStore of HyperMetro, you can only create a vStore pair when the secondary storage has the same version as that of the primary storage. If a vStore pair is created, you can create a GNS share only when the version of the primary and secondary storage systems is the same and is V3R6C01 or later.

For details about creating NFS GNS, see **3.9.1.9 Creating an NFS Share**. For details about accessing NFS GNS, see **3.9.1.11 Accessing NFS Share**.

CIFS GNS Management

- The share path of GNS is root directory / by default.

- You can create multiple GNS shares with different share names for each vStore.
- After GNS CIFS shares are created, all file systems are mounted to the root directory / by default. By enabling the access based enumeration (ABE) function, you can allow users to or not to visit unauthorized files and file folders. By setting ACL permissions on the file system, you can control user access to a specific file system.
- GNS root directory / only has read permissions. You cannot create, modify, delete directories or files under /, or modify directory attributes of /. Files or directories cannot be moved across level-1 directories (file systems).
- Directory names of the CIFS protocol are case insensitive. If file systems have duplicate names with different capitalization, for example file systems AA and aa, only the file system created earlier or with a smaller file system ID is added to GNS. Change the names of the files with duplicate names and ensure that the names are unique. After the modification is successful, the file system is automatically added to GNS.
- SMB1 does not support GNS.
- If GNS is created in the primary vStore of HyperMetro, you can only create a vStore pair when the secondary storage has the same version as that of the primary storage. If a vStore pair is created, you can create a GNS share only when the version of the primary and secondary storage systems is the same and is V3R6C01 or later.
- When the internal network of the LAN is stable, you can run the **change service cifs global_namespace_forward_enabled=yes** command to enable the GNS forwarding function so that the performance can be improved when the non-owning controller of the file system is accessed. For details, see the *Command Reference* of the corresponding product model. When the internal network of the LAN is unstable (for example, node fault, upgrade, or IP address failover), you are not advised to enable the GNS forwarding function, which may interrupt services.
  - After the GNS forwarding function is enabled or disabled, the client needs to remount the share for the client to take effect. In addition, the client may fail to access certain directories. In this case, the client needs to stop services and wait until the client cache times out, and then mount the share. You can also use the dfsutil.exe tool (provided by Microsoft) to clear the client cache and then mount the share.
  - To use the GNS forwarding function, you need to configure an IP address that can be accessed by the client for the logical port and enable the IP address failover.
  - If the GNS forwarding function is enabled, the DNS-based load balancing function is affected. To enable the function, you are advised to disable the DNS-based load balancing function.
- **c$** is the default GNS share whose Share Path is the root directory / and Permission is Full control by Administrators.
  - Share **c$** cannot be deleted but its properties and permission can be modified.
  - After a new vStore is created, a **c$** share is automatically created for this vStore.
  - After the **c$** share is created, you can choose a file system as the share path when creating shares on MMC and do not need to manually enter the share path.

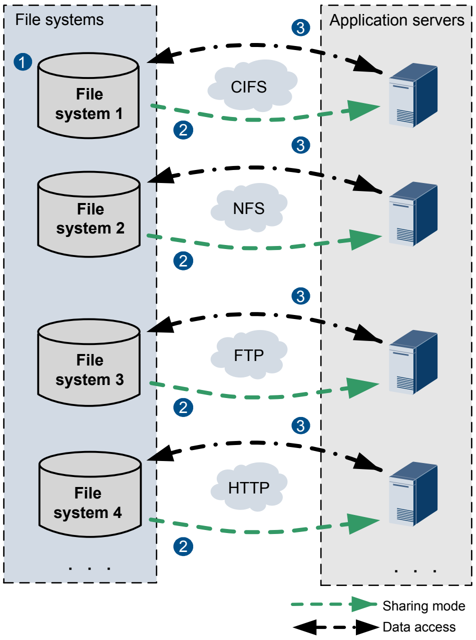
For details about creating CIFS GNS, see **3.9.2.9 Creating a CIFS share**. For details about accessing CIFS GNS, see **3.9.2.10 Accessing CIFS Shares**.

1.3.5 Procedure of an Application Server Accessing a File System

This section describes how an application server accesses file system.

Figure 1-7 shows how an application server accesses a file system.

Figure 1-7 Procedure of an application server accessing a file system



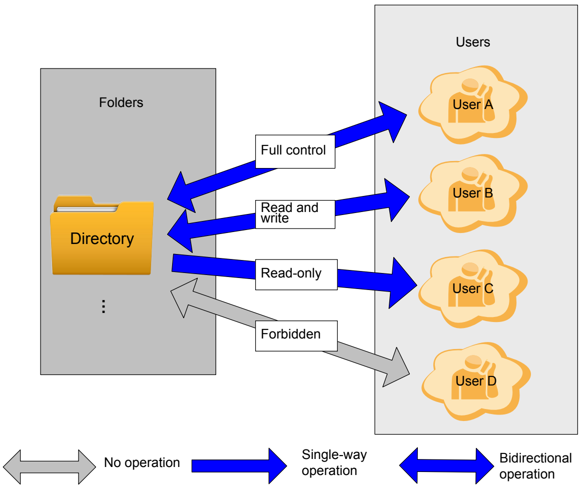
1. Create a file system. The storage system creates a file system based on the entered name, capacity, and quantity, and selects a storage pool for it. After the thin provisioning function of the file system is enabled, the storage system allocates storage space for the file system on demand based on site capacities used by hosts.
2. Share a file system. After creating a file system, you must create a share and then share the file system, so that application servers can access the file system. File systems can be shared in multiple modes. Specify the names of the file system and the quota tree to be shared. A shared directory consists of a file system name and quota tree name. When sharing the file system, you can configure a quota value for the quota tree and set the storage space and file quantity of the quota tree for optimal storage resource utilization. You can also set shared access permissions (including full control, read and write, read-only, and forbidden) for users or user groups to achieve easy user management and data maintenance.
3. Use an application server to access a shared file system. Use an application server to directly access a shared file system. You can perform related operations based on your share permission.

1.3.6 User Permission Control

This section mainly introduces the principle of user permission control.

You can assign different user permissions for the same directory, so that the users can only access the directory within their specified permissions. **Figure 1-8** shows user permission control.

Figure 1-8 User permission control



Users with the full control permission can not only read and write directories but also have permissions to modify directories and obtain all permissions of directories. Users with the forbidden permission can view shared directories but cannot perform operations in any directory.

1.3.7 File System Data Writing Process

This section mainly introduces the data writes process of the file system.

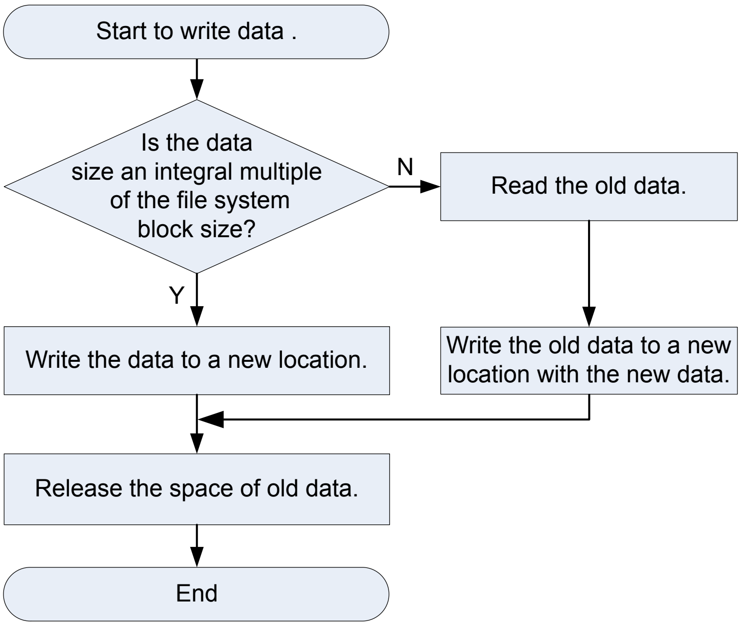
Space Occupation upon Data Writes

Users use the redirect-on-write (ROW) technology to write data into files in the following two scenarios:

- If the size of the data to be written is an integral multiple of the file system block size, the data will be written to a new location and the space of old data will be released (if the old data contains the created snapshots, the space of old data will not be released).
- If the size of the data to be written is not an integral multiple of the file system block size, the old data will be read and then written to a new location with the new data, and the space of old data will be released (if the old data contains the created snapshots, the space of old data will not be released).

The ROW technology is used to save data to a new location, enabling quick data writes. **Figure 1-9** shows how to modify data.

Figure 1-9 Data writes process


Start to write data .
Is the data size an integral multiple of the file system block size?
N
Read the old data.
Y
Write the data to a new location.
Write the old data to a new location with the new data.
Release the space of old data.
End

1.3.8 Write Mode Shifts from Write Back to Write Through

This section mainly introduces scenarios where the write mode of file system shifts from write back to write through and recommended actions.

Write mode shifts from write back to write through

Generally, the write mode of file system in a storage system is write back by default. However, the write mode will become write through in the event of a fault.

Table 1-3 Scenarios where the write mode of file system shifts from write back to write through and recommended actions

Symptom	Scenario	Impact and Recommended Action
The temperature of a controller exceeds the upper limit.	● If the **Controller Enclosure Temperature Exceeds The Upper Limit** alarm is generated due to an exception on equipment room temperate or the internal components of a storage system, file systems continue the write back mode within a specified period of time (192 hours). If the alarm persists after the specified period of time, file systems change the write mode to write through. ● If the **Controller Enclosure Temperature Exceeds The Upper Limit** alarm is generated due to a fault on the single controller of a controller enclosure, file systems continue the write back mode within a specified period of time (1 hour). If the alarm persists after the specified period of time, file systems change the write mode to write through. NOTE If the **Controller Enclosure Temperature Is Far Beyond The Upper Limit** alarm is generated in a storage system, the storage system will automatically powers off.	Impact The write mode of service objects on the entire engine becomes write through. Recommended action Check the external refrigerating system, fan modules, and air channels to locate the overtemperature causes and rectify faults.

Symptom	Scenario	Impact and Recommended Action
BBUs on an engine malfunction.	● Dual-controller storage device: If two BBUs malfunction and an alarm is generated, the write mode of file system shifts from write back to write through. ● Four-controller storage device: If two or more BBUs malfunction and an alarm is generated, the write mode of file system shifts from write back to write through.	Impact The write mode of service objects on the entire engine becomes write through. Recommended action ● Check whether BBUs are properly inserted. ● Check whether the BBUs break down. If the BBUs break down, replace them with the spare parts. ● Check whether the power of the BBUs is insufficient. If the power of the BBUs is insufficient, wait until the BBUs are fully charged.
The coffer disks of an engine malfunction.	● Dual-controller storage device: If both coffer disks break down, the write mode of file system shifts from write back to write through. ● Four-controller storage device: If all coffer disks of controllers A and B or controllers C and D break down (the controllers in the first row are controllers A and B and the controllers in the second row are controllers C and D), the write mode of file system shifts from write back to write through.	Impact The write mode of service objects on the entire engine becomes write through. Recommended action Check whether the coffer disks are faulty. If the coffer disks are faulty, replace them with spare parts.

Symptom	Scenario	Impact and Recommended Action
A controller malfunctions.	By default, the write mode of file system remains write back within a certain period (192 hours) in which a single controller malfunctions. If the fault is not rectified within this period, the write mode of file system shifts from write back to write through.	Impact The write mode of service objects on the entire engine becomes write through if the fault persists after 192 hours. Recommended action ● Replace the faulty controller at the off-peak point in time during the write back protection period. ● If the spare part is unavailable during the delay protection period of write through, add a proper period to the delay after assessing risks to prevent write through from adversely affecting service performance.
The remaining capacity of a storage pool is smaller than the reserved capacity.	An alarm is generated indicating that the capacity usage of a storage pool exceeds the threshold and reminding you of expanding the capacity.	Impact The write mode of thin file system and thick file system with value-added features shifts from write back to write through. Recommended action Expand the capacity of the storage pool.

Symptom	Scenario	Impact and Recommended Action
The remaining capacity of a file system is smaller than the threshold.	If the remaining capacity of a file system is smaller than the threshold, a device alarm will be generated. If the remaining space is about to be exhausted, the file system's write mode shifts to write through by default, but you can run the following command in developer mode to change write through to space exhaustion protection: **change file_system optimization file_system_id=? name=space_exhaust_protect enabled=yes**. For details, see the *Advanced O&M Command Reference* of the corresponding product model. **NOTE** When the following case occurs, the data write mode of file system shifts to write through due to insufficient file system capacity, however, it may not generate the alarm of the remaining capacity of file system is smaller than the threshold: **The used capacity of file system + the capacity that the grain occupies + the capacity of dirty data in cache > the total capacity of file system** the capacity that the grain occupies including space debris, space prefetch, delayed release space.	Impact The write mode of the file system that occurs alarm shifts from write back to write through, and the performance of the file system deteriorates. Recommended action Expand the capacity of the file system.

1.3.9 NFS Feature

This section describes the concept, availability, restrictions, and application scenarios of the NFS feature.

1.3.9.1 Overview

NFS is a protocol developed by Sun. Internet Engineering Task Force (IETF) is in charge of developing its new versions. This protocol is designed for file sharing among Linux and UNIX operating systems.

NFS works based on client/server architecture. The server provides other computers with file system access, whereas the client accesses the shared file system. The NFS feature enables clients running a variety of operating systems to share files over a network.

Storage system supports the NFS protocol, enabling users to flexibly and easily use clients and configure desired environments. When being configured as an NFS server, the storage system provides shared file system access for clients that use NFS v3 and NFS v4. NFS allows users to centrally store data in the storage system. With NFS, users can access remote file systems in the same way as accessing local files over a network, reducing local disk space required.

NFS highlights:

- High concurrency

  Multiple clients can use the same file so that all the users can access the same data.

- Data integrity

  All users can read the same group of files.

- Ease-of-use

  File system mounting and remote file system access are transparent to users.

NFS Lock Policy

The file lock policy is a file read and write mechanism, and is used to ensure data consistency. When clients of different protocols operate on the same file or directory, file locks ensure that the data does not conflict. The NFS mechanism includes advisory and mandatory locks. By default, mandatory locks are enabled. You are advised to use advisory locks when the requirements for read and write performance are high and clients of different protocols do not access the same file or directory at the same time. If clients of different protocols simultaneously access the same file or directory, mandatory locks are recommended.

- The file lock policy is a file read and write mechanism, and is used to ensure data consistency. When clients of different protocols operate on the same file or directory, file locks ensure that the data does not conflict.
- Mandatory locks are used for the kernel. When a client accesses a file, the kernel checks whether the file is configured with mandatory locks. If mandatory locks are set, the client cannot perform operations on the file. The kernel confines operations of the client.

NFS lock policies can be set both on the clients and the servers.

- If mandatory NFS lock policies are set on the clients, conflicts are less likely to occur when multiple client processes access the same file. If advisory NFS lock policies are set on the clients, conflicts may occur when clients of different protocols access the same file or directory.
- If mandatory NFS lock policies are set on the servers, conflicts are less likely to occur when multiple client processes access the same file or directory. If advisory NFS lock policies are set on the servers, conflicts may occur when clients of different protocols access the same file or directory.

The NFS client supports advisory locks by default. The SMB client and the server support mandatory locks by default. Since the NFS lock policy can be set on both the clients and servers, the file NFS lock policy depends on the settings of lock policies on the clients and the servers, as shown in **Table 1-4**.

Table 1-4 NFS Lock Policies of Files

NFS lock policy of clients	NFS lock policy of servers	NFS lock policy of files
Mandatory lock	Advisory lock	Mandatory lock
Mandatory lock	Mandatory lock	Mandatory lock
Advisory lock	Mandatory lock	Mandatory lock
Advisory lock	Advisory lock	Advisory lock

1.3.9.2 License Requirements and Compatible Products

This section describes license requirements and compatible products of NFS.

License Requirements

The NFS feature is a value-added feature that requires a license.

Compatible Products

Product Series	Product Model	Product Version
OceanStor 2000 V3 series	OceanStor 2200 V3 (16 GB memory) and 2600 V3	V300R006
OceanStor 5000 V3 series	OceanStor 5300 V3, 5500 V3, 5600 V3, and 5800 V3	V300R006
OceanStor 6000 V3 series	OceanStor 6800 V3	V300R006
OceanStor 18000 V3 series	OceanStor 18500 V3 and 18800 V3	V300R006

1.3.9.3 Restrictions

This section describes the NFS feature in terms of supported protocol versions, network requirements, dependency on other features, and impact on system performance.

Supported Protocol Versions

The storage system supports NFSv3 and NFSv4.

Item	Document
RFC1813	*NFS Version 3 Protocol Specification*
RFC3530	*NFS Version 4 Protocol*

NOTE

- A storage system is added to a NIS domain and an LDAP domain and an NFS share is added to the network groups of the two domains. When the NIS domain fails, mounting the NFS share using clients in the LDAP domain may time out.
- If an NIS domain fails after a storage system is added to the NIS domain and a client in a non-NIS domain fails to mount an NFS share using NFS v4 for the first time, enable the client to mount the NFS share again.

Network Requirements

The NFS feature supports the IPv4 and IPv6 network access protocols.

Interaction with Other Features

Table 1-5 describes the relationship between the NFS feature and other features.

Table 1-5 Relationship between the NFS feature and other features

Feature	Relationship
File system snapshot	Before accessing a file system snapshot, clients must create an NFS share for it.
CIFS/FTP/HTTP	● To prevent file data overwriting or loss and ensure shared data consistency, a file in a file system cannot be written concurrently in multi-protocol sharing mode. Configure read-write sharing based on one protocol and read-only sharing based on the other protocols. NOTICE A file in a file system that written concurrently in multi-protocol sharing mode will cause data loss, exercise caution when using it. ● If NFS and CIFS shares are used together and the same file system is operated, restrictions exist in user convergence, lock convergence, permission convergence, and link convergence. Evaluate the scenario based on actual conditions.

System Impact

File systems can be shared in NFS, CIFS, FTP and HTTP modes at the same time. When clients concurrently access a file system using different protocols, the overall performance slightly decreases.

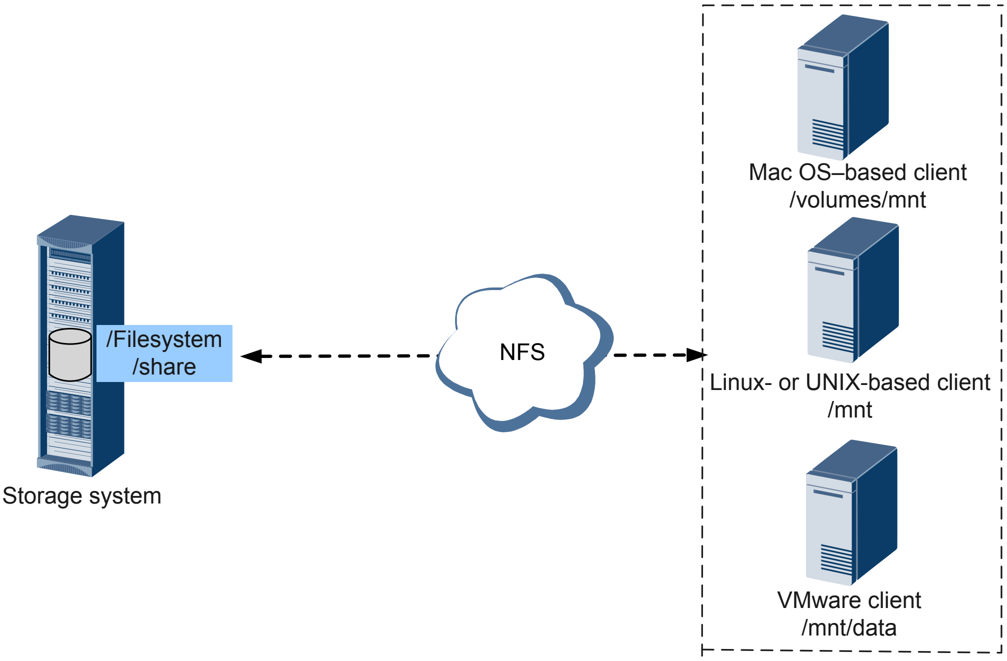
1.3.9.4 Application Scenarios

The NFS feature enables clients running a variety of operating systems to share files over a network. It applies to a wide range of network environments, including the non-domain environment, LDAP domain environment, and NIS domain environment.

NFS Share in a Non-Domain Environment

The NFS share in a non-domain environment is commonly used for small- and medium-sized enterprises. Figure 1-10 shows the networking. On the network, the storage system serves as the NFS server and employs the NFS protocol to provide shared file system access for clients. After the clients map the shared files to the local directories, users can access the files on the server in the same way as accessing local files. IP addresses are configured in the storage system for the clients that are allowed to access the shared file system.

Figure 1-10 NFS share in a non-domain environment



NFS Share in a Domain Environment

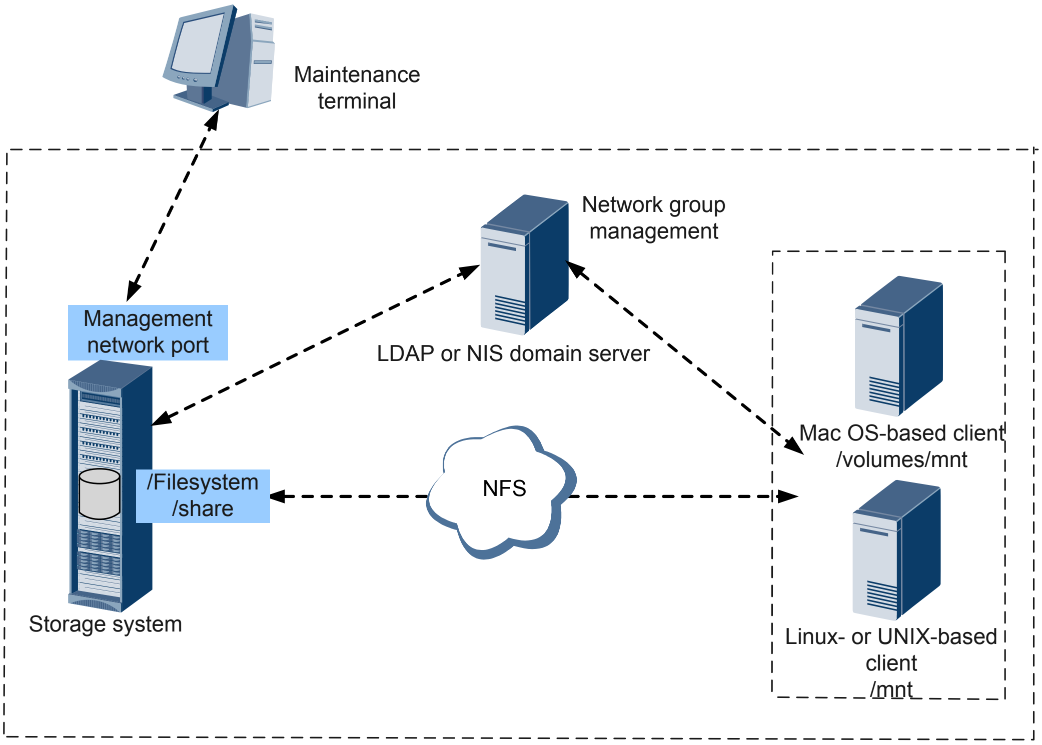
Domains enable accounts, applications, and networks to be centrally managed. In Linux, LDAP and NIS domains are available.

LDAP is an open, extendable network protocol. It is also becoming an important tool for network management with its user-friendly, secure, and powerful information query feature as well as its cross-platform data access capability. The purpose of LDAP-based authentication applications is to set up a directory-oriented user authentication system, specifically, an LDAP domain. When a client user needs to access applications in the LDAP domain environment, the LDAP server compares the user name and password sent by the client with corresponding authentication information in the directory database for identity verification.

NIS is a directory service technology that enables users to centrally manage system databases. It provides a yellow page function to support the centralized management of network information. NIS works based on client/server architecture. When the user name and password of a user are saved in the NIS server database, user can log in to an NIS client and maintain the database to centrally manage the network information on the LAN.

As shown in **Figure 1-11**, when a client needs to access an NFS share provided by the storage system in a domain environment, the storage system employs the domain server network group to authenticate the accessible IP address, ensuring the reliability of file system data.

Figure 1-11 NFS share in a domain environment



NOTE

If LDAP/NIS domain authentication is used, ensure that the first two controllers of the storage system can communicate with the domain controller.

1.3.10 CIFS Feature

This section describes the concept, availability, restrictions, and application scenarios of the CIFS feature.

1.3.10.1 Overview

CIFS is a protocol used for sharing network files. CIFS allows Windows clients on the Internet and intranet to access shared files and other resources. The CIFS share is mainly applicable to the file sharing.

Introduction to CIFS Protocol

Server Message Block (SMB) is a protocol used for network file access and CIFS is a public version of SMB. The SMB protocol allows a local PC to access files and request services on PCs over the local area network (LAN). Storage system supports SMB 1.0, SMB2 (SMB 2.0 and SMB 2.1) and SMB 3.0.

- If the client runs Windows Server 2003, Windows XP, Linux, or MAC OS, SMB 1.0 is used.
- If the client runs Windows Server 2008 or Windows Vista, SMB 2.0 is used.
- If the client runs Windows Server 2008 R2 or Windows 7, SMB 2.1 is used.

- If the client runs Windows Server 2012 or Windows 8, SMB 3.0 is used.

NOTE

- SMB 1.0 file sharing protocol, limited by its own mechanisms, cannot ensure service continuity during online upgrade.
- When the client supports multiple versions of the SMB protocol, it is recommended to select a higher version of the protocol. At this point, the security is higher.

With the continuous expansion of enterprises, more and more users need to access the share service in enterprises. Restricted by the server where shared files reside, the access speed decreases and system response slows down when a large number of users access shared files. Therefore, improving the performance of accessing shared files becomes an urgent need for enterprises.

The CIFS feature allows Windows clients to identify and access shared resources provided by storage system. With CIFS, clients can quickly read, write, and create files in storage system as on local PCs. The storage system delivers high performance, addressing the problems of decreased access speed and slow response.

The CIFS feature has the following advantages:

- High concurrency

  CIFS supports the file sharing and file locking mechanisms, allowing multiple clients to access and update a file. Multiple clients can access a file at the same time, but only one client is allowed to update the file each time.
- High performance

  Access requests sent by a client for a shared file are cached locally but not delivered to the storage system. When the client sends access requests for shared files again, the system directly reads shared files in the cache, improving access performance.
- Data integrity

  CIFS provides the cache, pre-read, and write back functions to ensure data integrity. If other clients want to access the shared file, the cached data is written to the storage system. Only one copy file is activated each time to prevent data conflicts.
- Robust security

  CIFS supports share access authentication. The authentication management function controls users' access permissions, ensuring data confidentiality and security.
- Wide application

  Any client that supports the CIFS protocol can access the CIFS share space.
- Unified coding standard

  CIFS supports various types of character sets, applicable to different language systems.

Related Concepts

Homedir: It is one of CIFS share modes. In Homedir share mode, a file system is shared to a specific user as an exclusive directory. The user can only view and access the exclusive directory named after its user name.

File system quota: A file system quota can restrict resource usage. There are three types of quotas: **Directory quota**, **User quota**, and **User group quota**.

- **Directory quota**: Restricts the maximum available space or number of all files in a directory. The storage system supports the default directory quota. The default directory quota indicates a quota value that takes effect for all quota trees in a file system. If the default quota is configured but no directory quota is configured for a newly created quota tree, the system enables the quota tree to use the default quota to restrict the available space and number of files.

- **User quota**: Restricts the space or number of files that can be used by a user. The storage system supports the default user quota. The default user quota indicates a quota value that takes effect for all users in a file system or quota tree. If the default quota is configured but no user quota is configured for a user, the system enables the user to use the default quota to restrict the available space and number of files.
- **User group quota**: Restricts the space or number of files that can be used by a user group. The space or number of files used by all members in a user group cannot exceed the user group quota. The storage system supports the default user group quota. The default user group quota indicates a quota value that takes effect for all user groups in a file system or quota tree. If the default quota is configured but no user group quota is configured for a user group, the system enables the user group to use the default quota to restrict the available space and number of files.

When a user or user group quota is configured, **Root Quota Tree** is used as the file system-level quota by default and the capacity and number of files in a file system are restricted with the exception of quota trees.

The following two quota types are involved in each preceding quota type.

- **Space Quota**: maximum capacity of quota tree in a file system
- **File Quantity Quota**: maximum number of files under quota tree in a file system

Access Control List (ACL): a collection of permissions that are authorized to users or user groups to operate shared files. ACL permissions are classified into ACL permission storage and ACL permission authentication. After a user logs in to a share, the user determines the share permissions, reads the ACL permissions, and determines whether files can be read and written. For storage, each ACL permission is called Access Control Entry (ACE). After CIFS shares are mounted to a Windows client, the client sends NT ACLs to a server (storage system that provides CIFS shares). NT ACLs can be discretionary access control lists (DACLs) but cannot be system access control lists (SACLs). That is, NT ACLs do not support audit permissions.

User group: four user groups that are provided by a storage system, namely, **default_group**, **Administrators**, **AntivirusGroup**, and **Backup Operators**.

- **default_group**: default user group. When the group members access the shared file system in the storage systems, they must be authenticated to obtain their permissions.
- **Administrators**: administrator group. When the group members access the shared file system in the storage system, they do not need to be authenticated by share level ACL and NT ACL. They can operate any file in any share with administrator permissions (such as full control, modify, read & execute, list folder contents, read, write, and special permissions).
- **AntivirusGroup**: antivirus user group. The group members can use third-party antivirus software to scan for shared file systems. They have administrator permissions.
- **Backup Operators**: backup user group. The group members can use third-party backup software to back up and recover shared file systems. They do not have administrator permissions.

Signature: data that identifies identities of CIFS clients and servers. It provides an identity verification mode during the transmission process. To prevent SMB packets from being attacked during the transmission process, the SMB protocol supports digital signature of SMB packets.

NOTE

If the signature function is disabled, the storage system may encounter man-in-the-middle (MITM) attacks, resulting in security risks.

1.3.10.2 License Requirements and Compatible Products

This section describes license requirements and compatible products of CIFS.

License Requirements

The CIFS feature is a value-added feature that requires a license.

Compatible Products

Product Series	Product Model	Product Version
OceanStor 2000 V3 series	OceanStor 2200 V3 (16 GB memory) and 2600 V3	V300R006
OceanStor 5000 V3 series	OceanStor 5300 V3, 5500 V3, 5600 V3, and 5800 V3	V300R006
OceanStor 6000 V3 series	OceanStor 6800 V3	V300R006
OceanStor 18000 V3 series	OceanStor 18500 V3 and 18800 V3	V300R006

1.3.10.3 Restrictions

This section describes the CIFS feature in terms of supported protocol versions, network requirements, dependency on other features, and impact on system performance.

Supported Protocol Versions

The storage system supports SMB 1.0, SMB2 (SMB 2.0 and SMB 2.1) and SMB 3.0.

Network Requirements

The CIFS feature supports the IPv4 and IPv6 network access protocols.

Interaction with Other Features

The following table describes the relationship between the CIFS share feature and other features.

Table 1-6 Relationship between the CIFS share feature and other features

Feature	Relationship
File system snapshot	Before accessing a file system snapshot, clients must create a CIFS share for it.

Feature	Relationship
NFS/FTP/HTTP share	● File systems can be shared using multiple protocols. In multi-protocol sharing mode, a file in a file system cannot be written concurrently. Configure read-write sharing based on one protocol and read-only sharing based on the other protocols. **NOTICE** A file in a file system that written concurrently in multi-protocol sharing mode will cause data loss, exercise caution when using it. ● If NFS and CIFS shares are used together and the same file system is operated, restrictions exist in user convergence, lock convergence, permission convergence, and link convergence. Evaluate the scenario based on actual conditions. ● The software that is tightly coupled (audit logs, NT encryption, NT compression, void files, and symbol connections) with NTFS is not supported.

System Impact

File systems can be shared in NFS, CIFS, FTP and HTTP modes at the same time. When clients concurrently access a file system using different protocols, the overall performance slightly decreases.

1.3.10.4 Application Scenarios

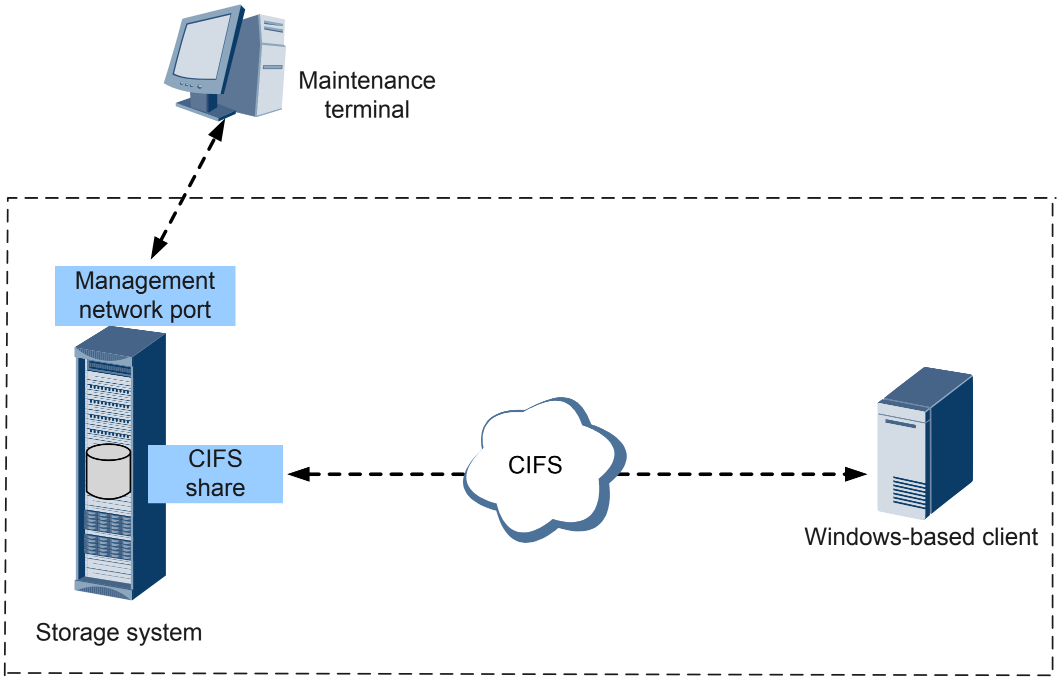
The CIFS share feature is primarily used by Windows-based clients to share files in a non-domain environment or an AD domain environment.

CIFS Share in a Non-Domain Environment

The storage system can employ CIFS shares to share the file systems to users as directories. The users can only view or access their own shared directories. Meantime, the storage system can set shared directories for different users to make shared directories and user names consistent. In this way, the users cannot view or access the shared directories of other users.

As shown in **Figure 1-12**, the storage system serves as the CIFS server and employs the CIFS protocol to provide shared directories system access for clients. After the clients map the shared files to the local directories, users can access the files on the server as accessing local files. You can set locally authenticated user names and passwords in the storage system to determine the local authentication information that can be used for accessing the file system.

Figure 1-12 CIFS share in a non-domain environment



NOTE

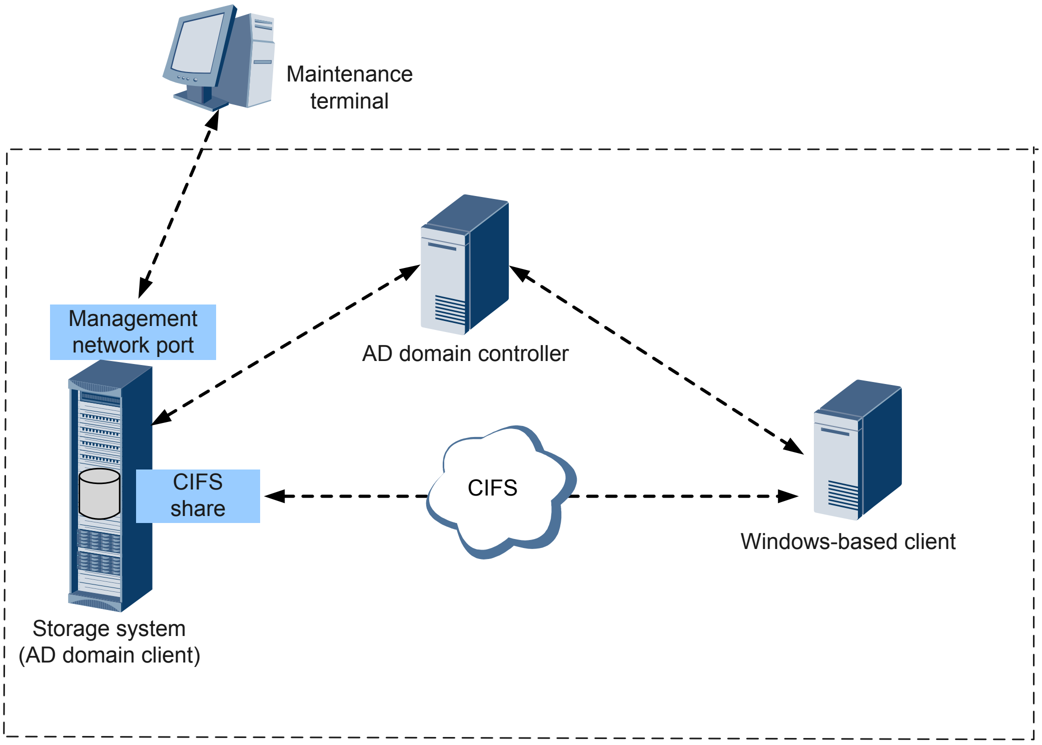
After Homedir is enabled, the storage system can set shared files for different users to make shared directories and user names consistent. In this way, the users cannot view or access the shared directories of other users.

CIFS Share in an AD Domain Environment

With the expansion of local area network (LAN) and wide area network (WAN), many enterprises use the AD domain to manage networks in Windows. The AD domain makes network management simple and flexible.

A storage system can be added to an AD domain as a client. That is, it can be seamlessly integrated with the AD domain. The AD domain controller saves information about all the clients and groups in the domain. Clients in the AD domain need to be authenticated by the AD domain controller before accessing the CIFS share provided by the storage system. All the domain users can access shared directories provided by the storage system. The AD domain user can implement file-specific permission management. Different clients have different permissions for each shared directory. Meantime, a client in the AD domain can only access the shared directory with the same name as the client, as shown in **Figure 1-13**.

Figure 1-13 CIFS share in an AD domain environment



NOTE

If AD domain authentication is used, ensure that the master controller of the storage system can communicate with the domain controller. You can run the **show controller general** command on the CLI to query the master controller.

1.3.11 FTP Feature Description

This chapter describes the basic concepts, availability, and restrictions of the FTP feature.

1.3.11.1 Overview

File Transfer Protocol (FTP) is one of the earliest protocols used by the Internet. It transfers files from one computer to another over the Internet.

Introduction to FTP Protocol

As network technologies continue to develop, increasing files must be shared to different users. Being one of the earliest file transfer protocols, FTP is widely used. FTP uses the Client/Server architecture. A client can send requests to a server for uploading, downloading, creating, and modifying a directory. When FTP is used, two connections are established between a client and a server.

- The control connection is used to control data transfer. Generally, port 21 is used.
- The data connection is used to transfer data between the client and server. Generally, port 20 is used.

Storage system supports the FTP protocol. When the FTP service is enabled in the storage system, a client can use the FTP protocol to access shared files in the storage system.

Advantages of the FTP protocol are as follows:

- The transfer speed is quick. The protocol is suitable for transferring large files. The transfer is faster as the file size increases.
- The FTP protocol is easy to use. It masks computer system information and enables file transfer among different operating systems.

FTPS (FTP-SSL), an extension to the commonly used FTP, adds support for the TLS and the SSL cryptographic protocols. SSL is a protocol that provides data encryption and decryption during secure data transmission between a client and an SSL-based server. The FTPS protocol has two transfer modes:

- Explicit

  Control connection uses port 21 by default and data connection uses port 20 by default.
- Implicit

  Control connection uses port 990 by default and data connection uses port 989 by default.

File Exchange Protocol (FXP) is a protocol for transmitting files between servers. It controls file transmission between two FXP-based servers. In other words, FXP works when an FTP-based client controls two FTP-based servers between which files are transmitted.

Storage systems support FTP, FTPS, and FXP.

NOTE

- The storage system provides the FTPS certificate by default. If you do not need the default certificate, export the certificate request file from the storage system, generate a new certificate file in the certificate server, and import it to the storage system.
- If you need to use FXP, run the **change service ftp fxp_enables=yes** command on the CLI to enable FXP.

Related Concepts

Anonymous user: Indicates users who do not have specified accounts on FTP servers but can still access some public resources using their passwords. User name **Anonymous** is used to access FTP shares.

File system quota: A file system quota can restrict resource usage. There are three types of quotas: **Directory quota**, **User quota**, and **User group quota**.

- **Directory quota**: Restricts the maximum available space or number of all files in a directory. The storage system supports the default directory quota. The default directory quota indicates a quota value that takes effect for all quota trees in a file system. After configured the default quota, if a directory quota is not configured for a newly created quota tree, the system enables the quota tree to use the default quota to restrict the available space and number of files.
- **User quota**: Restricts the space or number of files that can be used by a user. The storage system supports the default user quota. The default user quota indicates a quota value that takes effect for all users in a file system or quota tree. After configured the default quota, if a user quota is not configured for a user, the system enables the user to use the default quota to restrict the available space and number of files.
- **User group quota**: Restricts the space or number of files that can be used by a user group. The space or number of files used by all members in a user group cannot exceed the user group quota. The storage system supports the default user group quota. The default user group quota indicates a quota value that takes effect for all user groups in a file system or quota tree. After configured the default quota, if a user group quota is not

configured for a user group, the system enables the user group to use the default quota to restrict the available space and number of files.

When a user or user group quota is configured, **Root Quota Tree** is used as the file system-level quota by default and the capacity and number of files in a file system are restricted with the exception of quota trees.

The following two quota types are involved in each preceding quota type.

- **Space Quota**: maximum capacity of quota tree in a file system
- **File Quantity Quota**: maximum number of files under quota tree in a file system

1.3.11.2 License Requirements and Compatible Products

This section describes license requirements and compatible products of FTP.

License Requirements

The FTP feature is a basic feature. You do not need to purchase a license.

Compatible Products

Product Series	Product Model	Product Version
OceanStor 2000 V3 series	OceanStor 2200 V3 (16 GB memory) and 2600 V3	V300R006
OceanStor 5000 V3 series	OceanStor 5300 V3, 5500 V3, 5600 V3, and 5800 V3	V300R006
OceanStor 6000 V3 series	OceanStor 6800 V3	V300R006
OceanStor 18000 V3 series	OceanStor 18500 V3 and 18800 V3	V300R006

1.3.11.3 Restrictions

This section describes the FTP feature in terms of supported protocols, network requirements, dependency on other features, and impact on system performance.

Supported Protocols

The storage system supports the FTP and FTPS protocol and FXP mode.

Network Requirements

- The FTP feature supports the IPv4 and IPv6 network access protocols.
- When using the GE port as a service port, do not run NFS and CIFS services on the same port at the same time to ensure the performance of the FTP service.

Interaction with Other Features

Table 1-7 describes the relationship between the FTP feature and other features.

Table 1-7 Relationship between the FTP feature and other features

Feature	Relationship
CIFS/NFS/HTTP	File systems can be shared using multiple protocols. In multi-protocol sharing mode, a file in a file system cannot be written concurrently. When sharing a file system using multiple protocols, you are advised to configure read-write sharing for one protocol and read-only sharing for other protocols. **NOTICE** A file in a file system that written concurrently in multi-protocol sharing mode will cause data loss, exercise caution when using it.

Impact on System Performance

File systems can be shared in NFS, CIFS, FTP, and HTTP modes at the same time. When clients concurrently access a file system based on different protocols, the overall performance slightly decreases.

1.3.12 HTTP Feature Description

This chapter describes the basic concepts, availability, and restrictions of the HTTP feature.

1.3.12.1 Overview

Hypertext Transfer Protocol (HTTP) is one of transfer protocols at the application layer. It is used to transfer hypertext from servers to local clients.

HTTP

Hypertext Transfer Protocol (HTTP) is a protocol for transferring hypertext from web servers to local clients. It improves working efficiency of browsers and reduces data transfer latency on networks. With the protocol, computers can properly and quickly transfer hypertext and determine hypertext contents that need to be transferred and firstly displayed. HTTP works based on the Client/Server architecture. Servers provide hypertext contents for other computers. A client sends an HTTP request to a specified port (port 80 by default) of a server using a browser to access the hypertext contents.

NOTE

If HTTP Over SSL (HTTPS) is used to access a server, the default service port is port 443.

Storage system supports HTTP and HTTPS protocol. When the HTTP service is enabled in the storage system, a client can use HTTP or HTTPS protocol to access hypertext contents in the storage system.

WebDAV

Web-based Distributed Authoring and Versioning (WebDAV) is a communication protocol based on HTTP 1.1 and allows clients to release, lock, and manage web resources.

Storage system supports DAV. When DAV is enabled in the storage system, the WebDAV client can be used to manage HTTP shares in the storage system.

File system quota

Storage system support file system quota. A file system quota can restrict resource usage. There are three types of quotas: **Directory quota**, **User quota**, and **User group quota**.

- **Directory quota**: Restricts the maximum available space or number of all files in a directory. The storage system supports the default directory quota. The default directory quota indicates a quota value that takes effect for all quota trees in a file system. After configured the default quota, if a directory quota is not configured for a newly created quota tree, the system enables the quota tree to use the default quota to restrict the available space and number of files.
- **User quota**: Restricts the space or number of files that can be used by a user. The storage system supports the default user quota. The default user quota indicates a quota value that takes effect for all users in a file system or quota tree. After configured the default quota, if a user quota is not configured for a user, the system enables the user to use the default quota to restrict the available space and number of files.
- **User group quota**: Restricts the space or number of files that can be used by a user group. The space or number of files used by all members in a user group cannot exceed the user group quota. The storage system supports the default user group quota. The default user group quota indicates a quota value that takes effect for all user groups in a file system or quota tree. After configured the default quota, if a user group quota is not configured for a user group, the system enables the user group to use the default quota to restrict the available space and number of files.

When a user or user group quota is configured, **Root Quota Tree** is used as the file system-level quota by default and the capacity and number of files in a file system are restricted with the exception of quota trees.

The following two quota types are involved in each preceding quota type.

- **Space Quota**: maximum capacity of quota tree in a file system
- **File Quantity Quota**: maximum number of files under quota tree in a file system

1.3.12.2 License Requirements and Compatible Products

This section describes license requirements and compatible products of HTTP.

License Requirements

The HTTP feature is a basic feature. You do not need to purchase a license.

Compatible Products

Product Series	Product Model	Product Version
OceanStor 2000 V3 series	OceanStor 2200 V3 (16 GB memory) and 2600 V3	V300R006
OceanStor 5000 V3 series	OceanStor 5300 V3, 5500 V3, 5600 V3, and 5800 V3	V300R006
OceanStor 6000 V3 series	OceanStor 6800 V3	V300R006
OceanStor 18000 V3 series	OceanStor 18500 V3 and 18800 V3	V300R006

1.3.12.3 Restrictions

This section describes the HTTP feature in terms of supported protocols, network requirements, dependency on other features, and impact on system performance.

Supported Protocols

HTTPS (TLS1.1 and TLS1.2), HTTP 1.0 and HTTP 1.1 are supported.

Network Requirements

The HTTP feature supports the IPv4 and IPv6 network access protocols.

Interaction with Other Features

Table 1-8 describes the relationship between the HTTP feature and other features.

Table 1-8 Relationship between the HTTP feature and other features

Feature	Relationship
CIFS/NFS/FTP	File systems can be shared using multiple protocols. In multi-protocol sharing mode, a file in a file system cannot be written concurrently. When sharing a file system using multiple protocols, you are advised to configure read-write sharing for one protocol and read-only sharing for other protocols. **NOTICE** A file in a file system that written concurrently in multi-protocol sharing mode will cause data loss, exercise caution when using it.

Impact on System Performance

File systems can be shared in NFS, CIFS, FTP, and HTTP modes at the same time. When clients concurrently access a file system based on different protocols, the overall performance slightly decreases.

2 Planning Basic Storage Services of a File System

About This Chapter

To strike a balance among storage system security, performance, and cost, you must properly plan basic storage services of a file system before configuring them for the follow-up service configurations and management.

2.1 Planning Process
Before using a storage system, make the following plans to achieve a balance among the security, performance, and cost for using a storage system.

2.2 Planning the Capacity
The capacity of a storage system is used to store service data and system data. To ensure that the capacity for service data is sufficient, plan the capacity for system data properly.

2.3 Planning Disk Domains
A disk domain provides storage space for storage pools, whose storage tiers and available capacities depend on the disk types, capacity, and hot spare policy of the disk domain.

2.4 Planning Storage Pools
Before using a storage system, create storage pools to provide storage space for application servers, and make the following plans on the storage tiers, RAID levels, and hot spare policies based on your requirements.

2.5 Planning a File System
Before using a storage system, properly plan the application scenario, checksum, Atime, quota, capacity, snapshot space ratio, and WORM ensure optimal storage system performance.

2.6 Planning Networks
The network security settings of the storage system must be planned properly to ensure that application servers can safely, reliably, and efficiently access shared files.

2.7 Planning Service Data
Obtain the data required for configuration or plan the data based on site requirements.

2.8 Planning Management User Accounts
Any user that has logged in to a storage system can operate the storage system. Misoperations by a user can impair the storage system reliability and data integrity. To prevent

misoperations, the storage system defines types of users and assigns specific roles to them based on different service scenarios. Moreover, the storage system allows self-defined roles.

2.9 (Optional) Planning Local Authentication Users
When CIFS/FTP/HTTP shares are being matched, different local authentication users or user groups need to be selected for easy user permission control and management.

2.10 Planning File System Sharing
Storage system supports file system sharing in a variety of environments. To facilitate the use of file systems, plan file system sharing based on site requirements.

2.1 Planning Process

Before using a storage system, make the following plans to achieve a balance among the security, performance, and cost for using a storage system.

Figure 2-1 shows the recommended planning process, which is based on user behaviors in different stages. This document describes basic storage service (file services) configurations in non-tenant scenarios. For details about basic storage service (file services) configurations in tenant scenarios, see *OceanStor V3 Series V300R006 SmartMulti-Tenant Feature Guide for File*.

Figure 2-1 Planning Process

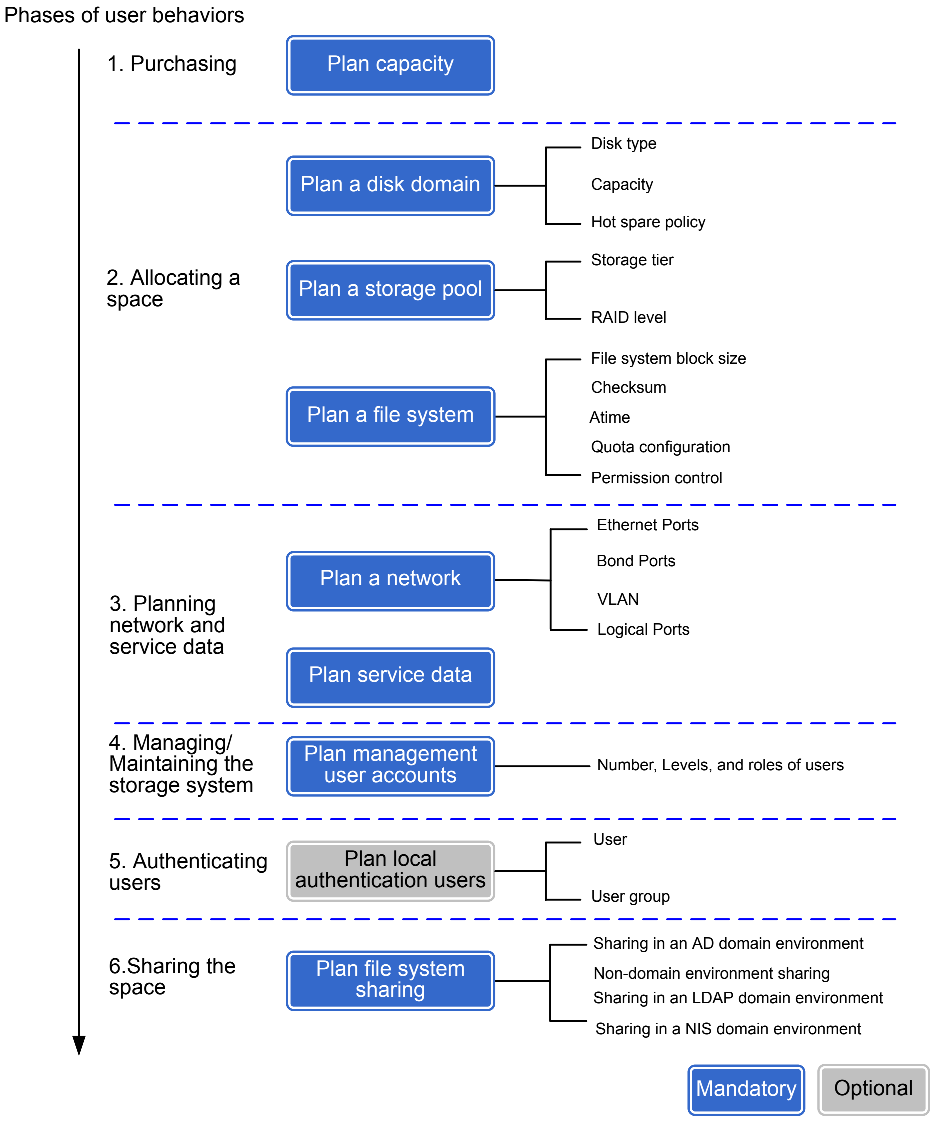


Table 2-1 describes the planning items.

Table 2-1 Planning items

Item	Description	Reference
Planning the capacity	The storage system capacity is used for service data and system data storage. To ensure sufficient capacity for service data, the storage system capacity must be properly planned.	**2.2 Planning the Capacity**

Item	Description	Reference
Planning disk domains	A disk domain provides storage space for storage pools, whose storage tiers and available capacities depend on the disk types, capacity, and hot spare policy of the disk domain. Therefore, the disk types, capacity, and hot spare policy must be properly planned for a disk domain. ● Disk type: Disk types of a disk domain determine the storage tiers of storage pools. Plan disk types based on site requirements. ● Capacity: The capacity of a disk domain determines the available capacities of storage pools. ● Hot spare policy: Plan hot spare policies and hot spare space so that the hot spare space can take over data from failed member disks.	**2.3 Planning Disk Domains**
Planning storage pools	A storage system provides storage space for application servers in the form of storage pools. The storage tiers and RAID levels of the storage pools must be properly planned in advance for better storage utilization. ● Storage tier: Plan storage tiers to meet the need for optimal distribution of hot data and cold data. ● RAID level: Plan RAID levels based on actual needs because RAID levels vary in performance, cost, and reliability.	**2.4 Planning Storage Pools**

Item	Description	Reference
Planning file systems	File systems must be properly planned to optimize storage system space utilization and effectively accelerate storage system responses. ● Application Scenario: Determine the application scenario based on the usage of file systems to ensure optimal allocation of system resources. ● File system block size: The sizes of file system blocks are determined by data blocks written, so that the storage space can be fully utilized. **NOTE** If **Application Scenario** is set to **User Defined**, this parameter needs to be specified. ● Checksum: Verifies data integrity. After the Checksum function is enabled, Checksum of data is automatically calculated when the data is being written. When the data is being read, Checksum ensures the integrity of the data. You can enable this function based on site requirements. ● Atime: Updates file system time. Because this function affects system performance, determine whether to enable this function based on site requirements. ● Quota configuration: Different space sizes and quantities can be configured for different directories to achieve efficient storage resource utilization. ● Permission control: Different permissions of the same directory can be configured for different users, so that the users can only access the directory within their specified permissions.	**2.5 Planning a File System**

Item	Description	Reference
Planning networks	Network security settings of the storage system must be planned properly to ensure that application servers can safely and efficiently access shared files. ● Ethernet Ports: Physically visible port on a device. Physical ports are the bases of VLANs and logical ports. Multiple physical ports can be bonded to form a bond port. ● Bond Ports: To improve data transmission performance of Ethernet ports, bond them and set bonding names and available ports. ● VLAN: Logically divides physical port resources of the storage system into multiple broadcast domains. In a VLAN, when service data is being sent or received, a VLAN ID is configured for the data, so that network and service isolation is implemented for each VLAN, further ensuring service data security and reliability. ● Logical Ports: It is created based on Ethernet ports, bond ports, or VLANs and used for service operation.	**2.6 Planning Networks**
Planning service data	Obtain the data required for configuration or plan the data based on site requirements.	**2.7 Planning Service Data**
Planning management user accounts	Plan the number of users and their permissions carefully for subsequent management and maintenance. Users with different responsibilities should have different permissions.	**2.8 Planning Management User Accounts**
(Optional) Planning local authenticati on users	When CIFS shares are being matched, different authenticated users or user groups need to be selected for easy user permission control and management. ● User: Different users need to be specified for shared directories. ● User group: Each user can only belong to a user group to facilitate user group permission control.	**2.9 (Optional) Planning Local Authentication Users**
Planning file system sharing	Application servers can access file systems only after these file systems are shared. Because file systems are shared differently in various environments, file system sharing must be planned properly.	**2.10 Planning File System Sharing**

2.2 Planning the Capacity

The capacity of a storage system is used to store service data and system data. To ensure that the capacity for service data is sufficient, plan the capacity for system data properly.

The capacity for storing system data refers to the file system capacity, hot spare capacity, and coffer disk capacity. The space overhead consumed by the storage system makes the actual available capacity smaller than the capacity provided by the storage system.

The space overhead consumed by the storage system comprises several parts:

- Capacity used by parity data or mirrored data in a RAID group

  Table 2-2 lists the disk utilization of different RAID levels.

Table 2-2 Disk utilization of different RAID levels

RAID Level	Disk Utilization
RAID 0	The disk utilization is 100%.
RAID 1	● 2D[a]: The disk utilization is about 50%. ● 4D: The disk utilization is about 25%.
RAID 3	RAID 3 supports flexible configurations. Specifically, a RAID 3 policy allows data block and parity block policies ranging from 2D+1P to 13D+1P. The following examples show disk utilization rates of several configurations commonly used by RAID 3: ● 4D + 1P[b]: The disk utilization is about 80%. ● 2D + 1P: The disk utilization is about 66.67%. ● 8D + 1P: The disk utilization is about 88.89%. **NOTE** For a flexibly configured RAID policy *x***D**+*y***P**, the disk utilization is [x/(x + y)] × 100%.
RAID 5	RAID 5 supports flexible configurations. Specifically, a RAID 5 policy allows data block and parity block policies ranging from 2D+1P to 13D+1P. The following examples show disk utilization rates of several configurations commonly used by RAID 5: ● 2D + 1P: The disk utilization is about 66.67%. ● 4D + 1P: The disk utilization is about 80%. ● 8D + 1P: The disk utilization is about 88.89%. **NOTE** For a flexibly configured RAID policy *x***D**+*y***P**, the disk utilization is [x/(x + y)] × 100%.

RAID Level	Disk Utilization
RAID 6	RAID 6 supports flexible configurations. Specifically, a RAID 6 policy allows data block and parity block policies ranging from 2D+2P to 26D+2P. The following examples show disk utilization rates of several configurations commonly used by RAID 6: ● 2D + 2P: The disk utilization is about 50%. ● 4D + 2P: The disk utilization is about 66.67%. ● 8D + 2P: The disk utilization is about 80%. ● 16D + 2P: The disk utilization is about 88.89%. **NOTE** For a flexibly configured RAID policy *x*D+*y*P, the disk utilization is [x/(x + y)] × 100%.
RAID 10	The disk utilization is 50%.
RAID 50	● (2D + 1P) x 2: The disk utilization is about 66.67%. ● (4D + 1P) x 2: The disk utilization is about 80%. ● (8D + 1P) x 2: The disk utilization is about 88.89%.
a: **D** indicates the data block. b: **P** indicates the parity block.	

- Capacity used by hot spare space

  To prevent data loss or performance deterioration caused by a member disk failure, the storage system employs hot spare space to take over data from the failed member disk. The supported hot spare policies are as follows:

  – ■ High

    The capacity of one disk is used as hot spare space if the number of disks at a storage tier equals to or fewer than 12. The hot spare space non-linearly increases as the number of disks increases. When the number of disks at a storage tier reaches 175, the storage tier uses the capacity of one disk in every 100 disks as the hot spare space.

  ■ Low

    The capacity of one disk is used as hot spare space if the number of disks at a storage tier equals to or fewer than 25. The hot spare space non-linearly increases as the number of disks increases. When the number of disks at a storage tier reaches 175, the storage tier uses the capacity of one disk in every 200 disks as the hot spare space.

  ■ None (not supported by 18000, 18000F series storage systems)

    The system does not provide hot spare space.

  Table 2-3 describes how hot spare space changes with the number of disks. The hot spare space changes at a storage tier are used as an example here. The hot spare space changes at different types of storage tiers are the same.

Table 2-3 Changes of hot spare space

Number of Disks	Number of Disks of Which Capacity Is Used as Hot Spare Space in High Hot Spare Policy[a]	Number of Disks of Which Capacity Is Used as Hot Spare Space in Low Hot Spare Policy[a]
(1, 12]	1	1
(12, 25]	2	
(25, 50]	3	2
(50, 75]	4	
(75, 125]	5	3
(125, 175]	6	
(175, 275]	7	4
(275, 375]	8	
...		
a: Huawei storage systems use RAID 2.0+ virtualization technology. Hot spare capacity is provided by member disks in each disk domain. Therefore, the hot spare capacity is expressed in number of disks in this table. For example, if a disk domain is composed of 12 SSDs and the high hot spare policy is used, the hot spare space occupies the capacity of one SSD and the capacity is provided by member disks in the disk domain. If a disk domain is composed of 13 SSDs and the high hot spare policy is used, the hot spare space occupies the capacity of two SSDs.		

NOTE

- For 18000 and 18000F series storage systems, the high hot spare policy is used by default. You can only run the **change disk_domain general** command on the CLI to modify the hot spare policy.
- When you are creating a disk domain, ensure that the disks used to provide hot spare space are sufficient.
- Hot spare space can be used for the current disk domain only.
- **Table 2-3** lists common capacity changes of the hot spare space. The number of disks supported by a storage system and the capacity of their hot spare space are based on actual specifications.

- Capacity used by coffer disks

  For the 2000 and 2000F series storage systems, the first four disks in the storage system are configured as coffer disks. Part of the coffer disk space (each coffer disk requires 5 GB capacity, and four coffer disks require 20 GB in total) can be used to store critical system data, including user configuration data and system logs. The rest of the coffer disk space can be used to store service data.

  If a storage system employs the disk and controller separation architecture, such as the 5000, 5000F, 6000 and 6000F series storage systems, the first four disks in the first disk enclosure are planned to act as coffer disks. (In OceanStor 6800 V3, the first four disks in the first disk enclosure connected to controllers A and B are coffer disks, and the first four disks in the first disk enclosure connected to controllers C and D are coffer disks.) If a storage system employs the disk and controller integration architecture, the first four disks in the storage system are configured as coffer disks. Part of the coffer disk space (each coffer disk provides 5 GB capacity, and four coffer disks provide 20 GB in total) can be used to store critical system data, including configuration data and system logs. The rest of the coffer disk space can be used to store service data.

For the 18000 and 18000F series storage systems, the first four disks in the disk enclosure of the storage system are configured as coffer disks. Part of the coffer disk space (each coffer disk requires 5 GB capacity, and four coffer disks require 20 GB in total) can be used to store critical system data, including configuration data and system logs. The rest of the coffer disk space can be used to store service data.

Capacity partitions of coffer disks are shown in **Table 2-4**.

Table 2-4 Description of coffer disk capacity partitions

Partition Name	Partition Size	Description
LogZone partition	2 GB	Stores system logs and run logs when the storage system is powered off and write through is enabled. The 4 coffer disks are mirrors of each other for redundancy.
CCDB partition	2 GB	Stores the user configuration information (such as replication, HyperMetro, and NAS data). The 4 coffer disks are mirrors of each other for redundancy.
DB partition	1 GB	Stores the user configuration information (such as information about the LUN capacity, ID, WWN, and Fibre Channel ports and iSCSI ports). The 4 coffer disks are mirrors of each other for redundancy.

NOTE

By default, the capacity used by coffer disks is hidden on DeviceManager (the capacity shown on DeviceManager is the value minus the capacity used by coffer disks). The remaining capacity can be used to store other business data.

- Capacity used by file systems and volume management software on the application server

  File systems and volume management software of multiple types on the application server may occupy a portion of space in the storage system. The actually occupied capacities depend on the deployment of applications on the application server.

- WriteHole capacity

  WriteHole is used to resolve inconsistent data stripe verification caused by certain operations before I/Os are delivered to disks. Each disk reserves a 256 MB space as WriteHole capacity.

- Capacity used by system information.

  The system information occupies 577 MB per disk.

- Metadata capacity

  Each disk reserves 0.6% of its total capacity as metadata capacity, and reserves 2% as metadata backup capacity.

- Reserved space for improving system performance and disk balance

  Each disk reserves 1% of its total capacity to improve system performance and disk balance. When 1% of the disk total capacity is smaller than 2 GB, 2 GB of space is reserved.

- Integrated capacity

  When disks are being formatted, if the size of a sector is 520 bytes, the sector uses 8 bytes to store parity data. If the size of a sector is 4160 bytes, the sector uses 64 bytes to store parity data. The integrated capacity usage is about 98.46% (512/520 or 4096/4160).

Without considering the hot spare capacity consumption, you can use the following formula to calculate RAID 2.0+ disk capacity usage: **RAID 2.0+ disk capacity usage = [1 – Metadata space – (1 – Metadata space) × Metadata backup space] × (1 – Disk space reserved for load balancing) x Integrated capacity usage = [1 – 0.6% – (1 – 0.6%) × 2%] × (1 – 1%) × 98.46% ≈ 94.95%**

The disk capacity defined by disk manufacturers is different from that calculated by operating systems. As a result, the nominal capacity of a disk is different from that displayed in the operating system.

- Disk capacity defined by disk manufacturers: 1 GB = 1,000 MB, 1 MB = 1,000 KB, 1 KB = 1,000 bytes.
- Disk capacity calculated by operating systems: 1 GB = 1,024 MB, 1 MB = 1,024 KB, 1 KB = 1,024 bytes.

NOTE

The preceding formulas are for reference only. The disk capacity displayed on the DeviceManager prevails.

Available Capacity Calculation Method

The following uses an example to explain how to calculate the allowed expansion capacity. Three valid digits are retained after the decimal point.

Assume that forty-eight 600 GB SAS disks will be added to the storage system, including four coffer disks and the hot spare policy and RAID policy are configured to **Low** and RAID 6 (8D + 2P) respectively. The allowed expansion capacity is calculated as follows:

1. 600 GB is the nominal capacity provided by the disk vendor. Use the following method to convert this capacity to one that can be identified by the storage system:

   600 GB x (1000/1024) x (1000/1024) x (1000/1024) = 572204.590 MB

   Storage systems provide the DIF function for end-to-end data protection. This function takes 1% to 2% of storage space. The following uses 2% as an example.

   572204.590 MB x (1 – 2%) = 560760.500 MB

2. Minus the WriteHole capacity:

   560760.500 MB – 256 MB = 560504.500 MB

3. Minus the reserved production space:

560504.500 MB － 577 MB = 559927.500 MB

4. Minus the metadata capacity:

   559927.500 MB x (1 － 0.6%) = 556567.935 MB

   NOTE

   The storage system reserves 0.6% of each disk's space as metadata space. It dynamically allocates metadata space as services increase. The actual services prevail. The following uses 0.6% as an example.

5. Minus the metadata backup capacity:

   556567.935 MB x (1 － 2%) = 545436.576 MB

6. Minus the reserved space for improving system performance and disk balance:

   545436.576 MB x (1 － 1%) = 539982.210 MB

7. Minus the integrated capacity: 539982.210 MB x 98.46% = 531666.484 MB

8. Because the hot spare policy of the storage system is set to **Low**, capacity of two disks is used as hot spare space capacity. Therefore, the remaining capacity is as follows after the hot space capacity is deducted:

   531666.484 MB x (48 － 2) = 24456658.264 MB

   Equals to 24456658.264 MB/1024/1024 = 23.324 TB

9. Minus the coffer data capacity:

   23.324 TB － 4 x 5 GB = 23.304 TB

10. Because the RAID policy of the storage system is RAID 6 (8D + 2P), the disk utilization is 80%. Therefore, the allowed expansion capacity is:

    23.304 TB x 80% = 18.643 TB

In this example, the allowed expansion capacity is **18.643 TB**.

NOTE

The preceding available capacity is for reference only. The capacity displayed on the DeviceManager management page prevails.

2.3 Planning Disk Domains

A disk domain provides storage space for storage pools, whose storage tiers and available capacities depend on the disk types, capacity, and hot spare policy of the disk domain.

Planning Disk Types for a Disk Domain (2000, 5000, 6000, 18000 Series Storage Systems)

Disks can be divided based on the following two factors:

- Encryption: Disks can be divided into self-encrypting and non-encrypting disks. Self-encrypting and non-encrypting disks cannot exist in the same disk domain. Encrypted disks are not sold in mainland China.
  - −Self-encrypting disk: When data is written into or read from a disk, the data is encrypted or decrypted using the hardware circuit and internal encryption key of the disk. The self-encrypting disk is a special type of disk.

    Before using self-encrypting disks to create an encrypted disk domain, install and configure key management servers, and complete their interconnections with the storage system. For details, see *OceanStor V3 Series V300R006 Disk Encryption User Guide*.

  - −Non-encrypting disk: Non-encrypting disks are common disks that do not support the encryption function.
- Medium: Disks can be divided into SSDs, SAS disks, and NL-SAS disks.

  A disk type in a disk domain corresponds to a storage tier of a storage pool. If the disk domain does not have a specific disk type, the corresponding storage tier cannot be created for a storage pool.

  Table 2-5 describes the mapping between disk types and storage tiers.

Table 2-5 Mapping between disk types and storage tiers

Disk Type	Storage Tier
SSD	High-performance tier
SAS disk	Performance tier
NL-SAS disk	Capacity tier

Planning Hot Spare Policies for a Disk Domain

To prevent data loss or performance deterioration caused by a member disk failure, the storage system employs hot spare space to take over data from the failed member disk.

To prevent data loss or performance deterioration caused by a member disk failure, the storage system employs hot spare space to take over data from the failed member disk. The supported hot spare policies are as follows:

- - High

    The capacity of one disk is used as hot spare space if the number of disks at a storage tier equals to or fewer than 12. The hot spare space non-linearly increases as the number of disks increases. When the number of disks at a storage tier reaches 175, the storage tier uses the capacity of one disk in every 100 disks as the hot spare space.
  - Low

    The capacity of one disk is used as hot spare space if the number of disks at a storage tier equals to or fewer than 25. The hot spare space non-linearly increases as the number of disks increases. When the number of disks at a storage tier reaches 175, the storage tier uses the capacity of one disk in every 200 disks as the hot spare space.
  - None (not supported by 18000, 18000F series storage systems)

    The system does not provide hot spare space.

  Table 2-6 describes how hot spare space changes with the number of disks. The hot spare space changes at a storage tier are used as an example here. The hot spare space changes at different types of storage tiers are the same.

Table 2-6 Changes of hot spare space

Number of Disks	Number of Disks of Which Capacity Is Used as Hot Spare Space in High Hot Spare Policy[a]	Number of Disks of Which Capacity Is Used as Hot Spare Space in Low Hot Spare Policy[a]
(1, 12]	1	1
(12, 25]	2	
(25, 50]	3	2
(50, 75]	4	
(75, 125]	5	3
(125, 175]	6	
(175, 275]	7	4
(275, 375]	8	
...		
a: Huawei storage systems use RAID 2.0+ virtualization technology. Hot spare capacity is provided by member disks in each disk domain. Therefore, the hot spare capacity is expressed in number of disks in this table. For example, if a disk domain is composed of 12 SSDs and the high hot spare policy is used, the hot spare space occupies the capacity of one SSD and the capacity is provided by member disks in the disk domain. If a disk domain is composed of 13 SSDs and the high hot spare policy is used, the hot spare space occupies the capacity of two SSDs.		

NOTE

- For 18000 and 18000F series storage systems, the high hot spare policy is used by default. You can only run the **change disk_domain general** command on the CLI to modify the hot spare policy.
- When you are creating a disk domain, ensure that the disks used to provide hot spare space are sufficient.
- Hot spare space can be used for the current disk domain only.
- Table 2-6 lists common capacity changes of the hot spare space. The number of disks supported by a storage system and the capacity of their hot spare space are based on actual specifications.

Recommended Configurations for Disks in the Disk Domain

You are advised to configure a maximum of 100 disks for each tier in a disk domain. For example, if the number of disks on a tier is D (divide D by 100 and then round off the result to N and the remainder is M), you can refer to the following configurations:

- If D ≤ 100, configure all disks on this tier in one disk domain.

- If D > 100, create N+1 disk domains and evenly distribute all disks to the N+1 disk domains. That is, the number of disks in each disk domain is D/(N+1). In addition, it is recommended that disk enclosures be fully configured.
- For SmartTier, it is recommended that a maximum of 100 disks be configured for each tier in a disk domain. The configuration of disks on each tier is the same as the preceding principle.

Example 1: The total number of SSDs in the storage system is 328, which is the value of D. (Divide 328 by 100. Round off the result to 3, which is the value of N. The remainder is 28, which is the value of M). You are advised to configure four disk domains, each of which contains 328/4 = 82 SSDs.

Example 2: If the total number of SSDs in the storage system is 223, which is the value of D. (Divide 223 by 100. Round off the result to 2, which is the value of N. The remainder is 23, which is the value of M). You are advised to configure three disk domains, each of which contains 223/3 = 74.3 disks. In this case, two disk domains are configured with 74 disks respectively and the other disk domain is configured with 75 disks.

Example 3: If a disk domain consists of SSDs, SAS disks, and NL-SAS disks, for SmartTier, the number of disks of each type cannot exceed 100.

NOTE

If the project requires a disk domain containing over 100 disks to meet capacity and service planning requirements, contact Huawei technical engineers to evaluate.

Planning Capacity for a Disk Domain (2000, 2000F, 5000, 5000F, 6000, 6000F Series Storage Systems)

The space of a storage pool originates from a disk domain. Therefore, the capacity of the disk domain determines the available capacity of the storage pool. The capacity of the disk domain must be properly planned to make full utilization of storage space. When planning the minimum capacity for a disk domain, you must set related parameters including the hot spare policy, RAID policy, and storage media to ensure that the disk domain can meet capacity requirements of storage pools and hot spare space. **Table 2-7** describes the minimum number of disks required for planning a disk domain (for a single engine).

Table 2-7 Planning a disk domain (for a single engine)

RAID Policy	Minimum Number of Disks in a Disk Domain
RAID 0	4
RAID 1 (2D)	4 NOTE For the 5000 and 6000 series storage systems, if the number of SSDs in a disk domain is two or three, you are advised to configure the corresponding high-performance tier to RAID 1 (2D).
RAID 1 (4D)	4
RAID 10	4

RAID Policy	Minimum Number of Disks in a Disk Domain
RAID 3 (2D+1P)	4
RAID 3 (4D+1P)	6
RAID 3 (8D+1P)	10
RAID 5 (2D+1P)	4
RAID 5 (4D+1P)	6
RAID 5 (8D+1P)	10
RAID 6 (2D+2P)	5
RAID 6 (4D+2P)	7
RAID 6 (8D+2P)	11
RAID 6 (16D+2P)	19
RAID 50 (2D+1P)x2	7
RAID 50 (4D+1P)x2	11
RAID 50 (8D+1P)x2	19

NOTE

- The previous table only lists the minimum disk numbers required in standard RAID levels. In addition to that, the storage system also supports flexible configuration, for example, RAID 5 supports the configuration of 9D+1P to 13D+1P and RAID 6 supports that of 9D+2P to 26D+2P. For a flexibly configured RAID policy **xD+yP**, the minimum disk number is **x+y+z** when the number of required hot spare disks is **z**. The **z** value is determined by the hot spare policy and disk quantity.
- The disks listed in the **Minimum Number of Disks in a Disk Domain** in a Disk Domain column of the preceding table must be provided by the same engine. If the disks that you use to create a disk domain are provided by different engines, ensure that the number of disks on each engine meets the disk number requirements (minimum number of disks).
- Under **Specify disk type** in the **Create Disk Domain** window, you can select the following three types of disks: **High-Performance tier: SSD**, **Performance tier: SAS**, and **Capacity tier: NL-SAS**. If you select only one type, at least four disks of this type are required for each engine. If you select two or three types of disks, at least two SSDs, four SAS disks, and four NL-SAS disks are required for each engine.
- RAID 0 only supports configuration in CLI mode. For details, see the *Command Reference* of the corresponding product model.

Refer to the following suggestions to plan disk domains:

- When creating a disk domain, manually select disks to ensure that all disks are from the same engine. Create disk domains on one engine to reduce the disk failure probability and improve the read and write performance of disks.
- You are advised to use disks of the same type, capacity, and rotating speed (except SSDs) at the same storage tier in a disk domain. If disk capacities are not the same, disks with large capacities may not be used effectively or may become performance bottlenecks, wasting capacities. If disk rotating speeds are different, performance may deteriorate.

- You are advised not to configure the disks of high-density and common disk enclosures in the same disk domain. Otherwise, storage system performance will be adversely affected.
- You are advised to use different disk domains to create storage pools for the block storage service and file storage service.

Planning Capacity for a Disk Domain (18000, 18000F series storage systems)

The space of a storage pool originates from a disk domain. Therefore, the capacity of the disk domain determines the available capacity of the storage pool. The capacity of the disk domain must be properly planned to make full utilization of storage space. When planning the minimum capacity for a disk domain, you must set related parameters including the hot spare policy, RAID policy, and storage media to ensure that the disk domain can meet capacity requirements of storage pools and hot spare space. **Table 2-8** describes the minimum number of disks required for planning a disk domain (for a single engine).

Table 2-8 Planning a disk domain (for a single engine)

RAID Policy	Minimum Number of Disks in a Disk Domain (SSD)	Minimum Number of Disks in a Disk Domain (SAS)[a]	Minimum Number of Disks in a Disk Domain (NL-SAS)[a]
RAID 0	6	8	8
RAID 1 (2D)	6	8	8
RAID 1 (4D)	6	8	8
RAID 10	6	8	8
RAID 3 (2D+1P)	6	8	8
RAID 3 (4D+1P)	6	8	8
RAID 3 (8D+1P)	10	10	10
RAID 5 (2D+1P)	6	8	8
RAID 5 (4D+1P)	6	8	8
RAID 5 (8D+1P)	10	10	10
RAID 6 (2D+2P)	6	8	8
RAID 6 (4D+2P)	7	8	8
RAID 6 (8D+2P)	11	11	11
RAID 6 (16D+2P)	19	19	19
RAID 50 (2D +1P)x2	7	8	8
RAID 50 (4D +1P)x2	11	11	11

RAID Policy	Minimum Number of Disks in a Disk Domain (SSD)	Minimum Number of Disks in a Disk Domain (SAS)[a]	Minimum Number of Disks in a Disk Domain (NL-SAS)[a]
RAID 50 (8D +1P)x2	19	19	19
a: only applies to the 18000 series storage systems.			

NOTE

- The previous table only lists the minimum disk numbers required in standard RAID levels. In addition to that, the storage system also supports flexible configuration, for example, RAID 5 supports the configuration of 9D+1P to 13D+1P and RAID 6 supports that of 9D+2P to 26D+2P. For a flexibly configured RAID policy **xD+yP**, the minimum disk number is **x+y+z** when the number of required hot spare disks is **z**. The **z** value is determined by the hot spare policy and disk quantity.
- The disks listed in the **Minimum Number of Disks in a Disk Domain** in a Disk Domain column of the preceding table must be provided by the same engine. If the disks that you use to create a disk domain are provided by different engines, ensure that the number of disks on each engine meets the disk number requirements (minimum number of disks).
- Under **Specify disk type** in the **Create Disk Domain** window, you can select the following three types of disks: **High-Performance tier: SSD**, **Performance tier: SAS**, and **Capacity tier: NL-SAS**. If you select only **High-Performance tier: SSD**, at least 6 disks of this type are required for each engine. If you select only **Performance tier: SAS** or **Capacity tier: NL-SAS**, at least 8 disks of this type are required for each engine. If you select two or three types of disks, at least two SSDs, four SAS disks, and four NL-SAS disks are required for each engine.
- RAID 0 only supports configuration in CLI mode. For details, see the *Command Reference* of the corresponding product model.

Refer to the following suggestions to plan disk domains:

- When creating a disk domain, manually select disks to ensure that all disks are from the same engine. Create disk domains on one engine to reduce the disk failure probability and improve the read and write performance of disks.
- You are advised to use disks of the same type, capacity, and rotating speed (except SSDs) at the same storage tier in a disk domain. If disk capacities are not the same, disks with large capacities may not be used effectively or may become performance bottlenecks, wasting capacities. If disk rotating speeds are different, performance may deteriorate.
- You are advised not to configure the disks of high-density and common disk enclosures in the same disk domain. Otherwise, storage system performance will be adversely affected.
- If both SAN and NAS services are deployed on a storage system, you are advised to create two disk domains, one for SAN services and the other for NAS services. If you want to configure both SAN and NAS services in one disk domain, contact Huawei technical support engineers to evaluate.

2.4 Planning Storage Pools

Before using a storage system, create storage pools to provide storage space for application servers, and make the following plans on the storage tiers, RAID levels, and hot spare policies based on your requirements.

Usage

Usage of a storage pool is unchangeable after it is configured. If **Usage** of a storage pool is set to **Block Storage Service**, the storage pool can only be used to create LUNs. If **Usage** of a storage pool is set to **File Storage Service**, the storage pool can only be used to create file systems. You are advised to use different disk domains to create storage pools for the block storage service and file storage service.

Storage Tiers (5000 / 6000 / 18000 series storage systems)

A storage pool is a logical combination of one or more storage tiers. The storage pool of the storage system supports a maximum of three storage tiers. A storage tier is a set of storage media that has the same performance and uses the same RAID level. Each storage tier provides different performance at different costs. You can configure storage tiers based on your requirements.

Table 2-9 lists the specifications of each storage tier.

Table 2-9 Specifications of each storage tier

Storage Tier	Storage Medium	Response Speed	Capacity Cost Per Gigabyte	Request Processing Cost Per Gigabyte
High-performance tier	SSD	Fast	High	High
Performance tier	SAS	Medium	Medium	Medium
Capacity tier	NL-SAS	Slow	Low	Low

Functions of different storage tiers are as follows:

- High-performance tier: delivers the highest performance among the three tiers. As the cost of SSDs is high and the capacity of a single SSD is small, the high-performance tier is suitable for applications that require high random read/write performance, for example, database indexes.
- Performance tier: delivers high-performance. As the cost of SAS disks is moderate and the capacity of a single SAS disk is large, the performance tier has good reliability and is suitable for general online applications.
- Capacity tier: delivers the lowest performance among the three tiers. As the cost of NL-SAS disks is the lowest and the capacity of a single NL-SAS disk is large, the capacity tier is suitable for non-critical services, for example, backup.

RAID Levels

Consider the following when selecting RAID levels:

- Reliability

- Read/Write performance
- Disk utilization

Different RAID levels provide different reliability, read/write performance, and disk utilization, as described in **Table 2-10**.

Table 2-10 RAID levels

RAID Level	Redundancy and Data Recovery Capability	Read Performance	Write Performance	Disk Utilization	Maximum Number of Allowed Faulty Disks
RAID 0	No data redundancy is provided and damaged data cannot be recovered.	High	High	The disk utilization is 100%.	0
RAID 1	High. RAID 1 provides completely redundancy. When a CK fails, the mirror CK can be used for data recovery.	Relatively high	Relatively low	● 2D[a]: The disk utilization is about 50%. ● 4D: The disk utilization is about 25%.	A maximum of N-1 disks can fail at the same time (in a RAID 1 disk array with N disks).

RAID Level	Redundancy and Data Recovery Capability	Read Performance	Write Performance	Disk Utilization	Maximum Number of Allowed Faulty Disks
RAID 3	Relatively high. Each CKG has one CK as the parity CK. Data on any data CK can be recovered using the parity CK. If two or more CKs fail, the RAID level fails.	High	Low	RAID 3 supports flexible configurations. Specifically, a RAID 3 policy allows data block and parity block policies ranging from 2D+1P to 13D+1P. The following examples show disk utilization rates of several configurations commonly used by RAID 3: ● 4D + 1P[b]: The disk utilization is about 80%. ● 2D + 1P: The disk utilization is about 66.67%. ● 8D + 1P: The disk utilization is about 88.89%. **NOTE** For a flexibly configured RAID policy *x***D**+*y***P**, the disk utilization is [x/(x + y)] × 100%.	1

RAID Level	Redundancy and Data Recovery Capability	Read Performance	Write Performance	Disk Utilization	Maximum Number of Allowed Faulty Disks
RAID 5	Relatively high. The parity data is distributed on different CKs. In each CKG, the parity data occupies space of a CK. RAID 5 allows the failure of only one CK. If two or more CKs fail, the RAID level fails.	Relatively high	Relatively high	RAID 5 supports flexible configurations. Specifically, a RAID 5 policy allows data block and parity block policies ranging from 2D+1P to 13D+1P. The following examples show disk utilization rates of several configurations commonly used by RAID 5: ● 2D + 1P: The disk utilization is about 66.67%. ● 4D + 1P: The disk utilization is about 80%. ● 8D + 1P: The disk utilization is about 88.89%. **NOTE** For a flexibly configured RAID policy *x***D**+*y***P**, the disk utilization is [x/(x + y)] × 100%.	1

RAID Level	Redundancy and Data Recovery Capability	Read Performance	Write Performance	Disk Utilization	Maximum Number of Allowed Faulty Disks
RAID 6	Relatively high. Two groups of parity data are distributed on different CKs. In each CKG, the parity data occupies space of two CKs. RAID 6 allows two CKs to fail simultaneously. If three or more CKs fail, the RAID level fails.	Medium	Medium	RAID 6 supports flexible configurations. Specifically, a RAID 6 policy allows data block and parity block policies ranging from 2D+2P to 26D+2P. The following examples show disk utilization rates of several configurations commonly used by RAID 6: ● 2D + 2P: The disk utilization is about 50%. ● 4D + 2P: The disk utilization is about 66.67%. ● 8D + 2P: The disk utilization is about 80%. ● 16D + 2P: The disk utilization is about 88.89%. **NOTE** For a flexibly configured RAID policy *x***D**+*y***P**, the disk utilization is [x/(x + y)] × 100%.	2

RAID Level	Redundancy and Data Recovery Capability	Read Performance	Write Performance	Disk Utilization	Maximum Number of Allowed Faulty Disks
RAID 10	High. RAID 10 allows multiple CKs to fail simultaneously. When a CK fails, the mirror CK can be used for data recovery. If a CK and its mirror CK fail simultaneously, the RAID level fails.	Relatively high	Relatively high	The disk utilization is 50%.	A maximum of N disks can fail at the same time (in a RAID 10 disk array with 2N disks).
RAID 50	Relatively high. The parity data is distributed on different CKs of each RAID 5 sub-group. In each RAID 5 sub-group, only one CK is allowed to fail. If two or more CKs of a RAID 5 sub-group fail simultaneously, the RAID level fails.	Relatively high	Relatively high	● (2D + 1P) x 2: The disk utilization is about 66.67%. ● (4D + 1P) x 2: The disk utilization is about 80%. ● (8D + 1P) x 2: The disk utilization is about 88.89%.	1
a: **D** indicates the data block. b: **P** indicates the parity block.					

Select a RAID policy based on the planned solution. The default RAID policy of a storage tier varies with the number of disks allocated to the storage tier.

- If the number of disks allocated to a storage tier is smaller than 10:
  - Default RAID policy of the high performance tier: RAID 10
  - Default RAID policy of the performance tier: RAID 5 (4D+1P)
  - Default RAID policy of the capacity tier: RAID 6 (4D+2P)
- If the number of disks allocated to a storage tier is equal to 10:
  - Default RAID policy of the high performance tier: RAID 10

  - Default RAID policy of the performance tier: RAID 5 (8D+1P)
  - Default RAID policy of the capacity tier: RAID 6 (4D+2P)
- If the number of disks allocated to a storage tier is greater than 10:
  - Default RAID policy of the high performance tier: RAID 10
  - Default RAID policy of the performance tier: RAID 5 (8D+1P)
  - Default RAID policy of the capacity tier: RAID 6 (8D+2P)

For 2000, 5000, 6000, 18000 series storage systems, you can configure RAID policies according to the following rules:

- For critical service systems, such as billing systems of operators and class-A financial online transaction systems, you are advised to configure RAID 6 (8D+2P) for the performance tier. For non-critical service systems, you can configure RAID 5 (8D+1P) for the performance tier.
- You must configure RAID 6 for the capacity tier (NL-SAS).

2.5 Planning a File System

Before using a storage system, properly plan the application scenario, checksum, Atime, quota, capacity, snapshot space ratio, and WORM ensure optimal storage system performance.

File System Parameter Planning

Table 2-11 lists each parameter of a file system.

Table 2-11 File system parameter planning

Parameter	Function	Value
Capacity	Capacity size of a file system to be created.	This parameter is: ● Optional when the default Thin file system is selected during the creation. ● Mandatory when the default Thin file system is not selected during the creation.
Snapshot Space Ratio	By default, 20% of storage system capacity is reserved for snapshots.	The default value is 20%.

Parameter	Function	Value
Application Scenario	Application scenarios of file systems. ● VM: File systems apply to VMs. After this scenario is selected, the system will set the block size of file systems to 8 KB, and automatically adjust system resources to adapt to this scenario. ● Database: File systems apply to databases. You are advised to use full-SSDs for storage pools to which file systems belong and enable the data compression function. – When storage pools to which file systems belong use full-SSDs, the system will set the size of a file system block to 16 KB and enable the data compression function by default. If you choose **Advanced** > **Tuning** and disable the data compression function, the system will set the size of a file system block to 8 KB. In this scenario, you are advised to enable the data compression function. – When storage pools to which file systems belong do not use full-SSDs, the system will set the size of a file system block to 8 KB and disable the data compression function by default. If you choose **Advanced** > **Tuning** and disable the data compression function, the system will still set the size of a file system block to 8 KB. In this scenario, you are not advised to enable the data compression function. ● User Defined: In this scenario, users need to manually specify the block size of file systems.	The value can be **VM**, **Database**, or **User Defined**. The default value is **User Defined**.

Parameter	Function	Value
File System Block Size	If **Application Scenario** is set to **User Defined**, this parameter needs to be specified. Data in the file system consists of fixed-length disk blocks. The size of the blocks (also known as file system block size) affects disk space usage and performance. You are advised to use the block size following the principles below. ● Select 4 KB when the size of most files in the file system is smaller than 100 KB. ● Select 8 KB when the size of most files in the file system is between 100 KB and 1 MB. ● Select 16 KB when the size of most files in the file system is between 1 MB and 100 MB. ● Select 32 KB when the size of most files in the file system is between 100 MB and 1 GB. ● Select 64 KB when the size of most files in the file system is larger than 1 GB, or the file system mainly process bandwidth-consuming large I/Os (in scenarios such as M&E industry, and archive and backup of large files).	The value can be 4 KB, 8 KB, 16 KB, 32 KB, and 64 KB. The default value is 64 KB.
Checksum	The Checksum function is used to check data when the data is being read or written to ensure its integrity. This function is disabled when the data integrity requirement is moderate.	By default, Checksum is enabled.
Automatic Update of Atime	The Atime function is used to update file system access time. Atime updates file system time upon each data read and write, and records file system access time. This function affects system performance because data can be read or written in a serial manner.	By default, Atime is disabled.

Parameter	Function	Value
Capacity Autonegotiation Policy	A storage system supports the following capacity autonegotiation policies: ● **Not Use Capacity Autonegotiation**: The storage capacity used by a file system is fixed and is not flexibly adjusted by the storage system. ● **Auto Expand Capacity**: increases file system capacity and meets users' requirements in data write when the available space of a file system is about to run out and the storage pool has available space. ● **Auto Reduce or Expand Capacity**: The storage system automatically adjusts the file system capacity based on file system space usage. When the available space of a file system is about to run out and the storage pool has available space, automatic capacity expansion will be used to increase file system capacity. When the file system's storage space is released, it can be reclaimed into a storage pool and used by other file systems in data write requests.	By default, the capacity autonegotiation policy is **Not Use Autonegotiation**.

Parameter	Function	Value
Quota	The file system allows quotas to be configured in a shared quota tree. A quota restricts the file quantity and storage space size in a quota tree. A quota can be soft and hard. ● For file quantity, a hard quota refers to the maximum number of files created in a quota tree, while, a soft quota refers to an alarm threshold of file quantity. ● For storage space, a hard quota refers to the maximum capacity of storage space in a quota tree, while, a soft quota refers to an alarm threshold in quota tree space. If the capacity value or number of files that a user created exceeds the soft quota, the creation will succeed but an alarm is returned. If the capacity value or number exceeds the hard quota, the creation will fail and a failure event is returned. The type of the file system can be **Directory Quota**, **User Quota** or **User Group Quota**. ● If you want to restrict the space used by files or the number of files in the root directory, select **Directory quota**. ● If you want to restrict the space used by files or the number of user, select **User Quota**. ● If you want to restrict the space used by files or the number of user group, select **User Group Quota**. Root Quota Tree is the quota tree created for the file system by default. This quota tree cannot be deleted and you cannot modify its name. Root Quota Tree is only available when creating user quota or user group quota for file system. It is not available for directory quota.	The quota value is blank.
WORM	WORM parameters, the WORM file system ensures the file after being written into the file system, cannot be modified, deleted, or migrated within the specific WORM protection period but can be read multiple times. **NOTE** For details about the WORM feature, see *OceanStor V3 Series V300R006 WORM Feature Guide*.	By default, WORM is disabled.

File System Value-Added Feature Planning

After a file system is shared to a host, the file system supports the following features or functions:

- HyperVault (Work as source or backup file system)
- SmartPartition
- SmartCache

  NOTE

  - SmartCache does not support self-encrypting SSD.
  - SmartCache is not supported by 2000F, 5000F, 6000F, 18000F series storage systems.
- SmartDedupe&SmartCompression
- VAAI
- SmartQoS
- Snapshot (Work as source file system)
- Remote Replication (Work as primary or secondary file system)

2.6 Planning Networks

The network security settings of the storage system must be planned properly to ensure that application servers can safely, reliably, and efficiently access shared files.

Planning Ethernet Ports

Ethernet ports are ports physically visible on a device. They are the bases of virtual local area networks (VLANs), bond ports and logical ports.

Bond Ports

Port bonding provides more bandwidth and redundancy for links. After Ethernet ports are bonded, **MTU** changes to the default value and you must set the link aggregation mode for the ports. For example, on Huawei switches, you must set the ports to the static LACP mode.

NOTE

- The port bond mode of a storage system has the following restrictions:
  - On the same controller, a bond port is formed by a maximum of eight Ethernet ports.
  - Only the interface modules with the same port rate (GE or 10GE) can be bonded.
  - The port cannot be bonded across controllers. Non-Ethernet network ports cannot be bonded.
  - SmartIO cards cannot be bonded if they work in cluster or FC mode or run FCoE service in FCoE/iSCSI mode.
  - Read-only users are unable to bind Ethernet ports.
  - Each port only allows to be added to one bonded port. It cannot be added to multiple bonded ports.
  - Physical ports are bonded to create a bond port that cannot be added to the port group.
- Although ports are bonded, each host still transmits data through a single port and the total bandwidth can be increased only when there are multiple hosts. Determine whether to bond ports based on site requirements.
- The detailed link aggregation mode varies with the switches' manufacturer.

Planning VLANs

VLANs logically divide the physical Ethernet port resources of the storage system into multiple broadcast domains. In a VLAN, when service data is being sent or received, a VLAN ID is configured for the data, so that the networks and services of VLANs are isolated, further ensuring service data security and reliability.

VLANs are created based on Ethernet ports or bond ports. One physical port can belong to multiple VLANs. A bond port instead of one of its bonded physical Ethernet port can be used to create a VLAN. The VLAN ID ranges from 1 to 4094. You can enter a VLAN ID or VLAN IDs in batches.

Planning Logical Ports

Logical ports, used for NAS service operation, are created based on Ethernet ports, bond ports, or VLANs.

- If logical ports are created based on Ethernet network ports, bond ports, or VLAN ports, ensure that IP addresses are not configured for the ports.
- If logical ports are created based on Ethernet network ports, bond ports, or VLAN ports, the Ethernet network ports, bond ports, or VLAN ports can only be used for one storage service, block storage service, or file system storage service.
- You must specify a primary port for logical port. If the primary port fails, services will fail over to a functional port.
- You must activate logical port before using it.

NOTICE

If you want to enable the IP address floating function (Shares of file systems do not support the multipathing mode. IP address floating is used to improve reliability of links) before configuring basic storage services, you must reserve at least two ports (Ethernet port and VLAN port or bond port) available for IP address floating and ensure that IP addresses are not configured for the ports. When a port fails, services can be smoothly switched to the other port.

2.7 Planning Service Data

Obtain the data required for configuration or plan the data based on site requirements.

Table 2-12 describes the data to be obtained before storage space configuration.

Table 2-12 Data to be obtained

Operation	Item	Default/Actual Value
Logging in to the DeviceManager	**IP addresses of the management network ports.** *IP address to be entered in the browser address box for logging in to the DeviceManager of the storage system.*	For 2000 series storage systems, the default IP addresses of the management network ports on controllers A and B are respectively 192.168.128.101 and 192.168.128.102, and the default subnet mask is 255.255.255.0. For a 2 U controller enclosure (5300 V3/5500 V3), the default IP addresses of the management network ports on controllers A and B are respectively **192.168.128.101** and **192.168.128.102**, and the default subnet mask is **255.255.255.0**. For a 3 U or 6 U controller enclosure (5600 V3/5800 V3/6800 V3), the default IP addresses of the management network ports on management modules 0 and 1 are respectively **192.168.128.101** and **192.168.128.102**, and the default subnet mask is **255.255.0.0**.
	User name and password *User name and password for logging in to the DeviceManager of the storage system.*	Super administrator user name: admin Initial password: Admin@storage
Creating a disk domain	**Disk domain name** *Name of the disk domain to be created.*	__________________
	Disk type *Disk types in the disk domain, which determine the storage tiers that can be created. SSDs correspond to the high performance tier, SAS disks correspond to the performance tier, and NL-SAS disks correspond to the capacity tier.*	High performance Tier (SSD)__________________ Performance Tier (SAS)__________________ Capacity Tier (NL-SAS)__________________
Creating a storage pool	**Storage pool name** *Name of the storage pool to be created.*	__________________

Operation	Item	Default/Actual Value
	Storage tier *The storage pool can have the high performance tier, performance tier, and capacity tier.*	High performance Tier (SSD)__________________ Performance Tier (SAS)__________________ Capacity Tier (NL-SAS)__________________
	RAID policy *Each tier is configured with a specific RAID policy. The default RAID policy on the DeviceManager is recommended. For example, the default RAID policy of the performance tier on the DeviceManager is* ***RAID5 4D+1P****, where D indicates the data block and P indicates the parity block.*	High performance Tier__________________ Performance Tier__________________ Capacity Tier__________________
	Capacity *Capacity of each storage tier. The value must be an integer on the DeviceManager.*	High performance Tier__________________ Performance Tier__________________ Capacity Tier__________________
Creating a file system	**File system name** *If LUNs are batch created, the storage system automatically names each file system by adding four digits after your specified file system name.*	__________________
	Thin enabled or not *After the thin provisioning function is enabled for a created file system, the storage system does not allocate all preset capacities to the file system. Instead, the storage system dynamically allocates storage resources on demand based on site requirements.*	Yes____ No____
	Capacity *Storage space size of a file system to be created.*	__________________

Operation	Item	Default/Actual Value
	Application Scenario *The file system block size determined by the application scenario.*	____________________
	File system quantity *Number of file systems to be created in the storage system.*	____________________
	Owning storage pool *Storage pool to which a file system to be created belongs.*	____________________
	Checksum *Parity switch for data integrity.*	Yes____ No____
	Atime *Switch to update file system access time.*	Yes____ No____
Creating a logical port	**Name of a logical port** *Name of a newly created logical port.*	____________________
	IP address type *Type of a logical port's IP address.*	____________________
	IPv4 address or IPv6 address *IP address of a logical port set for file system service operation.* **NOTE** Ensure that the IP address can be pinged on a host.	____________________
	Subnet mask or prefix *Subnet mask of a logical port's IPv4 address.*	____________________

Operation	Item	Default/Actual Value
	IPv4 gateway or IPv6 gateway *IPv4 gateway or IPv6 gateway of a logical port.* NOTE A gateway must be configured if the IP address and host IP address do not reside on the same network segment.	____________________
	Primary port *10GE/GE physical port reserved for file system service operation. Each logical port corresponds to a primary port.*	____________________

2.8 Planning Management User Accounts

Any user that has logged in to a storage system can operate the storage system. Misoperations by a user can impair the storage system reliability and data integrity. To prevent misoperations, the storage system defines types of users and assigns specific roles to them based on different service scenarios. Moreover, the storage system allows self-defined roles.

The storage system defines the following three user roles:

- Super administrator: A super administrator has full control permission over the storage system and can create users at the same or a lower level.
- Administrator: An administrator has partial control permission over the storage system but cannot create user accounts, upgrade the storage system, or import a configuration file.
- Read-only user: A read-only user has only access permission to the storage system and can perform queries only, for example, querying the working status and health status of the storage system.

Table 2-13 and **Table 2-14** show the roles preset by the storage system and their permissions.

Table 2-13 System roles

Preset Role	Function Group	Permissions
Super administrator	System group	All permissions over the system
Administrator	System group	All permission except those of user management and security configuration

Preset Role	Function Group	Permissions
Security administrator	System group	Permission of configuring system security, including managing security rules, certificates, auditing, KMC, anti-virus software, data erasing, and regulation clocks
Network administrator	System group	Permission of managing the system network, including physical ports, logical ports, VLANs, and failover groups
SAN resource administrator	System group	Permission of managing SAN resources, including storage pools, LUNs, mapping views, hosts, and ports
NAS resource administrator	System group	Permission of managing NAS resources, including storage pools, file systems, file servers, authenticated users, networks, quota trees, and shares
Data protection administrator	System group	Permission of data protection management, including local data protection, remote data protection, and HyperMetro data protection
Backup administrator	System group	Permission of managing data backup, remote data protection, including local data and mapping views

Table 2-14 Tenant roles

Preset Role	Function Group	Permissions
vStore administrator	vStore group	All permissions of managing vStores
vStore data protection administrator	vStore group	Permission of data protection management, including local data protection, remote data protection, and HyperMetro data protection for vStores
vStore protocol administrator	vStore group	Permission of managing vStore protocols, including authenticated users and shares of vStores

Besides preset roles, the storage system also supports self-defined roles. For details about the permissions of self-defined roles, see **A Permission Matrix for Self-defined Roles**.

2.9 (Optional) Planning Local Authentication Users

When CIFS/FTP/HTTP shares are being matched, different local authentication users or user groups need to be selected for easy user permission control and management.

Local Authentication Users

When planning a local authentication user, you need to pay attention to the following planning items:

- Username
- Password and security policies
- Primary group

  The primary group to which users belong controls the users' permission for CIFS shares. A user must and can only belong to one primary group.
- Secondary group

  The concepts of primary group and secondary group are for local authentication users and have no relationship with each other. A local authentication user must belong to a primary group but not to a secondary group.

NOTE

For details about how to create a local authentication user, see **Creating a Local Authentication User**.

Local Authentication User Groups

A user group consists of different users. You can assign different permissions for different user groups. Then users in the user groups can inherit the permissions of the user groups.

2.10 Planning File System Sharing

Storage system supports file system sharing in a variety of environments. To facilitate the use of file systems, plan file system sharing based on site requirements.

File systems can be shared using four protocols: NFS, CIFS, FTP, and HTTP. In Homedir share mode, a file system is shared to a specific user as an exclusive directory. The user can only access the exclusive directory named after its user name.

NFS Share

This sharing mode applies mainly to the file system sharing in Linux or UNIX. NFS works based on client/server architecture. A server provides other computers with file system access, and clients access the shared file systems. NFS enables clients running a variety of operating systems to share files over a network. It has the following highlights:

- Powerful concurrent processing capability. Multiple clients can use the same file so that all the users on the network can access the same data.
- Solid data integrity. All users can read the same group of files.
- Ease of use. File system mounting and remote file system access are transparent to users.

Planning an NFS share helps facilitate the follow-up service configuration. The following items need to be planned: networks, domains, permissions, and clients.**Table 2-15** lists the required preparation items.

Table 2-15 NFS share planning

Planned Item	Subitem	Requirement	Example
Network	IP address of the storage system	The storage system uses logical port (LIF[a]) to provide shared space for a client.	172.16.128.10
	IP address of the access client.	The access client and storage system are accessible, and they can ping each other.	192.168.0.10
	IP address of the maintenance terminal	The maintenance terminal and storage system are accessible, and they can ping each other.	192.168.128.10
	NIS or LDAP domain	In a NIS or LDAP domain, collect the domain server's IP address and domain information and ensure that the domain server and storage system reside on the same network and they can **ping** each other.	LDAP server 172.16.128.15
Domain	Non-domain, NIS domain, or LDAP domain	Configure a non-domain environment, NIS domain, or LDAP domain based on site requirements. Generally, configure a domain environment for a large-sized enterprise or an enterprise that requires high security. **NOTE** When adding a storage system to a domain, you must connect dual controllers of the storage system to the domain controller.	LDAP

Planned Item	Subitem	Requirement	Example
Permission	-	Set users' permissions for accessing a file system. ● When NFS v3 is used, the storage system supports UGO permissions but not ACL permissions. UGO permissions include **Execute**, **Read**, and **Write**. NOTE You can run command **admin:/ >change service nfs support_v3_enabled=on v3_acl_enabled=on** and remount the file system of the NFS share to enable ACL permissions. ● When NFS v4 is used, the storage system supports both UGO permissions and ACL permissions. ACL permissions include **List Directories**, **Read Data**, and **Write Data**.	Read-only
Quota	(Optional) Quota for quota tree of file system.	Quotas can be defined only for quota trees of a file system based on customer requirements. There are three types of quotas: **Directory quota, User quota**, and **User group quota**. ● **Directory quota**: Restricts the maximum available space or number of all files in a directory. ● **User quota**: Restricts the space or number of files that can be used by a user. ● **User group quota**: Restricts the space or number of files that can be used by a user group. The following two quota types are involved in each preceding quota type. ● **Space Quota**: maximum capacity of quota tree in a file system ● **File Quantity Quota**: maximum number of files under quota tree in a file system NOTE **User quota** and **User group quota** can be used for NFS share in only NIS or LDAP domain.	-

Planned Item	Subitem	Requirement	Example
a: A LIF is a logical port created on the physical port, bond port, and VLAN. Each LIF corresponds to an IP address.			

NOTE

In scenarios where a firewall is deployed, ensure that the RPCBIND service and the corresponding NFS port are enabled on the client.

CIFS Share

This sharing mode is mainly applied by Windows hosts to access files or other resources over the Internet or an intranet. CIFS allows Windows clients to identify and access shared storage system resources. With CIFS, clients can quickly read, write, and generate files in storage systems as on local PCs. CIFS helps maintain a high access speed and a short system response when even a large number of users concurrently access the same shared file. CIFS has the following highlights:

- Powerful concurrent processing capability. The file sharing and file lock mechanisms offered by CIFS prevent client conflicts when multiple clients read or update the same file. However, only one client can update the file at a time.
- High performance. Access requests sent by a client for a shared file are cached locally first instead of being directly delivered to the storage system. When the client sends a request for the shared file again, the file is read from cache to improve access performance.
- Solid data integrity. CIFS provides cache preemption, prefetch, and writeback to ensure data integrity. Access requests sent by a client for a shared file are cached locally first instead of being directly delivered to the storage system. If other clients want to access the shared file, the cached data is written to the storage system. Only one file copy is activated each time to prevent data conflicts.
- Robust security. CIFS can be used to authenticate the access requests for a share. The authentication management controls users' access permissions, ensuring data confidentiality and security.
- Wide application. Any CIFS-capable client can access a CIFS shared space.
- Unified coding standard. CIFS supports various types of character sets, applicable to different language systems.

Planning a CIFS share helps facilitate the follow-up service configuration. The following items need to be planned: networks, domains, authentication modes, sharing modes, users, user groups, permissions, and quotas.**Table 2-16** lists the required preparation items.

Table 2-16 CIFS share planning

Planned Item	Subitem	Requirement	Example
Network	IP address of the storage system	The storage system uses logical port (LIF[a]) to provide shared space for a client.	172.16.128.10

Planned Item	Subitem	Requirement	Example
	IP address of the access client.	The access client and storage system are accessible, and they can **ping** each other.	192.168.0.10
	IP address of the maintenance terminal	The maintenance terminal and storage system are accessible, and they can **ping** each other.	192.168.128.10
	(Optional) AD domain.	In an AD domain, IP addresses and host names of the AD domain server and DNS server must be configured. All those servers and the storage system must reside on the same network, and they can **ping** each other.	AD server 172.16.128.115
Domain environment	AD domain or non-domain environment.	Configure an AD domain or non-domain environment based on onsite requirements. The advantages of the AD domain and non-domain environments are described as follows: ● AD domain: The storage system can be seamlessly integrated with the AD domain. Domain users can directly access the shared space, and no local users need to be created. **NOTE** When adding a storage system to a domain, you must connect master controller of the storage system to the domain controller. ● Non-domain: No domain environments need to be set up.	AD domain
Authentication mode	Local, domain, or global authentication.	Configure an authentication mode based on the domain environment (AD domain or non-domain environment). ● Local authentication: Local user are used to validate the accounts identity. ● Domain authentication: Domain servers are used to validate the user identity. ● Global authentication: Local authentication is used first. If local authentication is not passed, domain authentication is used.	Global authentication

Planned Item	Subitem	Requirement	Example
Share mode	CIFS share.	In CIFS share mode, a file system or its quota tree[b] is shared among authentication users including local authentication users and domain authentication users. Users have their permissions set by storage system for accessing CIFS shares.	CIFS share
	Homedir.	In Homedir share mode, a file system is shared to a specific user as an exclusive directory. The user can only access the exclusive directory named after its user name.	-
User	-	Local authentication user or domain user.	user1
User group	-	Local authentication user group or domain user group.	default_group
Permission	Permission of a user or user group to access a share.	Set a user's permission to access a CIFS share. Possible permissions are: ● Read-only: The user can only read the CIFS share. ● Read-write: The user can read and write the CIFS share. ● Full control: The user has full permission for the CIFS share. ● Forbidden: The user is forbidden to access the CIFS share.	Read-only

Planned Item	Subitem	Requirement	Example
Quota	(Optional) Quota for quota tree of file system.	Quotas can be defined only for quota tree of a file system based on customer requirements. Quotas include: ● **Directory quota**: Restricts the maximum available space or number of all files in a directory. ● **User quota**: Restricts the space or number of files that can be used by a user. ● **User group quota**: Restricts the space or number of files that can be used by a user group. The following two quota types are involved in each preceding quota type. ● **Space Quota**: maximum capacity of quota tree in a file system ● **File Quantity Quota**: maximum number of files under quota tree in a file system	-
a: A LIF is a logical port created on the physical port, bond port, and VLAN. Each LIF corresponds to an IP address. b: Quota tree refers to the quota tree and is a special directory of the file system. You can set a directory quota on the quota tree to manage the space used by all files under the directory.			

NOTE

By default, the storage system uses port 445 to provide the CIFS share service (port 139 is not supported) for external devices. Therefore, in a scenario where a firewall is deployed, port 445 must be enabled for clients.

FTP Share

This sharing mode applies mainly to file transfer between computers. FTP uses client/server architecture. A client can send requests to a server for uploading, downloading, generating, and changing a directory. FTP requires two connections between a client and a server:

- Control connection. used to control data transfer. Generally, port 21 is used. In an environment with the firewall function, you need to enable port 21.
- Data connection. used to transfer data between the client and server. Generally, port 20 is used. In an environment with the firewall function, you need to enable port 20.

FTP has the following highlights:

- Quick transfer. FTP is suitable for transferring large files. The larger the files, the quicker the file transfer is.
- Ease of use. FTP masks computer system information and enables file transfer between different operating systems.

The storage system also supports the FTPS (FTP-SSL) protocol. FTPS, an extension to the commonly used FTP, adds support for the TLS and the SSL cryptographic protocols. SSL is a protocol that provides data encryption and decryption during secure data transmission between a client and an SSL-based server. The FTPS protocol has two transfer modes:

- Explicit

  Control connection uses port 21 by default and data connection uses port 20 by default. In an environment with the firewall function, you need to enable port 20 and 21.

- Implicit

  Control connection uses port 990 by default and data connection uses port 989 by default. In an environment with the firewall function, you need to enable port 989 and 990.

When a GE port is used as a service port, do not simultaneously run both NFS and CIFS share services on the port, to ensure the FTP service performance.

HTTP Share

HTTP is applied mainly to transfer hypertext from web servers to local browsers. It improves working efficiency of browsers and reduces network transfer workload. With HTTP, computers can correctly and quickly transfer hypertext. In addition, HTTP determines which part of hypertext content to transfer and which part of transferred content to be firstly displayed. HTTP works based on client/server architecture. Servers provide hypertext content for other computers. A client sends an HTTP request to a specified port of a server using a browser to access the hypertext content.

NOTE

If a client uses HTTPS protocol to access the server, the default port of the server is 443. In an environment with the firewall function, you need to enable port 443.

After learning the characteristics of different share protocols, users can select the appropriate protocol based on service requirements.

NOTE

When sharing a file system, ensure that the file system is online.

3 Configuring Basic Storage Services

About This Chapter

After configuring basic storage services, you can divide the storage space provided by the storage system into multiple file systems, so that application servers can access the storage space.

This operation enables you to restrict the space used by files or the number of files in the root directory or by user/user group.

3.9 Sharing File Systems
This section describes how to share file systems.

3.1 Configuration Process

The configuration process includes the overall procedures for configuring the storage space. You can learn about the storage space configuration logic.

The flowchart for configuring storage space is shown in **Figure 3-1**.

- This document describes basic storage service (file services) configurations in non-tenant scenarios. For details about basic storage service (file services) configurations in tenant scenarios, see *OceanStor V3 Series V300R006 SmartMulti-Tenant Feature Guide for File*.
- For details about how to interconnect OpenStack and storage systems, see **B Obtaining and Configuring Manila Driver**.

  NOTE

  Excluding OceanStor 2200 V3 (8 GB memory) edition.

Figure 3-1 Storage Space Configuration Process

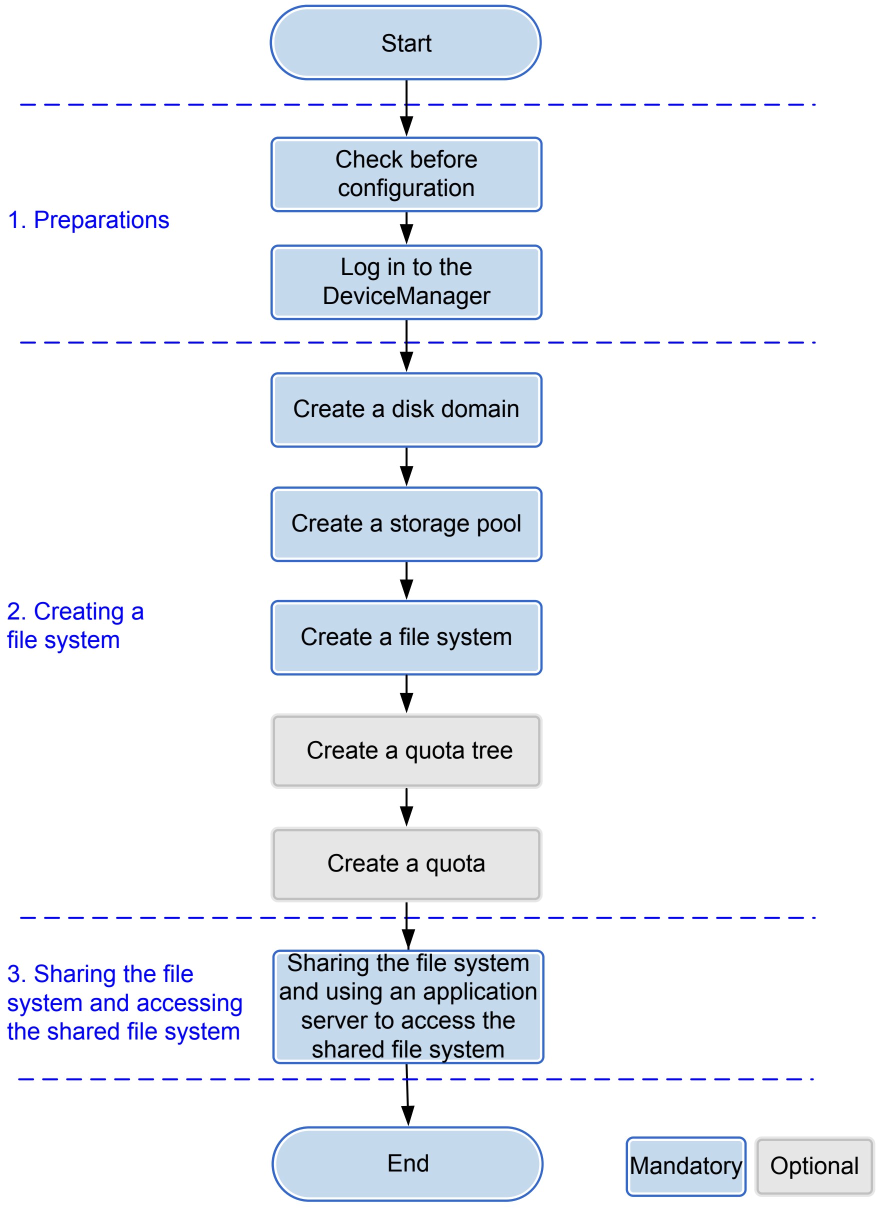

Start
1. Preparations
Check before configuration
Log in to the DeviceManager
2. Creating a file system
Create a disk domain
Create a storage pool
Create a file system
Create a quota tree
Create a quota
3. Sharing the file system and accessing the shared file system
Sharing the file system and using an application server to access the shared file system
End
Mandatory
Optional

Table 3-1 lists each storage space configuration step.

Table 3-1 Procedures for configuring storage space

Procedure	Operation	Description	Reference
1. Preparing for configuration	Check before configuration	Check whether the software installation and initial configuration meet the storage space requirements.	**3.2 Checking Before Configuration**
	Logging in to the DeviceManager	The DeviceManager is a device management platform program developed by Huawei Technologies Co., Ltd. You can log in to the DeviceManager to manage and maintain the storage system.	**3.3 Logging In to the DeviceManager**
2. Creating a file system	Creating a disk domain	A disk domain provides storage space for storage pools, whose storage tiers and available capacities depend on the disk types, capacity, and hot spare policy of the disk domain. The storage system automatically allocates hot spare space with different capacities based on hot spare policies to take over data from failed member disks.	**3.4 Creating a Disk Domain**
	Creating a storage pool	The storage space used by application servers is provided by the storage pools on the storage system.	**3.5 Creating a Storage Pool**

Procedure	Operation	Description	Reference
	Creating a file system	Application servers require a file system to access storage system space.	**3.6 Creating a File System**
	(Optional) Creating a quota tree	Quota tree is the level-1 subdirectory of a file system. In a quota tree, you can set directory quotas, user quotas, or user group quotas. You can manage space occupied by files in the directory.	**3.7 (Optional) Creating a Quota Tree**
	(Optional) Creating a quota	This operation enables you to restrict the space used by files or the number of files in the root directory or by user/user group.	**3.8 (Optional) Creating a Quota**
3. Sharing the file system and accessing the shared file system	Sharing the file system and using an application server to access the shared file system	A file system must be shared before application servers access storage system space.	**3.9 Sharing File Systems**

3.2 Checking Before Configuration

Check whether the software installation and initial configuration meet the storage space requirements.

Checking Initial Configuration

- Network connection status

  Table 3-2 lists the check items and provides the check methods.

Table 3-2 Network connection status checklist

Category	Check Item	Check Method
Connection between the maintenance terminal and storage system	Check whether the management network port on the storage system communicates with the maintenance terminal properly.	In the command-line interface (CLI) mode on the maintenance terminal, run the following command: ● For IPv4, **ping** *ip* (where *ip* indicates the IP address of the management network port). ● For IPv6, **ping6** *ip* (where *ip* indicates the IP address of the management network port). If the maintenance terminal receives data packets from the management network port, the communication between the storage system and maintenance terminal is normal. Check whether the physical link is up and then whether the IP address is correctly configured.
Connection between the storage system and application server (using the Windows-based application server as an example)	When an iSCSI host port on the storage system is used for connection, check whether the iSCSI host port communicates with the service network port on the application server properly.	On the CLI of the application server, run the following command: ● For IPv4, **ping** *ip* (where *ip* indicates the IP address of the iSCSI host port). ● For IPv6, **ping6** *ip* (where *ip* indicates the IP address of the iSCSI host port). If the application server receives data packets from the iSCSI host port, the communication between the storage system and application server is normal. If the application server receives no data packets from the iSCSI host port, replace network cable, change the IP address of the iSCSI host port or add a route between the iSCSI host port and service network port and try again. For details about how to change the IP address of an iSCSI host port or add a route between an iSCSI host port and a service network port, see the DeviceManager online help.

- Licenses

  Log in to the DeviceManager. Check whether information about basic features or value-added features in the existing license file is the same as that contained in the purchased license file. If the information is different, contact technical support engineers.

3.3 Logging In to the DeviceManager

The DeviceManager is a device management program developed by Huawei Technologies Co., Ltd. The DeviceManager has been loaded to the storage system before delivery. You can log in to the DeviceManager to achieve centralized management of storage resources.

3.3.1 Logging In to the DeviceManager Through Web

You can log in to the DeviceManager on any maintenance terminal connected to the storage system by using the management network port IP address of the storage system and the local or domain user name in a browser.

Prerequisites

Verify that the maintenance terminal meets the following requirements before you use the DeviceManager software:

- Operating system and browser versions.

  DeviceManager supports multiple operating systems and browsers. You can query the compatibility using the **OceanStor Interoperability Navigator**.
- For 2000, 5000 and 6000 series storage systems, the maintenance terminal communicates with the storage system properly.
- For 18000 series storage systems, you have recorded the management IP address of the SVP and the communication between the maintenance terminal and the SVP is normal.
- The super administrator can log in to the storage system using the **Local user** authentication mode only.
- To use a Lightweight Directory Access Protocol (LDAP) domain user account to log in to the DeviceManager, you must configure an LDAP server first, then set the LDAP server parameters, and create an LDAP user account on the DeviceManager.

Context

- DeviceManager only supports Transport Layer Security (TSL) protocols (including TLS 1.0, TLS 1.1, and TLS 1.2).
- For 2000 series storage systems, the default IP addresses of the management network ports on controllers A and B are **192.168.128.101** and **192.168.128.102** respectively, and the default subnet mask is **255.255.0.0**.
- For a 2 U controller enclosure (5300 V3 and 5500 V3), the default IP addresses of the management network ports on controllers A and B are **192.168.128.101** and **192.168.128.102** respectively, and the default subnet mask is **255.255.255.0**. For a 3 U or 6 U controller enclosure (5600 V3, 5800 V3 and 6800 V3), the default IP addresses of the management network ports on management modules 0 and 1 are **192.168.128.101** and **192.168.128.102** respectively, and the default subnet mask is **255.255.0.0**.
- The default user name and password of the super administrator are **admin** and **Admin@storage**.
- By default, DeviceManager allows 32 users to log in concurrently.
- This document uses the Windows operating system as an example to explain how to log in to the DeviceManager. The login operations on other operating systems need to be adjusted accordingly.

Procedure

Step 1 Run Internet Explorer on the maintenance terminal.

Step 2 In the address box, type **https://XXX.XXX.XXX.XXX:8088** and press **Enter**.

NOTE

- For 2000, 5000 and 6000 series storage systems, **XXX.XXX.XXX.XXX** represents the management network port IP address of the storage system. For 18000 series storage systems, **XXX.XXX.XXX.XXX** represents the IP address of the SVP management network port.
- In an environment with the firewall function, when the system externally provides web services, you need to enable port 8088.
- Your web browser may display that the website has a security certificate error. If the IP address is correct, you can neglect the prompt and continue to access the storage system.
- If you have a usable security certificate, you are advised to use corresponding commands to import the certificate to improve system security. For details about the corresponding commands, see the *Command Reference* of the corresponding product model.

Step 3 **Optional:** Set the authentication mode and language.

1. Click **Advanced**.
2. From the **Authentication Mode** list, select an authentication mode.
   - Local user: You will log in to the storage system in local authentication mode.

     The super administrator can log in to the storage system using the local user authentication mode only.
   - LDAP user: You will log in to the storage system in LDAP domain authentication mode.

     You can log in to the storage system in LDAP domain authentication mode only after the LDAP server is properly configured.
3. Choose a language from the **Language** list.

   NOTE

   DeviceManager supports two languages: simplified Chinese and English.

Step 4 Type the user name and password in **Username** and **Password**.

NOTE

- In **Verification Code**, enter the correct verification code.
- If **LDAP User** is selected, the user name and password must be a domain user name and password. If you want to log in as the super administrator, the default user name and password are **admin** and **Admin@storage** respectively.
- If an administrator or read-only user forgets the password, ask the super administrator to reset the password. If you forget the user name or password of the super administrator account, contact Huawei technical engineers.
- If you enter incorrect passwords a specified number of times (equal to the value specified in **Number of Incorrect Passwords** on the **Login Policy** page), the account is automatically locked for the period of lock time (The lock period of the super administrator is 15 minutes, and the lock period of other users is 15 minutes by default).
- You must change the default login password immediately when you are logging in to the storage system for the first time and periodically change your login password in the future. This reduces the password leakage risks. To change the password of an administrator or read-only user, go to the command-line interface (CLI), and run **change user user_name=*?* action=reset_password**.

Step 5 Click **Log In**.

The DeviceManager home page is displayed.

Figure 3-2 shows the home page of the DeviceManager.

Figure 3-2 Home page of the DeviceManager

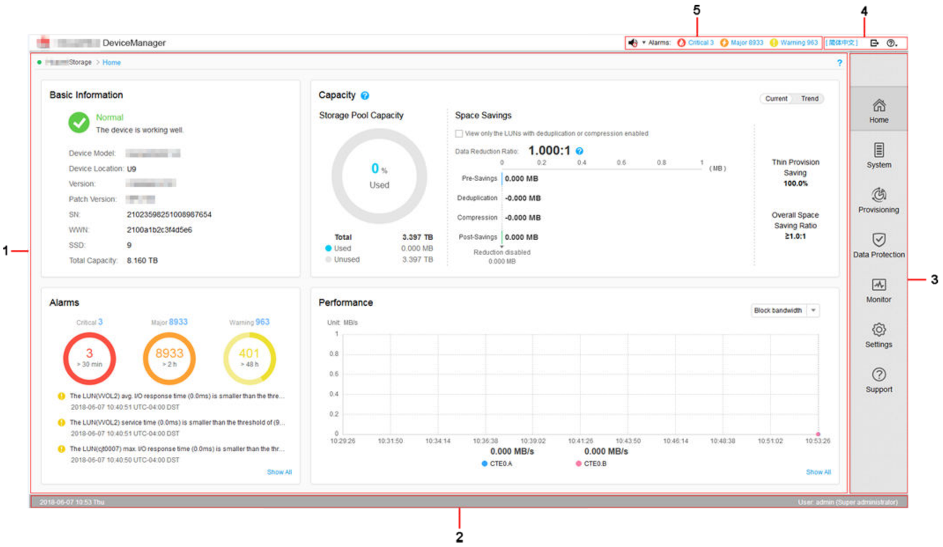


Table 3-3 describes DeviceManager components.

Table 3-3 DeviceManager components

No.	Name	Function
1	Function pane	Shows the basic information, capacity, alarms, and performance of the storage system.
2	Status bar	Shows the name of the currently logged-in user and the system time of the storage system.
3	Navigation tree	Lists all function modules of the storage system.
4	Logout, help, and language area	Shows the logout, help, and language buttons. **NOTE** DeviceManager supports two languages: simplified Chinese and English.
5	Fault statistics pane	Shows different severities of device alarms, which can be checked by users to learn about the running status of the storage system.

----End

Follow-up Procedure

If you need to log out of the DeviceManager, perform the following steps:

1. On the upper-right corner of the DeviceManager, click ⇥.

The **Confirm** dialog box is displayed.

2. Click **OK**. You have logged out of the DeviceManager.

3.3.2 Logging In to the DeviceManager Using a Tablet

Mobile devices such as a tablet can access, manage, and maintain a storage device through a virtual wireless network.

Prerequisites

A Wi-Fi network that is connected to the storage system's management network is available at the customer's site.

Context

- DeviceManager only supports TSL protocols (including TLS 1.0, TLS 1.1, and TLS 1.2).
- Customers can use a tablet to log in to the storage system through their wireless routers. You can use iPad Air (Safari) and HUAWEI MediaPad 10 FHD (Chrome) to log in to the storage system. This section uses iPad as an example to describe how to log in to the DeviceManager. The login operations on other mobile devices are similar.
- For 2000 series storage systems, the default IP addresses of the management network ports on controllers A and B are **192.168.128.101** and **192.168.128.102** respectively, and the default subnet mask is **255.255.0.0**.
- For a 2 U controller enclosure (5300 V3 and 5500 V3), the default IP addresses of the management network ports on controllers A and B are **192.168.128.101** and **192.168.128.102** respectively, and the default subnet mask is **255.255.255.0**. For a 3 U or 6 U controller enclosure (5600 V3, 5800 V and 6800 V3), the default IP addresses of the management network ports on management modules 0 and 1 are **192.168.128.101** and **192.168.128.102** respectively, and the default subnet mask is **255.255.0.0**.
- The default user name and password of the super administrator are **admin** and **Admin@storage**.
- If a user does not perform any operations after logging in to the system for a period longer than the timeout limit (the limit is 30 minutes by default and modifiable), the system logs out automatically.
- If an account is not used to log in to the system for a certain period of time (the period is 60 days by default and modifiable), it will be locked and can only be unlocked by the super administrator.
- By default, DeviceManager allows 32 users to log in concurrently.

Procedure

Step 1 Access a Wi-Fi network.

1. On the desktop of iPad, choose **Settings** > **WLAN**.

   The **WLAN** page is displayed.

2. In the **CHOOSE A NETWORK** area, select the desired Wi-Fi network.

   The **Enter Password** page is displayed.

3. Set **Password** to the password of the Wi-Fi network.

4. Click **Join**.

   The iPad is connected to the Wi-Fi network.

Step 2 Log in to the management software.

1. On the desktop of iPad, click **Safari**.
2. Set **Address** to **https://xxx.xxx.xxx.xxx:8088/deviceManager/ismpad/login.html** and click **Go**.

   The login page of the management software is displayed.

   For 2000, 5000 and 6000 series storage systems, **xxx.xxx.xxx.xxx** indicates the IP address of the management network port on the storage system. For 18000 series storage systems, **xxx.xxx.xxx.xxx** indicates the IP address of the SVP management network port.
3. **Optional:** In **Language**, select a language.

   NOTE

   DeviceManager supports two languages: simplified Chinese and English.
4. Set **User Name** and **Password** to the user name and password for logging in to the management software. Set **Verification Code** to a four-digit verification code.

   NOTE

   – The default user name and password are **admin** and **Admin@storage** respectively.

   – You are advised to change the default login password immediately after you have logged in to the storage system for the first time. In addition, periodically change your login password to reduce password leakage risks. For details about how to change a password, see the *Administrator Guide* of the corresponding product model.
5. Click **Login**.

   The home page of the management software is displayed.

----End

3.3.3 Logging In to the DeviceManager Through SVP (18000 Series)

To log in to the DeviceManager, you can use the keyboard, video, and mouse (KVM) on system bay 0 to operate the SVP, or visit the SVP using the Remote Desktop Protocol (RDP) on a maintenance terminal connected to the service processor (SVP).

Prerequisites

- The communication between the maintenance terminal and the SVP is normal.
- Before logging in to the DeviceManager as a Lightweight Directory Access Protocol (LDAP) domain user, first configure the LDAP domain server, and then configure LDAP server parameters on the storage device accordingly, at last create an LDAP user.
- The initial user name and password for logging in to the DeviceManager are **admin** and **Admin@storage** respectively.

Context

This document exemplifies how to log in to the DeviceManager in Windows using Mozilla Firefox. For other operating systems, revise the login procedure accordingly.

Procedure

Step 1 Log in to the SVP server.

- If you use the KVM to operate the SVP, complete the following steps to log in to the SVP.

  a. Log in to the SVP host as user **svp_user**. The default password is **Aguser@12#$**.

  b. On the host desktop, choose **Applications** > **System** > **Terminal** > **Xterm**.

  c. In the command window that is displayed, run **vncviewer -fullscreen 127.0.0.1:1**. Go to the login page of the Windows operating system built in the SVP.

- If you visit the SVP on a maintenance terminal using the RDP, complete the following steps to log in to the SVP.

  NOTE

  SVP's remote desktop function requires network-level identity verification. Therefore, you must use operating systems and remote desktop clients that support network-level identity verification to connect to SVP. Windows XP and Windows Server 2003 of certain versions do not support this function. You are recommended to adopt Windows 7 or a later version, together with a built-in remote desktop client.

  a. Choose **Start** > **All Programs** > **Accessories** > **Remote Desktop Connection**. The **Remote Desktop Connection** dialog box is displayed.

  b. Type the IP address of the management network port in the **Computer** text box and press **Enter** (the default IP address is **192.168.0.136**).

  c. Type the correct user name and password to log in.

  The initial user name and password for logging in to the SVP are **maintainer** and **Maintainer@svp** respectively.

NOTE

For storage system security, you need to modify the password of the **maintainer** account upon your first login.

Step 2 On the desktop, double-click ⚙.

NOTE

- Your web browser may display that the website has a security certificate error. If the IP address is correct, you can neglect the prompt and continue to access the storage system.
- If you have a usable security certificate, you are advised to use corresponding commands to import the certificate to improve system security. For details about the corresponding commands, see the *Command Reference* of the corresponding product model.

The DeviceManager login page is displayed.

Step 3 **Optional:** Choose an authentication mode and language.

1. Click **Advanced**.
2. Select an authentication mode from the **Authentication mode** list.

   – **Local user**: Logs in to the storage system using local authentication.

   NOTE

   The **admin** user can log in to the storage system only in **Local user** authentication mode.

   – **LDAP user**: Logs in to the storage system using LDAP domain authentication.

3. Choose a language from the **Language** list.

   NOTE

   DeviceManager supports two languages: simplified Chinese and English.

Step 4 Type your user name and password in **Username** and **Password** respectively.

NOTE

- In **Verification Code**, enter the correct verification code.
- If you log in to the storage system in **LDAP user** authentication mode, enter your LDAP user name and password. If you want to log in as the super administrator, the default user name and password are **admin** and **Admin@storage** respectively.
- If the administrator or read-only user forgets the password, ask the super administrator to reset the password. If you forget the user name or password of the super administrator account, contact Huawei technical engineers.
- If you enter incorrect passwords a specified number of times (equal to the value specified in **wrong times** on the **Password Policy Management** page), the account is automatically locked for the period of time specified in **Lock Time**.
- You must change the default login password immediately when you are logging in to the storage system for the first time and periodically change your login password in the future. This reduces the password leakage risks. For details about how to change the password, see the *Administrator Guide* of the corresponding product model.

Step 5 Click **Log In**.

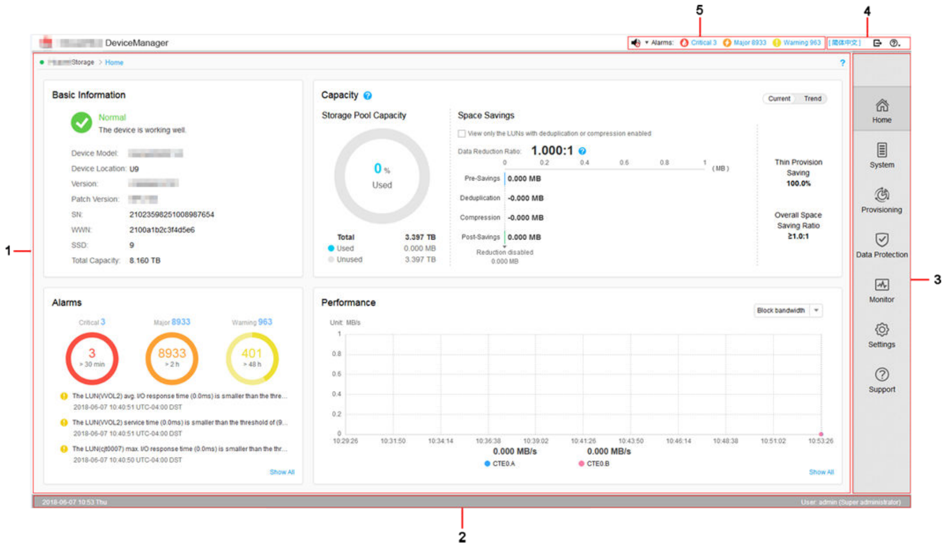
NOTE

- To log out of the DeviceManager, click ⇥ in the upper right corner.
- To view online help, click ⓘ in the upper right corner. The online help provides details about each step and operation.

The DeviceManager main window is displayed.

Figure 3-3 shows the main window of the DeviceManager.

Figure 3-3 Main window of the DeviceManager



Basic Information

Normal
The device is working well.

Device Model: [redacted]
Device Location: U9
Version: [redacted]
Patch Version: [redacted]
SN: 21023598251008987654
WWN: 2100a1b2c3f4d5e6
SSD: 9
Total Capacity: 8.160 TB

Capacity

Storage Pool Capacity: 0 % Used
Total 3.397 TB
Used 0.000 MB
Unused 3.397 TB

Space Savings
□ View only the LUNs with deduplication or compression enabled
Data Reduction Ratio: 1.000:1
Pre-Savings 0.000 MB
Deduplication -0.000 MB
Compression -0.000 MB
Post-Savings 0.000 MB
Reduction disabled 0.000 MB
Thin Provision Saving 100.0%
Overall Space Saving Ratio ≥1.0:1

Alarms
Critical 3 — 3 > 30 min
Major 8933 — 8933 > 2 h
Warning 963 — 401 > 48 h

The LUN(VVOL2) avg. I/O response time (0.0ms) is smaller than the thre...
2018-06-07 10:40:51 UTC-04:00 DST
The LUN(VVOL2) service time (0.0ms) is smaller than the threshold of (9...
2018-06-07 10:40:51 UTC-04:00 DST
The LUN(cjt0007) max. I/O response time (0.0ms) is smaller than the thr...
2018-06-07 10:40:50 UTC-04:00 DST

Performance
Block bandwidth
0.000 MB/s CTE0.A
0.000 MB/s CTE0.B

2018-06-07 10:53 Thu
User: admin (Super administrator)

Table 3-4 describes DeviceManager components.

Table 3-4 DeviceManager components

No.	Name	Function
1	Function pane	Shows the basic information, capacity, alarms, and performance of a storage system.
2	Status bar	Shows the name of the currently logged-in user and the system time of the storage device.
3	Navigation tree	Lists all function modules of a storage system.
4	Log out, help, and language area	Shows the log out, help, and language buttons. **NOTE** DeviceManager supports two languages: simplified Chinese and English.
5	Fault statistics pane	Shows different severities of device alarms, which can be checked by users to learn about the running status of the storage device.

----End

3.3.4 Logging In to the DeviceManager Through Management Network Port (18000 Series)

To log in to the DeviceManager management page, open a web browser on a maintenance terminal connected to the storage system, and type the IP address of the management network port of the storage system in the address box.

Prerequisites

- Operating system and browser versions.

  DeviceManager supports multiple operating systems and browsers. You can query the compatibility using the **OceanStor Interoperability Navigator**.
- The IP address of the management port of the storage system has been configured.
- The maintenance terminal communicates with the storage system properly.
- Before logging in to the DeviceManager as a Lightweight Directory Access Protocol (LDAP) domain user, first configure the LDAP domain server, and then configure LDAP server parameters on the storage device accordingly, at last create an LDAP user.
- The initial user name and password for logging in to the DeviceManager are **admin** and **Admin@storage** respectively.

Context

- DeviceManager only supports TSL protocols (including TLS 1.0, TLS 1.1, and TLS 1.2).

- The default IP addresses of the management network ports on management modules 0 and 1 are respectively **192.168.128.101** and **192.168.128.102**, and the default subnet mask is **255.255.0.0**.
- By default, DeviceManager allows 32 users to log in concurrently.
- This document exemplifies how to log in to the DeviceManager in Windows using Mozilla Firefox. For other operating systems, revise the login procedure accordingly.

When logging in to DeviceManager on the maintenance terminal through the management port of the storage system, you can obtain different operational permissions based on the SVP status.

- When the SVP runs normally, the system redirects to the DeviceManager of SVP. You can query, configure, and manage storage services on DeviceManager, as well as query and manage the services on SVP.
- When the SVP encounters an exception (for example, SVP is not connected to the customer's network, becomes faulty, or cannot communicate with the storage system), you can query, configure, and manage storage services. However, you cannot restart the storage system, dump performance files to SVP, or query and manage SVP services.

Procedure

Step 1 Open Mozilla Firefox on the maintenance terminal.

Step 2 In the address box, type **https://XXX.XXX.XXX.XXX:8088** and press **Enter**.

The DeviceManager login page is displayed.

NOTE

- *XXX.XXX.XXX.XXX* represents the IP address of the storage system management network port.
- A message indicating that your website has a security certificate error may be displayed on your browser. If the IP address is correct, you can neglect the prompt and continue to access the storage system.
- If you have a usable security certificate, you are advised to use corresponding commands to import the certificate to improve system security. For details about the corresponding commands, see the *Command Reference* of the corresponding product model.

Step 3 **Optional:** Choose an authentication mode and language.

1. Click **Advanced**.
2. Select an authentication mode from the **Authentication mode** list.
   - **Local user**: Logs in to the storage system using local authentication.

     NOTE

     The **admin** user can log in to the storage system only in **Local user** authentication mode.
   - **LDAP user**: Logs in to the storage system using LDAP domain authentication.
3. Choose a language from the **Language** list.

   NOTE

   DeviceManager supports two languages: simplified Chinese and English.

Step 4 Type your user name and password in **Username** and **Password** respectively.

NOTE

- In **Verification Code**, enter the correct verification code.
- If you log in to the storage system in **LDAP user** authentication mode, enter your LDAP user name and password. If you want to log in as the super administrator, the default user name and password are **admin** and **Admin@storage** respectively.
- If the administrator or read-only user forgets the password, ask the super administrator to reset the password. If you forget the user name or password of the super administrator account, contact Huawei technical engineers.
- If you enter incorrect passwords a specified number of times (equal to the value specified in **wrong times** on the **Password Policy Management** page), the account is automatically locked for the period of time specified in **Lock Time**.
- You must change the default login password immediately when you are logging in to the storage system for the first time and periodically change your login password in the future. This reduces the password leakage risks. For details about how to change the password, see the *Administrator Guide* of the corresponding product model.

Step 5 Click **Log In**.

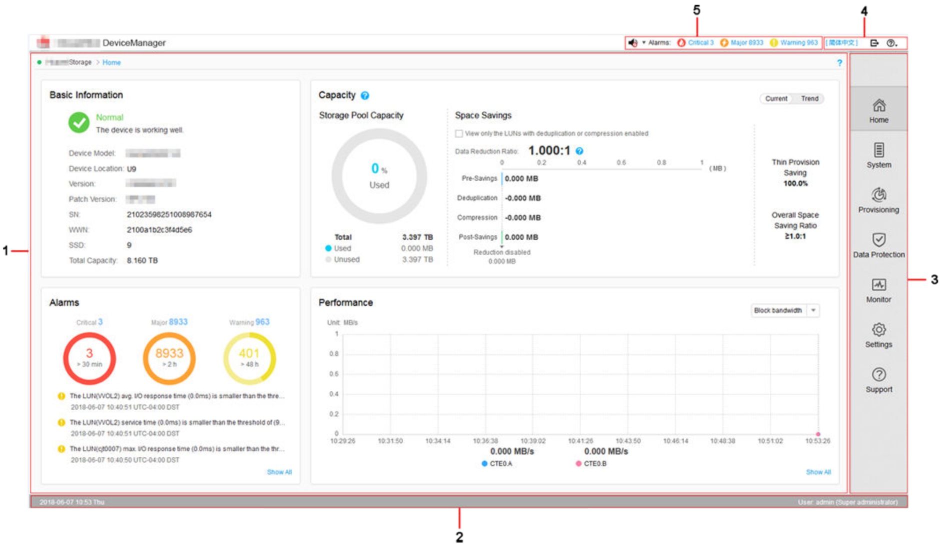
NOTE

- To log out of the DeviceManager, click ⇨ in the upper right corner.
- To view online help, click ⓘ in the upper right corner. The online help provides details about each step and operation.

The DeviceManager main window is displayed.

Figure 3-4 shows the main window of the DeviceManager.

Figure 3-4 Main window of the DeviceManager



[redacted] DeviceManager

[redacted]Storage > Home

Basic Information

Normal
The device is working well.

Device Model: [redacted]
Device Location: U9
Version: [redacted]
Patch Version: [redacted]
SN: 21023598251008987654
WWN: 2100a1b2c3f4d5e6
SSD: 9
Total Capacity: 8.160 TB

Capacity

Storage Pool Capacity
0 % Used
Total 3.397 TB
Used 0.000 MB
Unused 3.397 TB

Space Savings
☐ View only the LUNs with deduplication or compression enabled
Data Reduction Ratio: 1.000:1
Pre-Savings 0.000 MB
Deduplication -0.000 MB
Compression -0.000 MB
Post-Savings 0.000 MB
Reduction disabled 0.000 MB
Thin Provision Saving 100.0%
Overall Space Saving Ratio ≥1.0:1

Alarms
Critical 3 Major 8933 Warning 963

The LUN(VVOL2) avg. I/O response time (0.0ms) is smaller than the thre...
2018-06-07 10:40:51 UTC-04:00 DST

The LUN(VVOL2) service time (0.0ms) is smaller than the threshold of (9...
2018-06-07 10:40:51 UTC-04:00 DST

The LUN(cjt0007) max. I/O response time (0.0ms) is smaller than the thr...
2018-06-07 10:40:50 UTC-04:00 DST

Performance
Block bandwidth
CTE0.A 0.000 MB/s
CTE0.B 0.000 MB/s

2018-06-07 10:53 Thu
User: admin (Super administrator)

Table 3-5 describes DeviceManager components.

Table 3-5 DeviceManager components

No.	Name	Function
1	Function pane	Shows the basic information, capacity, alarms, and performance of a storage system.
2	Status bar	Shows the name of the currently logged-in user and the system time of the storage device.
3	Navigation tree	Lists all function modules of a storage system.
4	Log out, help, and language area	Shows the log out, help, and language buttons. **NOTE** DeviceManager supports two languages: simplified Chinese and English.
5	Fault statistics pane	Shows different severities of device alarms, which can be checked by users to learn about the running status of the storage device.

----End

3.4 Creating a Disk Domain

The types of disks in a disk domain decide which storage tiers can be created. The first step for creating a storage pool is to create a disk domain and specify the types and number of member disks.

Context

When creating a disk domain, you can select self-encrypting disks to encrypt the disk domain. Encrypted disks are not sold in mainland China.

You are advised to use different disk domains to create storage pools for the block storage service and file storage service.

For 2000, 5000, 6000, 18000 series storage systems, a disk domain consists of the same storage media or different storage media of disks. Disks of the same storage media form a storage tier. The system supports the following storage tiers:

- The high-performance tier consists of SSDs and provides the highest performance. As the SSD storage media have a high cost and low capacity, this tier is suitable for storing frequently accessed data.
- The performance tier consists of SAS disks and provides modest performance. As SAS storage media have a modest cost and large capacity, this tier is suitable for storing infrequently accessed data.
- The capacity tier consists of NL-SAS disks and provides the lowest performance. As NL-SAS storage media have the lowest cost and largest capacity, the capacity tier is suitable for storing a large amount of seldom accessed data.

To prevent data loss or performance deterioration caused by a member disk failure, the storage system employs hot spare space to take over data from the failed member disk. The supported hot spare policies are as follows:

- - High

    The capacity of one disk is used as hot spare space if the number of disks at a storage tier equals to or fewer than 12. The hot spare space non-linearly increases as the number of disks increases. When the number of disks at a storage tier reaches 175, the storage tier uses the capacity of one disk in every 100 disks as the hot spare space.

  - Low

    The capacity of one disk is used as hot spare space if the number of disks at a storage tier equals to or fewer than 25. The hot spare space non-linearly increases as the number of disks increases. When the number of disks at a storage tier reaches 175, the storage tier uses the capacity of one disk in every 200 disks as the hot spare space.

  - None (not supported by 18000, 18000F series storage systems)

    The system does not provide hot spare space.

Table 3-6 describes how hot spare space changes with the number of disks. The hot spare space changes at a storage tier are used as an example here. The hot spare space changes at different types of storage tiers are the same.

Table 3-6 Changes of hot spare space

Number of Disks	Number of Disks of Which Capacity Is Used as Hot Spare Space in High Hot Spare Policy[a]	Number of Disks of Which Capacity Is Used as Hot Spare Space in Low Hot Spare Policy[a]
(1, 12]	1	1
(12, 25]	2	
(25, 50]	3	2
(50, 75]	4	
(75, 125]	5	3
(125, 175]	6	
(175, 275]	7	4
(275, 375]	8	
...		

Number of Disks	Number of Disks of Which Capacity Is Used as Hot Spare Space in High Hot Spare Policy[a]	Number of Disks of Which Capacity Is Used as Hot Spare Space in Low Hot Spare Policy[a]
a: Huawei storage systems use RAID 2.0+ virtualization technology. Hot spare capacity is provided by member disks in each disk domain. Therefore, the hot spare capacity is expressed in number of disks in this table. For example, if a disk domain is composed of 12 SSDs and the high hot spare policy is used, the hot spare space occupies the capacity of one SSD and the capacity is provided by member disks in the disk domain. If a disk domain is composed of 13 SSDs and the high hot spare policy is used, the hot spare space occupies the capacity of two SSDs.		

NOTE

- For 18000 and 18000F series storage systems, the high hot spare policy is used by default. You can only run the **change disk_domain general** command on the CLI to modify the hot spare policy.
- When you are creating a disk domain, ensure that the disks used to provide hot spare space are sufficient.
- Hot spare space can be used for the current disk domain only.
- **Table 3-6** lists common capacity changes of the hot spare space. The number of disks supported by a storage system and the capacity of their hot spare space are based on actual specifications.

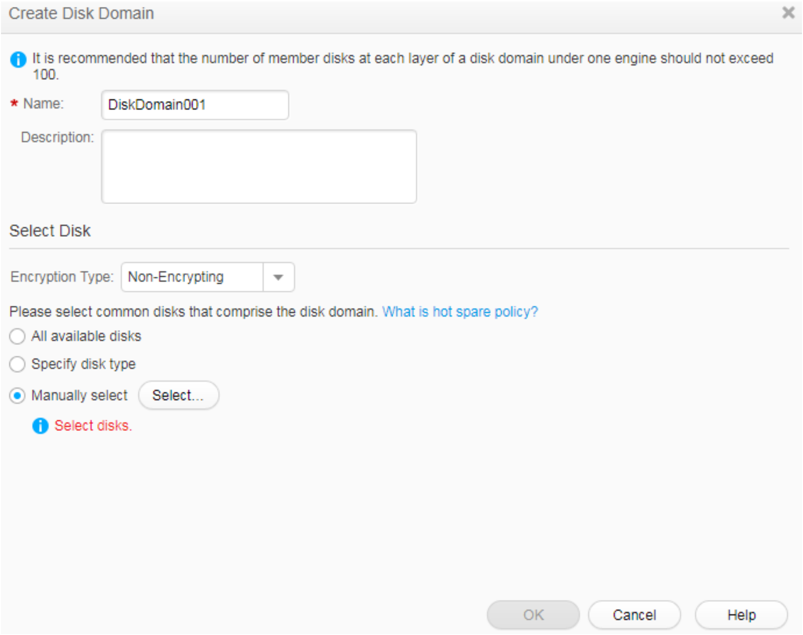
Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Provisioning** > **Disk Domain**.

Step 3 Click **Create**.

The **Create Disk Domain** dialog box is displayed.



Create Disk Domain

It is recommended that the number of member disks at each layer of a disk domain under one engine should not exceed 100.

* Name: DiskDomain001

Description:

Select Disk

Encryption Type: Non-Encrypting

Please select common disks that comprise the disk domain. What is hot spare policy?

○ All available disks

○ Specify disk type

● Manually select Select...

Select disks.

Step 4 Name and describe the disk domain.

1. In **Name**, enter a name for the disk domain.

   NOTE

   – The name must be unique.

   – The name can contain only letters, digits, periods (.), underscores (_), and hyphens (-).

   – The value contains 1 to 31 characters.

2. In **Description**, enter the function and properties of the disk domain. The descriptive information helps identify the disk domain.

Step 5 In **Encryption Type**, select a type to determine whether the disk domain is created by using self-encrypting disks.

Encryption types include:

- **Non-Encrypting Disk**: create an unencrypted disk domain.
- **Self-Encrypting Disk**: create an encrypted disk domain.

NOTE

- **Non-Encrypting Disk**: Non-encrypting disks are common disks that do not support the encryption function.
- **Self-Encrypting Disk**: When data is written into or read from a disk, the data is encrypted or decrypted using the hardware circuit and internal encryption key of the disk. The self-encrypting disk is a special type of disk. Before using self-encrypting disks, install and configure key management servers, and complete their interconnections with the storage system. For details, see *OceanStor V3 Series V300R006 Disk Encryption User Guide*.
- Encrypted disks are not supported by 2000F, 5000F, 6000F, 18000F series storage systems.
- Self-encrypting and non-encrypting disks cannot exist in the same disk domain.

Step 6 Select the disks that comprise the disk domain. There are three ways to select the disks:

- Select **All available disks**.

  You only need to configure the hot spare policy for the storage tier.

NOTE

It is recommended that you create a disk domain by **Manually select** disks, ensure that all disks are from the same engine, so that disk domain on one engine reduces the disk failure probability and improve the read and write performance of disks.

- Select **Specify disk type** or **Specify the number of disks**.
  - Select **Specify disk type** (2000, 5000, 6000, 18000 series storage systems).
    1. Select the storage tier according to the storage media of disks.
    2. Configure the number of disks for each storage tier.
    3. Configure the hot spare policy for each storage tier.

       NOTE

       For 18000 series storage systems, the high hot spare policy is used by default. You can only run the **change disk_domain general** command on the CLI to modify the hot spare policy.
  - Select **Specify the number of disks** (2000F, 5000F, 6000F, 18000F series storage systems).

    The number of disks composing the storage tier will be configured.
- Select **Manually select**.
  1. Click **Select**.
  2. In the **Select Disk** dialog box, select the disks you need and click >.
  3. Click **OK** to finish selecting disks.
  4. Configure the hot spare policy for each storage tier.

NOTE

If you plan to create a RAID 10 storage pool in the disk domain that you are creating, you are advised to manually select an even number of disks owned by each engine for each storage tier in the disk domain to ensure the reliability of RAID 10.

The storage system provides hot spare space by configuring hot space policies, so that the hot spare space can take over data from failed member disks.

You are advised to configure a maximum of 100 disks for each tier in a disk domain. For example, if the number of disks on a tier is D (divide D by 100 and then round off the result to N and the remainder is M), you can refer to the following configurations:

- If D ≤ 100, configure all disks on this tier in one disk domain.
- If D > 100, create N+1 disk domains and evenly distribute all disks to the N+1 disk domains. That is, the number of disks in each disk domain is D/(N+1).
- For SmartTier, it is recommended that a maximum of 100 disks be configured for each tier in a disk domain. The configuration of disks on each tier is the same as the preceding principle.

Example 1: The total number of SSDs in the storage system is 328, which is the value of D. (Divide 328 by 100. Round off the result to 3, which is the value of N. The remainder is 28, which is the value of M). You are advised to configure four disk domains, each of which contains 328/4 = 82 SSDs.

Example 2: If the total number of SSDs in the storage system is 223, which is the value of D. (Divide 223 by 100. Round off the result to 2, which is the value of N. The remainder is 23, which is the value of M). You are advised to configure three disk domains, each of which contains 223/3 = 74.3 disks. In this case, two disk domains are configured with 74 disks respectively and the other disk domain is configured with 75 disks.

Example 3: If a disk domain consists of SSDs, SAS disks, and NL-SAS disks, for SmartTier, the number of disks of each type cannot exceed 100.

If the project requires a disk domain containing over 100 disks to meet capacity and service planning requirements, contact Huawei technical engineers to evaluate.

Step 7 Click **OK**.

A message is displayed, indicating that the operation succeeded.

Step 8 Click **OK**. The disk domain has been created. To view basic information about disks in the current disk domain, click the **Disk** tab in the information display area below. To view the engine to which a disk belongs, click ︾.

----End

3.5 Creating a Storage Pool

Create storage pools for application servers to use the storage space provided by a storage system.

Prerequisites

A disk domain is created.

Context

- You are advised to use different disk domains to create storage pools for the block storage service and file storage service.
- For 2000, 5000, 6000, 18000 series storage systems, a storage pool is a logical combination of one or multiple storage tiers in a disk domain. Different storage tiers may have different RAID policies.
- A RAID policy includes a RAID level and the number of disk blocks and parity blocksof this RAID level.
- The RAID level is classified into typical configuration and flexible configuration based on the number of data blocks and parity blocks. The detailed configuration is shown in **Table 3-7**.

Table 3-7 RAID level configuration

RAID Level	Typical Configuration	Flexible Configuration
RAID 0	-	-
RAID 1	● 2D[a] ● 4D	-
RAID 10	-	-
RAID 3	● 2D+1P[b] ● 4D+1P ● 8D+1P	2D+1P to 13D+1P
RAID 5	● 2D+1P ● 4D+1P ● 8D+1P	2D+1P to 13D+1P

RAID Level	Typical Configuration	Flexible Configuration
RAID 50	● (2D+1P)x2 ● (4D+1P)x2 ● (8D+1P)x2	-
RAID 6	● 2D+2P ● 4D+2P ● 8D+2P ● 16D+2P	2D+2P to 26D+2P

a: **D** indicates the data block.

b: **P** indicates the parity block.

NOTE

For 2000, 5000, 6000, 18000 series storage systems, if the RAID level of one storage tier is configured with flexible configuration first, this tier is the primary control tier that controls other tiers' RAID policies. The number of RAID data disks of the primary control tier and the number of RAID data disks of other tiers must be a multiple of 1, 2, 4, or 8. For example, if the performance tier is the primary control tier and its RAID policy is 3D+1P, the RAID policy of other tiers must be 3D+1P, 6D+2P, or so on, and cannot be 4D+1P. If you want to change the current primary control tier, deselect this tier and select it again.

- For 2000, 5000, 6000, 18000 series storage systems, the following describes the storage tiers in a storage pool:
  - The high performance tier, providing the highest performance, consists of SSDs. As SSD storage media have a high cost and low capacity, this tier is applicable to the applications such as database indexes that require a high random read/write performance.
  - The performance tier, providing modest performance, consists of SAS disks. As SAS storage media have a modest cost and large capacity, this tier provides high reliability, suitable for online applications.
  - The capacity tier, providing the lowest performance, consists of NL-SAS disks. As NL-SAS storage media have the lowest cost and largest capacity, the capacity tier is suitable for non-critical services such as data backup.

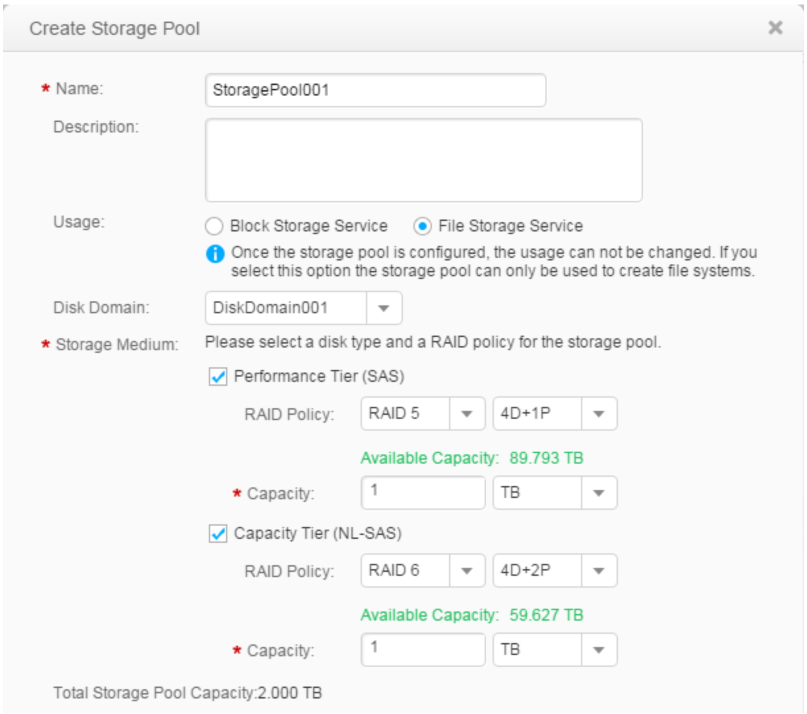
Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Provisioning** > **Storage Pool**.

Step 3 Click **Create**.

The **Create Storage Pool** dialog box is displayed.



Create Storage Pool

* Name: StoragePool001

Description:

Usage: ○ Block Storage Service ● File Storage Service

Once the storage pool is configured, the usage can not be changed. If you select this option the storage pool can only be used to create file systems.

Disk Domain: DiskDomain001

* Storage Medium: Please select a disk type and a RAID policy for the storage pool.

☑ Performance Tier (SAS)

RAID Policy: RAID 5 4D+1P

Available Capacity: 89.793 TB

* Capacity: 1 TB

☑ Capacity Tier (NL-SAS)

RAID Policy: RAID 6 4D+2P

Available Capacity: 59.627 TB

* Capacity: 1 TB

Total Storage Pool Capacity:2.000 TB

Step 4 Enter a name and description for the storage pool.

1. In the **Name** text box, enter a name for the storage pool.

   NOTE

   – The name must be unique.

   – The name can contain only letters, digits, periods (.), underscores (_), and hyphens (-).

   – The value contains 1 to 31 characters.

2. In the **Description** text box, enter the function and properties of the storage pool. The descriptive information helps identify the storage pool.

Step 5 In the **Usage** text box, select **File Storage Service**.

NOTE

Usage is unchangeable after it is configured.

- A storage pool whose **Usage** is **Block Storage Service** allows you to create LUNs only.
- A storage pool whose **Usage** is **File Storage Service** allows you to create file systems only.

Step 6 In **Disk Domain**, select the disk domain that the storage pool belongs to.

Step 7 In **Storage Medium**, select the storage tiers needed for the storage pool and set related parameters.

1. Select storage tiers that meet service requirements.
2. Set basic properties for the storage tiers. **Table 3-8** describes related parameters.

Table 3-8 Storage tier parameters

Parameter	Description	Setting
RAID Policy	RAID level. The system supports RAID 0, RAID 1, RAID 10, RAID 3, RAID 5, RAID 50, and RAID 6. **NOTE** RAID 0 only supports configuration in CLI mode. For details, see the *Command Reference* of the corresponding product model.	Select a RAID policy based on the planned solution. The default RAID policy of a storage tier varies with the number of disks allocated to the storage tier. – If the number of disks allocated to a storage tier is smaller than 10: ■ Default RAID policy of the high performance tier: RAID 10 ■ Default RAID policy of the performance tier: RAID 5 (4D+1P) ■ Default RAID policy of the capacity tier: RAID 6 (4D+2P) – If the number of disks allocated to a storage tier is equal to 10: ■ Default RAID policy of the high performance tier: RAID 10 ■ Default RAID policy of the performance tier: RAID 5 (8D+1P) ■ Default RAID policy of the capacity tier: RAID 6 (4D+2P) – If the number of disks allocated to a storage tier is greater than 10: ■ Default RAID policy of the high performance tier: RAID 10

Parameter	Description	Setting
		■ Default RAID policy of the performance tier: RAID 5 (8D+1P) ■ Default RAID policy of the capacity tier: RAID 6 (8D+2P) **NOTE** If the number of SSDs in a disk domain is two or three, you are advised to configure the corresponding high-performance tier to RAID 1 (2D).
Capacity	The capacity that the storage tier provides for the storage pool. Three capacity levels are provided: TB, GB, and PB. **NOTE** Select **Use all available capacity**, and then you can allocate all available capacity in this storage layer to the new storage pool.	The capacity must be not larger than the available capacity of the storage tier.

NOTE

You are advised to create RAID 6 groups on the capacity tier to ensure data security.

Step 8 Set properties of the storage pool according to the usage types.

1. Click **Advanced** to set advanced properties for the storage pool.

   Table 3-9 describes the related parameters.

Table 3-9 Storage pool advanced parameters

Parameter	Description	Setting
Used Capacity Alarm Threshold (%)	When the percentage of the used capacity of the storage pool to the total capacity of the storage pool (the used capacity for short) reaches the used capacity alarm threshold, the system generates an alarm. The alarm is generated in 3 circumstances: – When the used capacity reaches the used capacity alarm threshold, the system generates an alarm informing that the capacity of storage pool is insufficient. – When the used capacity alarm threshold is not greater than 88 and the used capacity reaches 90%, the system generates an alarm informing that the storage pool is running out. – When the used capacity alarm threshold is not greater than 88 and the used capacity reaches (used capacity alarm threshold +2)%, the system generates an alarm informing that the storage pool is running out. **NOTE** If the used capacity alarm threshold is set to 85 and the used capacity reaches 85%, the system generates an alarm informing that the capacity of storage pool is insufficient, and when the used capacity reaches 90%, the system generates an alarm informing that the storage pool is running out. If the used capacity alarm threshold is set as 91, when the used capacity reaches 93%, the system generates an alarm informing that the storage pool is running out. A proper used capacity alarm threshold helps you monitor the capacity usage of a storage pool.	[Value range] 1 to 95 [Default value] 80
Data Migration Granularity	A logical storage space with a fixed size divided from a CKG. It is the smallest unit (granularity) for data migration and hotspot data statistics collection. It is also the smallest unit for space application and release in a storage pool. The default value **4 MB** is recommended. The value cannot be changed after being set. **NOTE** You can configure this parameter only when RAID levels of storage tiers are of typical configuration.	[Value range] 512 KB to 64 MB [Default value] 4 MB

Parameter	Description	Setting
Stripe Depth	Stripe refers to that continuous data is divided into data blocks of the same size and data blocks are distributed on different disks of storage devices. In this way, I/O loads are balanced among disks, improving read/write performance. Stripe depth refers to stripe size, indicating the size of data blocks on each disk. Smaller stripe size indicates smaller data blocks. These data blocks are distributed on more disks, improving transmission performance. However, more time is required to find different data blocks, decreasing disk locating performance. On the contrary, fewer data blocks indicate lower transmission performance but higher disk locating performance. The value of this parameter can be: – System auto select The system selects the optimal stripe depth based on the RAID policy of the storage tier and data migration granularity. – 32 KB – 64 KB – 128 KB 128 KB is recommended for random read/write services (such as in database scenarios). – 256 KB – 512 KB 512 KB is recommended for sequential read/write services (such as media asset scenarios) **NOTE** The parameter value cannot be changed after being determined.	[Default value] System auto select

2. Click **OK**.

Step 9 In the **Create Storage Pool** dialog box, Click **OK**.

The **Execution Result** dialog box is displayed indicating that the operation succeeded.

Step 10 Click **Close**.

----End

3.6 Creating a File System

This section explains how to create file systems. File systems can share storage resources in the form of directories.

Prerequisites

- A storage pool is created and is used for file storage service.
- Only administrators and super administrators are allowed to create file systems.
- After enabling the file system function of a mirror domain, you can run the **show mirror_domain general [mirror_domain_id=?]** command to query the mirror domain information about a storage system. To obtain the mirror domain ID, run the **show mirror_domain general** command without parameters. To enable or disable the file system function of a mirror domain, run the **change mirror_domain general mirror_domain_id=? nas_switch=?** command. For details, see the *Command Reference* of the corresponding product model.

Context

Mirror domain: the storage engine that is responsible for access to and storage structure of data and indexes, storage space management, cache management, lock mechanism, and transaction mechanism at the storage layer.

Precautions

If a storage pool has thin file systems and the capacity of all file systems exceeds that of the storage pool, services may be interrupted if the capacity of the storage pool is used up.

Procedure

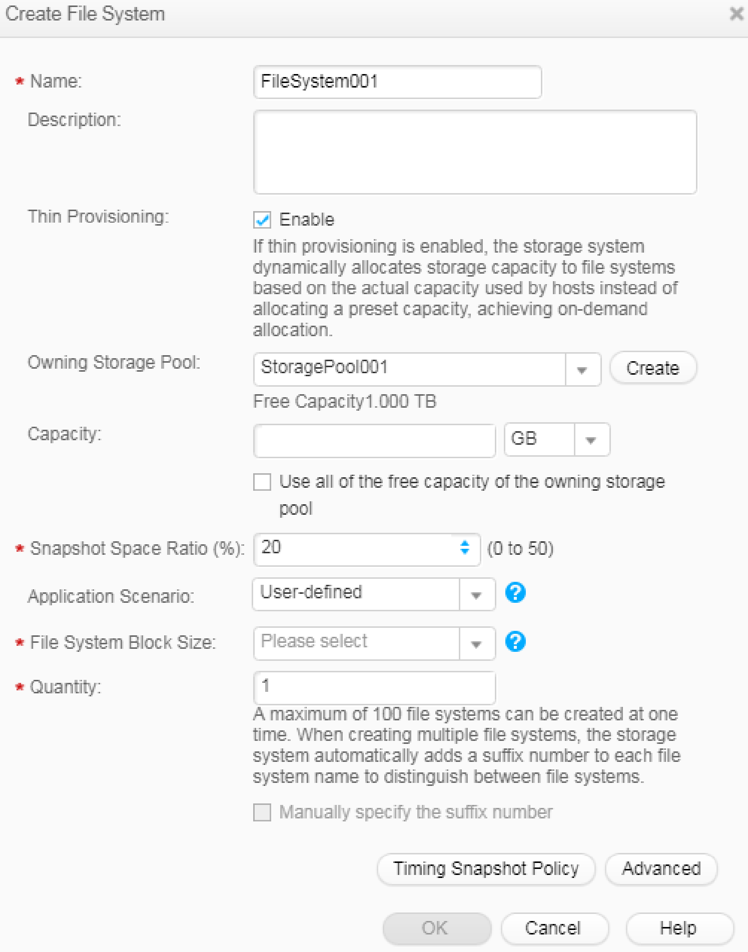
Step 1 Log in to DeviceManager.

Step 2 Choose **Provisioning** > **File System**.

Step 3 Click **Create**.

The **Create File System** dialog box is displayed.

Step 4 Create a file system. **Table 3-10** describes related file system parameters.



Create File System

* Name: FileSystem001

Description:

Thin Provisioning: ☑ Enable

If thin provisioning is enabled, the storage system dynamically allocates storage capacity to file systems based on the actual capacity used by hosts instead of allocating a preset capacity, achieving on-demand allocation.

Owning Storage Pool: StoragePool001 ▾ Create

Free Capacity1.000 TB

Capacity: GB ▾

□ Use all of the free capacity of the owning storage pool

* Snapshot Space Ratio (%): 20 (0 to 50)

Application Scenario: User-defined ▾

* File System Block Size: Please select ▾

* Quantity: 1

A maximum of 100 file systems can be created at one time. When creating multiple file systems, the storage system automatically adds a suffix number to each file system name to distinguish between file systems.

□ Manually specify the suffix number

Table 3-10 File system parameters

Parameter	Description	Value
Name	Name of the file system.	[Value range] ● The name must be unique. ● For V300R006C00 and V300R006C10, the name can only contain letters, digits, and underscores (_). ● The name can be 1 to 255 characters in length. [Example] filesystem001
Description	Description of the file system.	[Example] -

Parameter	Description	Value
Thin Provisioning	Determine whether the thin provisioning function is enabled so that you can create thin file systems. **NOTE** After the function is enabled, the storage system does not allocate the configured capacity to the file system at a time. Within configured capacity, the storage system allocates the storage resource to the file system on demand, based on the actual capacity used by the host.	[Example] Enable
Owning Storage Pool	Storage pool to which the file system you are creating belongs. **NOTE** ● You can only choose the storage pool which is used for **File Storage Service**. ● If the storage system has no storage pool, click **Create** to create one.	[Example] storagepool002
Capacity	File system capacity. ● When the Thin function is enabled, the capacity is the maximum capacity allocated to the thin file system. That is, the total capacity dynamically allocated to the file system cannot exceed the maximum capacity. ● When the Thin function is disabled, the capacity will be allocated to a thick file system once and for all. ● The system support creating block-level file system. Select capacity unit Blocks when creating a file system. One Block = 512 Bytes.	[Value range] ● The maximum capacity for creating a thick file system does not exceed the available capacity of the storage pool where the thick file system resides. ● The maximum capacity for creating a file system can exceed the available capacity of the storage pool where the thin file system resides but cannot exceed 1 GB to 16384 TB. ● The system support creating block-level file system. Select capacity unit **Blocks** when creating a file system. One Block = 512 Bytes. [Example] 3 GB

Parameter	Description	Value
Use all the free capacity of the owning storage pool	If this option is selected, all free space of the owning storage pool is allocated to this file system. **NOTE** If a thin file system exists in a storage pool, services of the thin file system may fail after all free capacity of the storage pool is used to create a thick file system.	[Example] Disable
Snapshot Space Ratio (%)	Percentage of the file system snapshot space to the file system space.	[Value range] The value is an integer ranging from 0 to 50. [Example] 20 [Default] 20

Parameter	Description	Value
Application Scenario	Application scenarios of file systems. ● VM: File systems apply to VMs. After this scenario is selected, the system will set the block size of file systems to 8 KB, and automatically adjust system resources to adapt to this scenario. ● Database: File systems apply to databases. You are advised to use full-SSDs for storage pools to which file systems belong and enable the data compression function. – When storage pools to which file systems belong use full-SSDs, the system will set the size of a file system block to 16 KB and enable the data compression function by default. If you choose **Advanced** > **Tuning** and disable the data compression function, the system will set the size of a file system block to 8 KB. In this scenario, you are advised to enable the data compression function. – When storage pools to which file systems belong do not use full-SSDs, the system will set the size of a file system block to 8 KB and disable the data compression function by default. If you choose **Advanced** > **Tuning** and disable the data compression function, the system will still set the size of a file system block to 8 KB. In this scenario, you are not advised to enable the data compression function.	[Value range] The value can be **VM**, **Database**, or **User-defined**. [Example] User-defined

Parameter	Description	Value
	● User-defined: In this scenario, users need to manually specify the block size of file systems.	
File System Block Size	If **Application Scenario** is set to **User Defined**, this parameter needs to be specified. Data in the file system consists of fixed-length disk blocks. The size of the blocks (also known as file system block size) affects disk space usage and performance. You are advised to use the block size following the principles below. ● Select 4 KB when the size of most files in the file system is smaller than 100 KB. ● Select 8 KB when the size of most files in the file system is between 100 KB and 1 MB. ● Select 16 KB when the size of most files in the file system is between 1 MB and 100 MB. ● Select 32 KB when the size of most files in the file system is between 100 MB and 1 GB. ● Select 64 KB when the size of most files in the file system is larger than 1 GB, the file system mainly processes bandwidth-consuming large I/Os (in scenarios such as M&E industry, and archive and backup of large files), or the file size and scenarios are not specified.	[Value range] The value can be **4KB**, **8KB**, **16KB**, **32KB**, or **64KB**. [Example] 64KB

Parameter	Description	Value
Quantity	Number of file systems batch created. Set this parameter based on your need. NOTE ● This option is invalid when you select **Use all the free capacity of the owning storage pool**. ● A maximum of 100 file systems can be created at one time. When multiple file systems are created, the system will automatically add suffixes to distinguish between file systems. ● File systems batch created have the same capacity.	[Value range] 1 to 100 [Example] 5
Manually specify the suffix	When creating multiple file systems, the system automatically appends a suffix number to the name of each file system for file system distinction. You can manually set the start suffix number after selecting this option. NOTE If this option is not selected, the suffix number starts at 0000 by default.	[Example] -
Start Number	This parameter is valid after **Manually specify the suffix** is selected. From the start number you configured, the system incrementally appends a suffix number to the name of each file system for file system distinction.	[Value range] 0 to (10000 - the quantity of file systems to create) NOTE If you want to create 30 file systems, the start number is from 0 to 9970.

Step 5 **Optional:** Set a timing snapshot policy.

1. Click **Timing Snapshot Policy**.

   The **Timing Snapshot Policy** dialog box is displayed.

2. Set a timing snapshot policy.
   - Select **Hours** and **Minute** to execute the timing snapshot. Begin calculating at 0 o'clock every day. For example, if **Every 6 Hours 10 Minute** is specified, then timing snapshot will be executed at **06:10**, **12:20**, and **18:30** every day.
   - Select **Daily** and set **Hours** and execution start time. For example, if **Hours: 01:00** and **17:00** are specified, and **Minute: 1** is specified, then timing snapshot will be executed at **01:01** and **17:01** every day.
   - Select **Weekly** and set **Week** and execution start time. For example, if **Week: Day 3**, and **Time: 11:50** is specified, then timing snapshot will be executed at **11:50** on **Sunday** and **Wednesday** every week.

- Select **Monthly** and set **Date** and execution start time. For example, if **Date: 2** and **30** are specified, and **Time: 12:10** is specified, then timing snapshot will be executed at **12:10** on dates **2** and **30** every month.

3. Click **OK**.

Step 6 **Optional:** Modify advanced properties of the file system.

1. Click **Advanced**.

   The **Advanced** dialog box is displayed.

2. Set advanced properties of the file system.

   Click the **Properties**, **Tuning** and **WORM** tabs and set related parameters. **Table 3-11**, **Table 3-12** and **Table 3-13** describe related parameters.

Table 3-11 Property parameters

Parameter	Description	Value
Owning Controller	Controller to which the file system belongs. NOTE To allocate file systems to controllers for load balancing, you are advised to select **Auto select**.	[Value range] Based on actual conditions of available controllers of the storage device. [Example] Auto select [Default] Auto select
Capacity Alarm Threshold (%)	Alarm threshold of the file system capacity.	[Value range] The value is an integer ranging from 50 to 95. [Example] 90 [Default] 90

Parameter	Description	Value
Initial Capacity Allocation Policy	Policy for the storage tier to allocate capacity to a file system. – Automatic allocation: The storage system automatically allocates capacity to a file system based on the ratio of the available capacity of the performance tier to that of the capacity tier. Capacity is allocated from the high performance tier only when the capacity of the performance tier and capacity tier is insufficient. – Allocate from the high performance tier first: The storage system allocates capacity to a file system from the high performance tier first. If the capacity of the high performance tier is insufficient, the storage system allocates capacity from the other storage tiers, first from the performance tier and then from the capacity tier. – Allocate from the performance tier first: The storage system allocates capacity to a file system from the performance tier first. If the capacity of the performance tier is insufficient, the storage system allocates capacity from the other storage tiers, first from the capacity tier and then from the high performance tier. – Allocate from the capacity tier first: The storage system allocates capacity to a file system from the capacity tier first. If the capacity of the capacity tier is insufficient, the storage system allocates capacity from the other storage tiers, first from the performance tier and then from the high performance tier.	[Value range] The value can be **Automatic allocation**, **Allocate from the high performance tier first**, **Allocate from the performance tier first**, or **Allocate from the capacity tier first**. [Example] Automatic allocation [Default] Automatic allocation

Parameter	Description	Value
Snapshot Directory Visibility	Specifies whether snapshot directories are visible.	[Value range] The value can be **Visible** or **Invisible**. [Example] Visible [Default] Visible
Max. Number of Timing Snapshots	Upper limit of the file system timing snapshots. When the number of created snapshots reaches the upper limit, the system automatically deletes the earliest timing snapshots.	[Value range] The value is an integer ranging from 1 to 2048. [Example] 16 [Default] 16
Delete Obsolete Read-Only Snapshots	Specifies whether **Delete Obsolete Read-Only Snapshots** is enabled. When used space of a file system reaches the Capacity alarm threshold and used space of snapshots is larger than reserved space for snapshots, the system automatically deletes the earliest read-only snapshots.	[Example] Enable [Default] Disable
Checksum	Specifies whether **Checksum** is enabled. This function is used to check data integrity. When it is enabled, checksum will be automatically calculated when data is being written, ensuring integrity of the data to be accessed. **NOTE** Enabling **Checksum** will impair the system performance.	[Example] Enable [Default] Enable
Automatic Update of Atime	Specifies whether **Automatic Update of Atime** is enabled. Atime is a time when file systems are accessed. After this function is enabled, Atime will be updated every time data on file systems is accessed. **NOTE** Enabling **Automatic Update of Atime** will impair the system performance.	[Example] Enable [Default] Disable

Parameter	Description	Value
Capacity Autonegotiation Policy	A storage system supports the following capacity autonegotiation policies: – **Not Use Capacity Autonegotiation**: The storage capacity used by a file system is fixed and is not flexibly adjusted by the storage system. – **Auto Expand Capacity**: increases file system capacity and meets users' requirements in data write when the available space of a file system is about to run out and the storage pool has available space. – **Auto Reduce or Expand Capacity**: The storage system automatically adjusts the file system capacity based on file system space usage. When the available space of a file system is about to run out and the storage pool has available space, automatic capacity expansion will be used to increase file system capacity. When the file system's storage space is released, it can be reclaimed into a storage pool and used by other file systems in data write requests. **NOTE** Parameters related to **Capacity Autonegotiation** are only supported in V300R006C10 and later versions.	[Example] Auto Expand Capacity [Default] Not Use Autonegotiation

Parameter	Description	Value
Capacity Reclamation Mode	A storage system supports the following capacity reclamation modes: - **Preferentially Expand Capacity**: Expand the capacity to increase the file system capacity. - **Preferentially Delete Old Snapshot**: Delete old snapshots to reclaim space for increasing the file system capacity. If HyperReplication and HyperMetro are configured for storage systems, the capacity autonegotiation policy of the primary storage system will be synchronized to the secondary storage system. If Preferentially Delete Old Snapshot is adopted, ensure that **Delete Obsolete Read-Only Snapshots** is enabled for the secondary storage system.	[Example] Preferentially Expand Capacity [Default] Preferentially Expand Capacity
Auto Adjust Capacity	After you select **Auto Adjust Capacity**, automatic capacity expansion or reduction policy for a file system will take effect during the service running.	[Example] Enable [Default] Enable
Auto Expand Trigger Threshold (%)	When the ratio of the used capacity to the total capacity of the file system is greater than the preset value, the storage system automatically triggers file system capacity expansion.	[Value range] The value is an integer ranging from 1 to 99. [Example] 85 [Default] 85
Auto Reduce Trigger Threshold (%)	When the ratio of the used capacity to the total capacity of the file system is smaller than the preset value, the storage system automatically triggers file system space reclamation and reduces file system capacity.	[Value range] The value is an integer ranging from 1 to 99. [Example] 50 [Default] 50

Parameter	Description	Value
Auto Expand Upper Limit	Set the auto expand upper limit.	[Value range] The value is an integer ranging from file system capacity to 16PB. [Example] 120GB [Default] File system capacity * 120%
Auto Reduce Lower Limit	Set the auto reduce lower limit.	[Value range] The value is an integer ranging from 1GB to **Auto Expand Upper Limit**. [Example] 100GB [Default] File system capacity
Auto Expanded/ Reduced Capacity Each Time	Set the auto expanded or reduced capacity for each time.	[Value range] The value is an integer ranging from 64MB to 100GB. [Example] 1GB [Default] 1GB

Table 3-12 Tuning parameters

Parameter	Description	Value
Priority Control	Priority control of SmartQoS. **NOTE** To apply this policy, you must purchase the SmartQoS license.	[Value range] The value can be **Low**, **Medium**, or **High**. [Example] Low [Default] Low

Parameter	Description	Value
Traffic Control	Traffic control policy of SmartQoS. **NOTE** To apply this policy, you must purchase the SmartQoS license. If no traffic control policy exists, click **Create** to create one.	[Default] -
Enable deduplication	Enable the deduplication function. Storage space saved by using deduplication. **NOTE** – To apply this policy, you must purchase the SmartDedupe license. – OceanStor 2200 V3 storage system does not support this function.	[Example] Enable deduplication
Enable data compression	Enable the data compression function. Storage space saved by using data compression. **NOTE** – To apply this policy, you must purchase the SmartCompression license. – OceanStor 2200 V3 storage system does not support this function.	[Example] Enable data compression
SmartPartition	Specify SmartPartition for the file system. SmartPartition allocates cache resources of storage system to the file system to meet the cache hit ratio required by different applications. **NOTE** – To apply this policy, you must purchase the SmartPartition license. – Select the owning controller of file system manually. This controller must be the same as the owning controllers of SmartPartition, or SmartPartition is unavailable. If no SmartPartition exists, click **Create** to create one.	[Default] -

Parameter	Description	Value
SmartCache Partition	To specify SmartCache partition for the file system. In the scenario that read operations are more than write operations and hot spot data exists, use the SSDs as cache by employing SSD high read performance to improve system read performance. **NOTE** – To apply this policy, you must purchase the SmartCache license. – Please select the owning controller of the file system manually. This controller must be the same as the owning controllers of SmartCache partition, or SmartCache is unavailable. – SmartCache does not support self-encrypting SSD. If no SmartCache partition exists, click **Create** to create one.	[Default] -

Table 3-13 WORM parameters

Parameter	Description	Value
Enable	If you want to create a WORM file system, select **Enable**.	[Default value] Not enabled

Paramete r	Description	Value
Mode	Compliance mode of WORM protection. Modes are: – **Enterprise Compliance Mode** ■ Files within the protection period cannot be modified, renamed, or deleted by command users, but can be deleted by system administrators. ■ When the protection period is overdue, the file expires and it can be deleted, but cannot be modified or renamed by common users and system administrators. – **Regulatory Compliance Mode** ■ Files within the protection period cannot be modified, renamed, or deleted by common users and system administrators. ■ When the protection period is overdue, the file expires and it can be deleted, but cannot be modified or renamed by common users and system administrators.	[Default value] Regulatory Compliance
Min. Retention	The shortest file protection period supported by WORM file system.	[Value range] 0 to 70 years or **Indefinite**. [Default value] 3 years NOTE **Min. Retention** must be smaller than or equal to **Default Retention** and **Max. Retention**.
Max. Retention	The longest file protection period supported by WORM file system.	[Value range] 1 day to 70 years or **Indefinite**. [Default value] 70 years

Paramete r	Description	Value
Default Retention	If no expiration time is configured for a file, the expiration time of the file is determined by the default retention.	[Value range] No less than **Min. Retention** and no bigger than **Max. Retention** or **Indefinite**. [Default value] Regulatory compliance Mode:70 years Enterprise compliance Mode:3 years NOTE To set **Default Retention** as **Indefinite**, you must set **Max. Retention** to **Indefinite**. Otherwise, the setting fails.
Automatic Lock	If the function is enabled, and a file is not modified within the **Lockout Wait Time (hours)**, files enters locked state automatically. Therefore, the file is under protection, and you can only read the file under locked state, but cannot modify, delete or rename it. NOTE Write operation include file data change or metadata change.	[Default value] Enable
Lockout Wait Time (hours)	Retention of a file enters the locked state. NOTE This parameter is valid only when **Automatic Lock** is enabled.	[Value range] The value is an integer ranging from 2 to 168. [Default value] 2
Automatically Delete	If this mode is enabled, the system automatically deletes files whose protection period is overdue.	[Default value] Disabled

NOTE

- If WORM is enabled, the file system created is a WORM file system. More information about WORM file system, see *OceanStor V3 Series V300R006 WORM Feature Guide*.
- Before creating a WORM file system, you must initialize WORM regulatory clock through CLI. The CLI command is **change system secure_compliance_clock date=***?*.

3. Click **OK**.

   The **Create File System** dialog box is displayed.

Step 7 Confirm that you want to create this file system.

1. Click **OK**.

   The **Execution Result** dialog box is displayed indicating that the operation succeeded.

2. Click **Close**.

----End

3.7 (Optional) Creating a Quota Tree

Quota tree is the level-1 subdirectory of a file system. In a quota tree, you can set directory quotas, user quotas, or user group quotas. You can manage space occupied by files in the directory.

Prerequisites

At least one file system is created.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Provisioning** > **File System**.

Step 3 Select a file system for which you want to create a quota tree. On the menu bar, choose **More** > **Create Quota Tree**.

The **Create Quota Tree** dialog box is displayed.

NOTE

You can also right-click a file system for which you want to create a quota tree and then choose **Create Quota Tree**.

Step 4 Create a quota tree. **Table 3-14** describes the related parameters.

Table 3-14 Quota tree parameters

<table>
<tr><th>Parameter</th><th>Description</th><th>Value</th></tr>
<tr><td>Name</td><td>Name of the quota tree.</td><td>[Value range]
● The name must be unique.
● For V300R006C00, the name can only contain letters, digits, and underscores (_).
● For V300R006C10, the name can only contain letters, digits and special characters. Special characters include !"#$%&'()*+-.;<=>?@[\]^`{_|}~ and spaces. On the CLI, some characters need to be entered as escape characters. For example, \| indicates |, || indicates \, \q indicates ?, and \s indicates spaces.
● The name can be 1 to 127 characters in length.
[Example]
quotatree001</td></tr>
<tr><td>Quantity</td><td>Number of quota trees created in a batch. Set this parameter based on your need.</td><td>[Value range]
1 to 500
[Example]
5</td></tr>
<tr><td>Owning File System</td><td>Owning file system of the quota tree.</td><td>[Example]
filesystem_001</td></tr>
<tr><td>Quota</td><td>After quota is enabled, the system restricts the number of files and file size of quota tree.
NOTE
If there is quota requirement on the file system for which you want to create a quota tree, you are advised to enable the quota function.</td><td>[Example]
Enable</td></tr>
</table>

Step 5 Confirm that quota tree is successfully created.

1. Click **OK**.

   The security alert dialog box is displayed.

   NOTE

   This message will be displayed only after the quota function is enabled.

2. Confirm the information in the dialog box and select **I have read and understand the consequences associated with performing this operation**, click **OK**.

The **Execution Result** dialog box is displayed indicating that the operation succeeded.

3. Click **Close**.

----End

3.8 (Optional) Creating a Quota

This operation enables you to restrict the space used by files or the number of files in the root directory or by user/user group.

Prerequisites

- At least one file system and quota tree have been created.
- If you want to create quota for a specified user or user group, the user or user group must have been created.

Context

For the following types of groups and users, the quota is not limited but is tracked and displayed: **root** user group and its users, and a storage system's **Administrators** user group and its users, and users in a Windows operating system's **Administrators** user group.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Provisioning** > **File System**.

Step 3 Select a file system for which you want to create a quota. On the menu bar, choose **More** > **Create Quota**.

The **Create Quota Wizard** dialog box is displayed.

Step 4 Select a quota type and directory, user or user group.

- Directory quota
  a. Select a quota type of **Directory quota**, and click **Next**.
  b. Select the directory whose quota you want to restrict.
     - Select **All Quota Tree**.
     - Select **Specific Quota Tree**. Click ... and select a quota tree whose quota you want to restrict.

       NOTE

       If no quota tree is available, create one.
  c. Click **Next**.
- User quota
  a. Select a quota type of **User quota**, and click **Next**.
  b. Select a specified quota tree in **Quota Tree**.
  c. Select the user whose quota you want to restrict.

        - Select **All Users**.
        - Select **Specific Users**. Select a specified user in the lower area.

          NOTE

          - If no user is available, add one.
          - If you select **Local authentication user**, click **Find**, in the pop-up **Add User** dialog boxes to select the user or user group you want to add. Click **OK**. You can choose **Provisioning** > **User Authentication** to create local authentication user in the **Local Authentication User** tab.
          - If you select **Domain user**, enter the corresponding name in **Name**, and click **Add**. For NIS domain and LDAP domain, the name format is **Domain user name**. For AD domain, the name format is **Domain name\Domain user name**. Please contact the domain server administrator to obtain the domain user name.
          - When CIFS users are mapped to NFS users, quota statistics will be collected for the NFS users or owning user group.

    d. Click **Next**.

- User group quota

    a. Select a quota type of **User group quota**, and click **Next**.

    b. Select a specified quota tree in **Quota Tree**.

    c. Select the user group whose quota you want to restrict.

        - Select **All Users Groups**.
        - Select **Specific User Groups**. Select a specified user in the lower area.

          NOTE

          - If no user group is available, add one.
          - If you select **Local authentication user group**, click **Find**, in the pop-up **Add User Group** dialog boxes to select the user or user group you want to add. Click **OK**. You can choose **Provisioning** > **User Authentication** to create local authentication user group in the **Local Authentication User Group** tab.
          - If you select **Domain user group**, enter the corresponding name in **Name**, and click **Add**. The name format is **Domain user group name**. Please contact the domain server administrator to obtain the domain user group name.
          - User group quota does not support AD domain.

    d. Click **Next**.

Step 5 Set the space quota or file quantity quota, and click **Next**.

Table 3-15 describes related parameters.

Table 3-15 Quota parameters

Parameter	Description	Value
Hard Quota	If the space quota exceeds the hard quota, the system immediately forbids write operations and prevents users from using extra file space.	[Value range] The value must be greater than the space soft quota, and smaller than or equal to **Maximum capacity of a file system**. NOTE ● You can query **Maximum capacity of a file system** in section "Software Specifications" in the *Product Description* specific to your product. ● The space quota is not limited by the file system capacity, and can be greater than or smaller than the file system capacity. [Example] 100 GB
Soft Quota	If the space quota exceeds the soft quota, the system generates an alarm but still allows write operations. After exceeding the hard quota, the system immediately forbids write operations.	[Value range] The value must be smaller than the space hard quota. If the space hard quota is not entered, the value must be smaller than or equal to **Maximum capacity of a file system**. NOTE ● You can query **Maximum capacity of a file system** in section "Software Specifications" in the *Product Description* specific to your product. ● The space quota is not limited by the file system capacity, and can be greater than or smaller than the file system capacity. [Example] 80 GB
Hard Quota (K)	If the file quantity quota exceeds the hard quota, the system immediately forbids write operations and prevents users from using extra files. The unit of the hard quota is set to **K**.	[Value range] The value must be greater than the soft quota of file quantity, and smaller than or equal to 2,000,000. [Example] 2

Parameter	Description	Value
Soft Quota (K)	If the file quantity quota exceeds the soft quota, the system generates an alarm but still allows write operations. After exceeding the hard quota, the system immediately forbids write operations. The unit of the soft quota is set to **K**.	[Value range] The value must be smaller than the hard quota of file quantity. If the hard quota of file quantity is not specified, the value must be smaller than or equal to 2,000,000. [Example] 1

Step 6 Confirm that the quota is successfully created.

1. Confirm the quota information and click **Finish**.

   The **Execution Result** dialog box is displayed indicating that the operation succeeded.

   NOTE

   If **Quota Type** in step 1 is set to **User quota** or **User group quota**, **Quota Tree** in step 2 is set to a specific quota tree, and the quota function has not been enabled for the quota tree, **Enable quota immediately** in the lower left corner is selected by default.

2. Click **Close**.

   The security alert dialog box is displayed.

   NOTE

   This message will be displayed only after **Enable quota immediately** is selected.

3. Confirm the information in the dialog box and select **I have read and understand the consequences associated with performing this operation**, click **OK**.

   The **Execution Result** dialog box is displayed indicating that the operation succeeded.

4. Click **Close**.

----End

3.9 Sharing File Systems

This section describes how to share file systems.

A file system can be accessed only after it is shared. File systems can be shared using four protocols: NFS, CIFS, FTP, and HTTP. This section describes configuration operations required for sharing file systems using the protocols.

NFS

NFS is a protocol developed by Sun. Internet Engineering Task Force (IETF) is in charge of developing its new versions. This protocol is designed for file sharing among Linux, UNIX, Mac OS, and VMware operating systems.

CIFS

CIFS is a file system share protocol developed by Microsoft and primarily used in Windows environments. The CIFS share and Homedir share use the CIFS protocol.

- CIFS share: a file system or its quota tree is shared among authentication users including local authentication users and domain authentication users. Users have their permissions set by the storage system for accessing CIFS shares.
- Homedir share: a file system is shared to a specific user as an exclusive directory. The user can only access the exclusive directory named after its user name.

Cross-Protocol Share Access

The storage system allows NFS sharing and CIFS sharing to be configured for the same file system concurrently. The storage system uses the user mapping function to allow users to access shared files across protocols (CIFS-NFS) used by clients on different platforms and obtain precise permission control.

FTP

File Transfer Protocol (FTP) is a universal protocol for transferring files between two computers over a TCP/IP network and primarily used in Internet environments.

HTTP

Hypertext Transfer Protocol (HTTP) is a protocol for transferring hypertext from web servers to local clients and primarily used in Internet environments.

3.9.1 Configuring an NFS Share

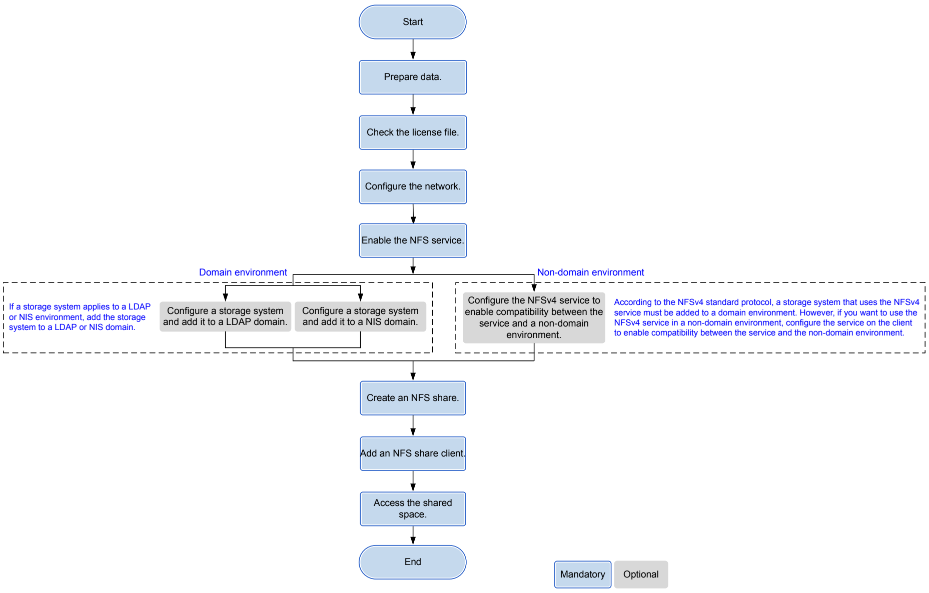
Storage system supports the NFS share mode. After configuring an NFS share, you can set different access permissions for clients.

3.9.1.1 Configuration Process

This section describes the NFS share configuration process.

Figure 3-5 shows the NFS share configuration process.

Figure 3-5 NFS share configuration process


Start
Prepare data.
Check the license file.
Configure the network.
Enable the NFS service.
Domain environment
Non-domain environment
If a storage system applies to a LDAP or NIS environment, add the storage system to a LDAP or NIS domain.
Configure a storage system and add it to a LDAP domain.
Configure a storage system and add it to a NIS domain.
Configure the NFSv4 service to enable compatibility between the service and a non-domain environment.
According to the NFSv4 standard protocol, a storage system that uses the NFSv4 service must be added to a domain environment. However, if you want to use the NFSv4 service in a non-domain environment, configure the service on the client to enable compatibility between the service and the non-domain environment.
Create an NFS share.
Add an NFS share client.
Access the shared space.
End
Mandatory
Optional

3.9.1.2 Preparing Data

Before configuring an NFS share in a storage system, plan and collect required data to assist in the follow-up service configuration.

You need to prepare the following data:

- Logical IP address

  Logical IP address used by a storage system to provide shared space for a client.
- File system

  File system used to create an NFS share.
- LDAP domain or NIS domain information
- Permission

  The permissions include read-only and read-write.
  - Read-only: Clients have the read-only permission for NFS shares.
  - Read-write: Clients have the read-write permission for NFS shares.

NOTE

You can contact your network administrator to obtain desired data.

3.9.1.3 Checking the License File

Each value-added feature requires a license file for activation. Before configuring a value-added feature, ensure that its license file is valid for the feature.

Context

On the DeviceManager interface, NFS feature is displayed in **Feature** of **NFS Protocol**.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Settings** > **License Management**.

Step 3 Check the active license files.

1. In the navigation tree on the left, choose **Active License**.
2. In the middle information pane, verify the information about active license files.

----End

Follow-up Procedure

- If the information about the license of the feature is not displayed on the **Active License** page, apply for and import a license file as instructed in the *Installation Guide* of the corresponding product model.
- If the storage system generates an alarm indicating that the license expired, purchase and import another license file.

3.9.1.4 Configuring a Network

This section describes how to use DeviceManager to configure a logical IP address for a storage system. The logical IP address is used for accessing shares.

3.9.1.4.1 (Optional) Configuring DNS-based Load Balancing Parameters (Applicable to V300R006C10 and Later Versions)

Storage arrays' DNS-based load balancing feature can detect the IP address load on the arrays in real time and use a proper IP address as the DNS response to achieve load balancing among IP addresses. This section describes how to configure DNS-based load balancing and DNS zones.

Context

Working principle:

1. When a host accesses the NAS service of a storage array using the domain name, the host first sends a DNS request to the built-in DNS server of the storage array and the DNS server obtains the IP address according to the domain name.
2. When a domain name contains multiple IP addresses, the storage array selects the IP address with a light load as the DNS response based on the configured load balancing policy and returns the DNS response to the host.
3. After receiving the DNS response, the host sends a service request to the destination IP address.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Settings** > **Storage Settings** > **File Storage Service** > **DNS-based Load Balancing**.

Step 3 **Table 3-16** lists parameters related to DNS-based load balancing.

Table 3-16 DNS-based load balancing parameters

Parameter	Description	Value
DNS-based Load Balancing	Enables or disables DNS-based load balancing. **NOTE** ● When enabling the DNS-based load balancing function, you are advised to disable the global namespace forwarding function. This function affects DNS-based load balancing. ● After the DNS-based load balancing function is disabled, the domain name resolution service is unavailable and file systems cannot use the function. ● This parameter can be set only in the system view, not in the vStore view. The setting takes effect for the entire storage system.	[Example] Enable

Parameter	Description	Value
Load Balancing Policy	This parameter enables you to configure DNS-based load balancing policies. A storage system supports the following load balancing policies: ● Weighted round robin: When a client uses a domain name to initiate an access request, the storage system calculates the weight based on the performance data. Under the same domain name, IP addresses that are required to process loads have the same probability to be selected to process client services. ● CPU usage: When a client uses a domain name to initiate an access request, the storage system calculates the weight based on the CPU usage of each node. Using the weight as the probability reference, the storage system selects a node to process the client's service request. ● Bandwidth usage: When a client uses a domain name to initiate an access request, the storage system calculates the weight based on the total bandwidth usage of each node. Using the weight as the probability reference, the storage system selects a node to process the client's service request. ● Open connections: When a client uses a domain name to initiate an access request, the storage system calculates the weight based on the NAS connections of each node. Using the weight as the probability reference, the storage system selects a node to process the client's service request. ● Overall load: When a client uses a domain name to initiate an access request, the storage system selects a node to process the client's service request based on the comprehensive load. The comprehensive node load is calculated based on the CPU usage, bandwidth usage, and number of NAS connections. Less	[Example] Weighted round robin

Parameter	Description	Value
	loaded nodes are more likely to be selected. NOTE This parameter can be set only in the system view, not in the vStore view. The setting takes effect for the entire storage system.	

Step 4 Configure a DNS zone.

A DNS zone contains IP addresses of a group of logical ports. A host can use the name of a DNS zone to access shared services provided by a storage system. Services can be evenly distributed to logical ports.

NOTE

Only the logical ports whose **Role** is **Service** or **Management+Service** can be added into a DNS zone. The logical ports whose **Role** is **Management** cannot be added in to a DNS zone.

1. Add a DNS zone.
   a. Click **Add**.
   b. The **Add DNS Zone** dialog box is displayed. In **Domain Name**, type the domain name of the DNS zone you want to add and click **OK**.

      NOTE

      The domain name complexity requirements are as follows:

      ■ A domain name contains 1 to 255 characters and consists of multiple labels separated by periods (**.**).

      ■ A label contains 1 to 63 characters including letters, digits, hyphens (-), and underscores (_), and must start and end with a letter or a digit.

      ■ The domain name must be unique.
2. Remove a DNS zone.
   a. In the DNS zones that are displayed, select a DNS zone you want to remove.
   b. Click **Remove**.
3. Modify a DNS zone.
   a. In the DNS zones that are displayed, select a DNS zone you want to modify.
   b. Click **Modify**.
   c. The <**Modify DNS Zone** dialog box is displayed. In **Domain Name**, type the domain name of the DNS zone you want to modify and click **OK**.
4. View a DNS zone.
   a. In **DNS Zone**, type a keyword and click **Search**.
   b. In **DNS Zone**, the DNS zone names relevant to the keyword will be displayed.

      NOTE

      You can select a DNS zone to modify or remove it.

Step 5 Click **Save**. The **Warning** dialog box is displayed.

Step 6 Confirm the information in the dialog box and select **I have read and understand the consequences associated with performing this operation**.

Step 7 Click **OK**. The **Execution Result** page is displayed.

Step 8 On the **Execution Result** page, confirm the modification and click **Close**. The DNS zone configuration is complete.

----End

Follow-up Procedure

Choose **Provisioning** > **Port** > **Logical Ports** to configure **Listen DNS Query Request** and **DNS Zone** information for logical ports.

3.9.1.4.2 Creating a Logical Port

This operation enables you to create a logical port for managing and accessing file based on Ethernet ports, bond ports, or VLANs.

Precautions

The number of logical ports created for each controller is recommended not more than 64. If the number exceeds 64 and a large number of ports do not work properly, logical ports drift towards the small number of ports available. As a result, service performance deteriorates.

Procedure

Step 1 Log in to DeviceManager.

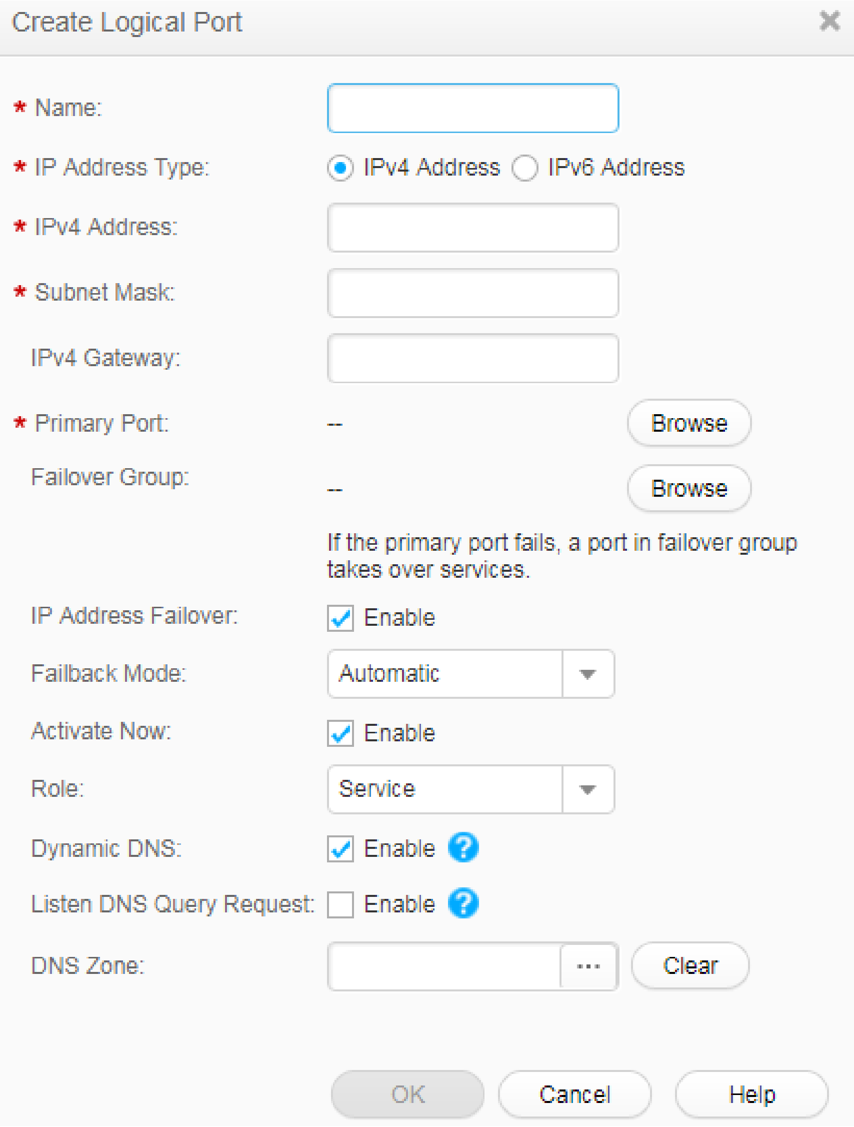
Step 2 Choose **Provisioning** > **Port** > **Logical Ports**.

Step 3 Click **Create**.

The **Create Logical Port** dialog box is displayed.

Step 4 In the **Create Logical Port** dialog box, configure related parameters.

Table 3-17 describes related parameters.



Create Logical Port

* Name:	
* IP Address Type:	● IPv4 Address ○ IPv6 Address
* IPv4 Address:	
* Subnet Mask:	
IPv4 Gateway:	
* Primary Port:	-- Browse
Failover Group:	-- Browse If the primary port fails, a port in failover group takes over services.
IP Address Failover:	☑ Enable
Failback Mode:	Automatic
Activate Now:	☑ Enable
Role:	Service
Dynamic DNS:	☑ Enable
Listen DNS Query Request:	□ Enable
DNS Zone:	... Clear

Table 3-17 Logical port parameters

Parameter	Description	Value
Name	Name of the logical port. The name must meet the following requirements so that the logical port is available to compatible applications: ● The name must be unique. ● The name can contain only letters, digits, underscores (_), periods (.), and hyphens (-). ● The name contains 1 to 31 characters.	[Example] lif01
IP Address Type	IP address type of the logical port, including IPv4 or IPv6.	[Example] IPv4
IPv4 Address	IPv4 address of the logical port.	[Example] 192.168.100.11
Subnet Mask	IPv4 subnet mask of the logical port.	[Example] 255.255.0.0
IPv4 Gateway	IPv4 gateway of the logical port.	[Example] 192.168.100.1
IPv6 Address	IPv6 address of the logical port.	[Example] fc00::1234
Prefix	IPv6 prefix length of the logical port.	[Example] 64
IPv6 Gateway	IPv6 gateway of the logical port.	[Example] fc00::1
Primary Port	Port to which the logical port belongs, including the Ethernet port, Bond port, and VLAN.	[Example] None

Parameter	Description	Value
Failover Group	Failover group name. **NOTE** - If a failover group is specified, services on the failed primary port will be taken over by a port in the specified failover group. - If no failover group is specified, services on the failed primary port will be taken over by a port in the default failover group.	[Example] None
IP Address Failover	After IP address failover is enabled, services are failed over to other normal ports within the failover group if the primary port fails. However, the IP address used by services remains unchanged. **NOTE** Shares of file systems do not support the multipathing mode. IP address failover is used to improve reliability of links.	[Example] Enable
Failback Mode	Mode in which services fail back to the primary port after the primary port is recovered. The mode can be manual or automatic. **NOTE** - If **Failback Mode** is **Manual**, ensure that the link to the primary port is normal before the failback. Services will manually fail back to the primary port only when the link to the primary port keeps normal for over five minutes. - If **Failback Mode** is **Automatic**, ensure that the link to the primary port is normal before the failback. Services will auto fail back to the primary port only when the link to the primary port keeps normal for over five minutes.	[Example] Automatic

Parameter	Description	Value
Activate Now	To activate the logical port immediately.	[Example] Enable
Role	Roles of logical ports include the following: ● Management: The port is used by a super administrator to log in to the system for management. ● Service: The port is used by a super administrator to access services such as file system CIFS shares. ● Management+Service: The port is used by a super administrator to log in to the system to manage the system and access services.	[Example] Service
Dynamic DNS	When the dynamic DNS is enabled, the DNS server will automatically and periodically update the IP address configured for the logical port.	[Example] Enable
Listen DNS Query Request	After this function is enabled, external NEs can access the DNS service provided by the storage system by using the IP address of this logical port.	[Example] Enable

Parameter	Description	Value
DNS Zone	Name of a DNS zone. **NOTE** ● If the value is blank, the logical port is not used for DNS-based load balancing. ● Only the logical ports whose **Role** is **Service** or **Management+Service** can be added into a DNS zone. The logical ports whose **Role** is **Management** cannot be added in to a DNS zone. ● One logical port can be associated with only one DNS zone. One DNS zone can be associated with multiple logical ports. ● A DNS zone can be associated with both IPv4 and IPv6 logical ports. ● The load balancing effect varies with the distribution of logical ports associated with a DNS zone. To obtain a better load balancing effect, ensure that logical ports associated with a DNS zone are evenly distributed among controllers.	[Example] None

Step 5 Click **OK**.

The **Success** dialog box is displayed indicating that the logical port has been successfully created.

Step 6 Click **OK**.

----End

3.9.1.4.3 (Optional) Creating a Bond Port

This section describes how to bond Ethernet ports on a same controller.

Prerequisites

Ethernet ports that have IP addresses cannot be bound. The IP addresses of the bonded host ports need to be cleared before bonding.

Context

- Port bonding provides more bandwidth and redundancy for links. Although ports are bonded, each host still transmits data through a single port and the total bandwidth can

be increased only when there are multiple hosts. Determine whether to bond ports based on site requirements.

- The port bond mode of a storage system has the following restrictions:
  - On the same controller, a bond port is formed by a maximum of eight Ethernet ports.
  - Only the interface modules with the same port rate (GE or 10GE) can be bonded.
  - The port cannot be bonded across controllers. Non-Ethernet network ports cannot be bonded.
  - SmartIO interface modules cannot be bonded if they work in cluster or FC mode or run FCoE service in FCoE/iSCSI mode.
  - Read-only users are unable to bind Ethernet ports.
  - Each port only allows to be added to one bonded port. It cannot be added to multiple bonded ports.
  - Ports are bonded to create a bond port that cannot be added to the port group.
- After Ethernet ports are bonded, **MTU** changes to the default value and you must set the link aggregation mode for the ports. For example, on Huawei switches, you must set the ports to the static LACP mode.

  NOTE

  The detailed link aggregation mode varies with the switches' manufacturer.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Provisioning** > **Port** > **Bond Ports**.

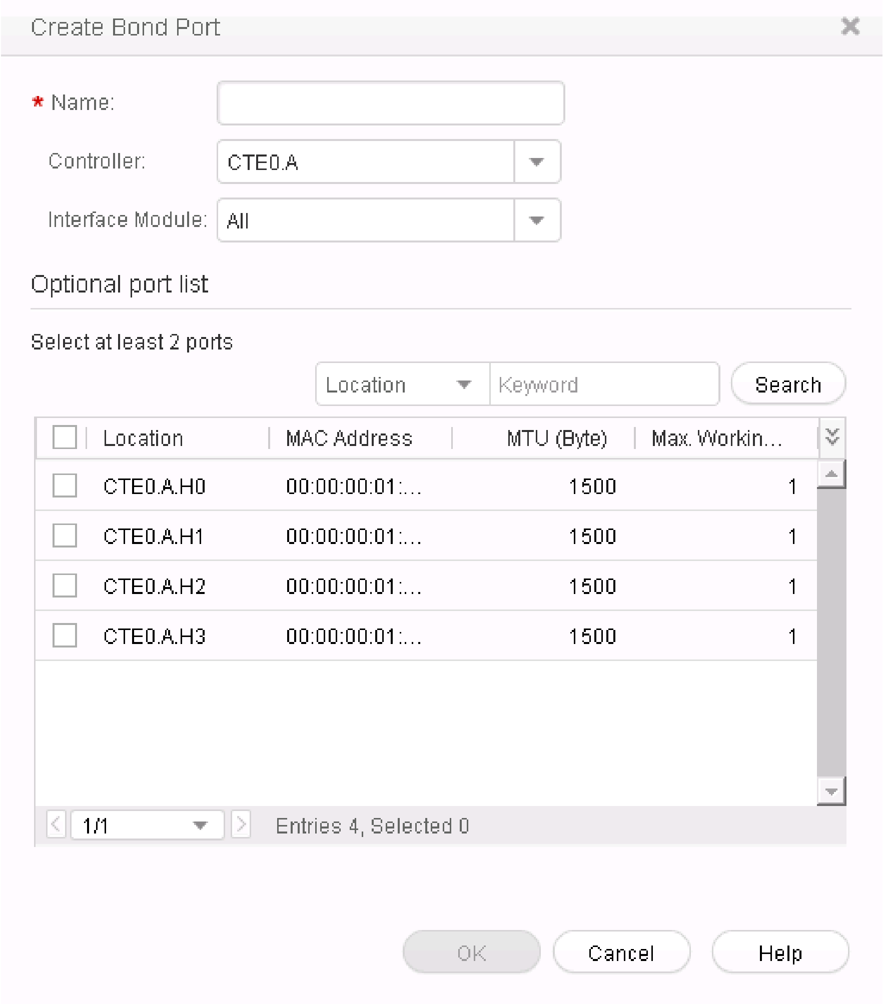
Step 3 Click **Create**.

The **Create Bond Port** dialog box is displayed.

NOTE

The port name format is **controller enclosure ID.interface module ID.port ID**.

Step 4 Set the name, interface module, and optional ports that can be bonded with the current Ethernet port.



* Name:

Controller: CTE0.A

Interface Module: All

Optional port list

Select at least 2 ports

□	Location	MAC Address	MTU (Byte)	Max. Workin...
□	CTE0.A.H0	00:00:00:01:...	1500	1
□	CTE0.A.H1	00:00:00:01:...	1500	1
□	CTE0.A.H2	00:00:00:01:...	1500	1
□	CTE0.A.H3	00:00:00:01:...	1500	1

1/1 Entries 4, Selected 0

1. In **Name**, enter a name for the bond port.

   The name:

   - Contains only letters, digits, underscores (_), periods (.), and hyphens (-).
   - Contains 1 to 31 characters.
2. From the **Controller**, select the controller the Ethernet ports own to.
3. Select the **Interface Module**.
4. From the **Optional port list**, select the Ethernet ports you want to bond.

   NOTE

   Select at least two ports.
5. Click **OK**.

   The security alert dialog box is displayed.

Step 5 Confirm that you want to bond these Ethernet ports.

1. Confirm the information of the dialog box and select **I have read and understand the consequences associated with performing this operation.**.
2. Click **OK**.

   The **Success** dialog box is displayed indicating that the operation succeeded.
3. Click **OK**.

----End

3.9.1.4.4 (Optional) Managing a Route of Logical Port

You need to configure a route when the NFS server and the storage system are not on the same network. When a domain controller server exists, ensure that the logical IP addresses and domain controller server can ping each other. If they cannot ping each other, add a route from the logical IP addresses to the network segment of the domain controller server. When configuring NFS share access, if the NFS server and logical IP addresses cannot ping each other, add a route from the logical IP addresses to the network segment route of the NFS server.

Prerequisites

The logical port has been assigned an IP address.

Procedure

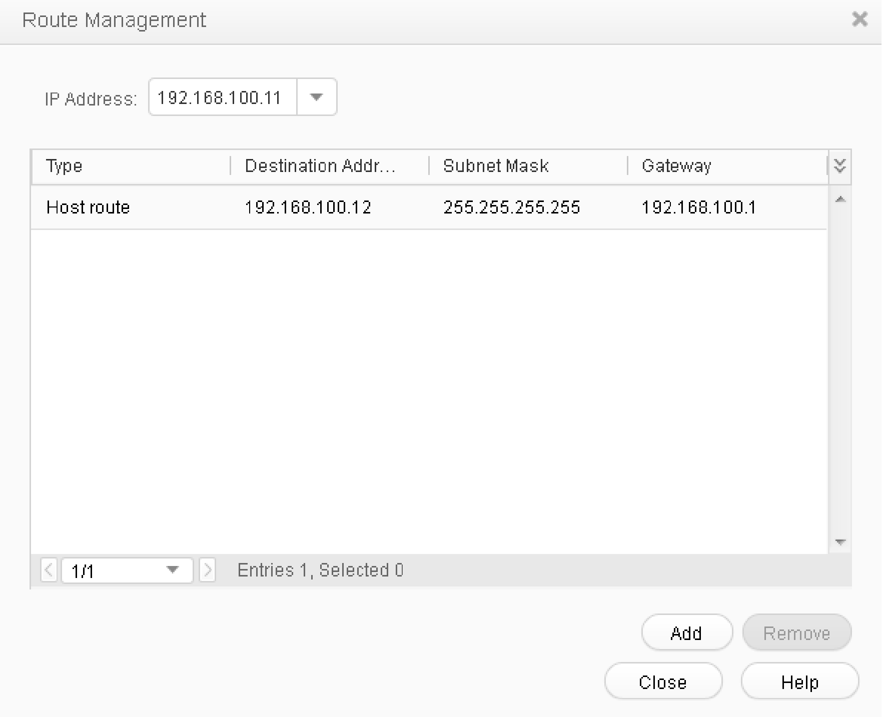
Step 1 Log in to DeviceManager.

Step 2 Go to the route management page.

You can go to the route management page by using either of the following methods:

- Choose **Provisioning** > **Port** > **Logical Ports**. Select a logical port for which you want to add a route and click **Route Management**. The **Route Management** dialog box is displayed.
- Choose **System** and click ↻ to switch to the rear view of the controller enclosure. Select the Ethernet port that you want to configure and click **Logical Port Management**. In the **Logical Port Management** dialog box that is displayed, select a logical port for which you want to add a route and click **Route Management**. The **Route Management** dialog box is displayed.

Step 3 Configure the route information for the logical port.



Route Management

IP Address: 192.168.100.11

Type	Destination Addr...	Subnet Mask	Gateway
Host route	192.168.100.12	255.255.255.255	192.168.100.1

1/1 Entries 1, Selected 0

1. In **IP Address**, select the IP address of the logical port.
2. Click **Add**.

   The **Add Route** dialog box is displayed.

   ⚠ **NOTICE**

   The default IP addresses of the internal heartbeat on the dual-controller storage system are **127.127.127.10** and **127.127.127.11**, and the default IP addresses of the internal heartbeat on the four-controller storage system are **127.127.127.10**, **127.127.127.11**, **127.127.127.12**, and **127.127.127.13**. Therefore, the IP address of the router cannot fall within the 127.127.127.XXX segment. Besides, the IP address of the gateway cannot be **127.127.127.10**, **127.127.127.11**, **127.127.127.12**, or **127.127.127.13**. Otherwise, routing will fail. (Internal heartbeat links are established between controllers for these controllers to detect each other's working status. You do not need to separately connect cables. In addition, internal heartbeat IP addresses have been assigned before delivery, and you cannot change these IP addresses).

3. In **Type**, select the type of the route to be added.

   Possible values of **Type** are **Default route**, **Host route**, and **Network segment route**.
4. Set **Destination Address**.
   - If **IP Address** is an IPv4 address, set **Destination Address** to the IPv4 address or network segment of the application server's service network port or that of the other storage system's logical port.
   - If **IP Address** is an IPv6 address, set **Destination Address** to the IPv6 address or network segment of the application server's service network port or that of the other storage system's logical port.
5. Set **Destination Mask** (IPv4) or **Prefix** (IPv6).
   - If a **Destination Mask** is set for an IPv4 address, this parameter specifies the subnet mask of the IP address for the service network port on the application server or storage device.
   - If a **Prefix** is set for an IPv6 address, this parameter specifies the prefix of the IPv6 address for application server's service network port or that of the other storage system's logical port.
6. In **Gateway**, enter the gateway of the local storage system's logical port IP address.

Step 4 Click **OK**. The route information is added to the route list.

The security alert dialog box is displayed.

Step 5 Confirm the information of the dialog box and select **I have read and understand the consequences associated with performing this operation.**.

Step 6 Click **OK**.

The **Success** dialog box is displayed indicating that the operation succeeded.

NOTE

To remove a route, select it and click **Remove**.

Step 7 Click **Close**.

----End

3.9.1.5 Setting the NFS Service

Before configuring an NFS share, enable the NFS service for clients to access the NFS share. The storage system supports NFSv3 and NFSv4.

Prerequisites

The license for NFS protocol has been imported and activated.

Context

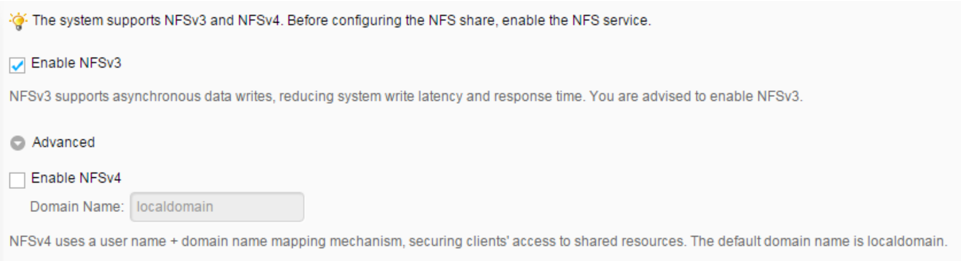
The system supports NFSv3 and NFSv4.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose ⚙ **Settings** > **Storage Settings** > **File Storage Service** > **NFS Service**.

Step 3 Enable the NFS service according to the protocol version used when the host mounts NFS share.



The system supports NFSv3 and NFSv4. Before configuring the NFS share, enable the NFS service.

☑ Enable NFSv3

NFSv3 supports asynchronous data writes, reducing system write latency and response time. You are advised to enable NFSv3.

● Advanced

□ Enable NFSv4

Domain Name: localdomain

NFSv4 uses a user name + domain name mapping mechanism, securing clients' access to shared resources. The default domain name is localdomain.

- If the host needs to use NFSv3 to mount shares, select **Enable NFSv3**.
- If host uses NFSv4 to mount share, execute the following steps.
  a. Click **Advanced** and select **Enable NFSv4**.
  b. After NFSv4 has been enabled, enter the storage domain name in **Domain Name**.

NOTE

– NFSv4 adopts the **user+domain** name mapping mechanism, enhancing the security of clients' access to shared resources. It is recommended that host use this version to mount share.

– In non-domain or LDAP environment, enter the default domain name **localdomain**.

– In an NIS environment, the entered information must be consistent with domain in the **/etc/idmapd.conf** file on the Linux client that accesses shares. It is recommended that both the two be the domain name of the NIS domain.

– The domain name must be no longer than 64 characters.

– To disable NFS service, do not select **Enable NFSv3/NFSv4**.

Step 4 Click **Save**.

The **Success** dialog box is displayed indicating that the operation succeeded.

Step 5 Click **OK**.

----End

3.9.1.6 (Optional) Configuring a Storage System to Add It to an LDAP Domain

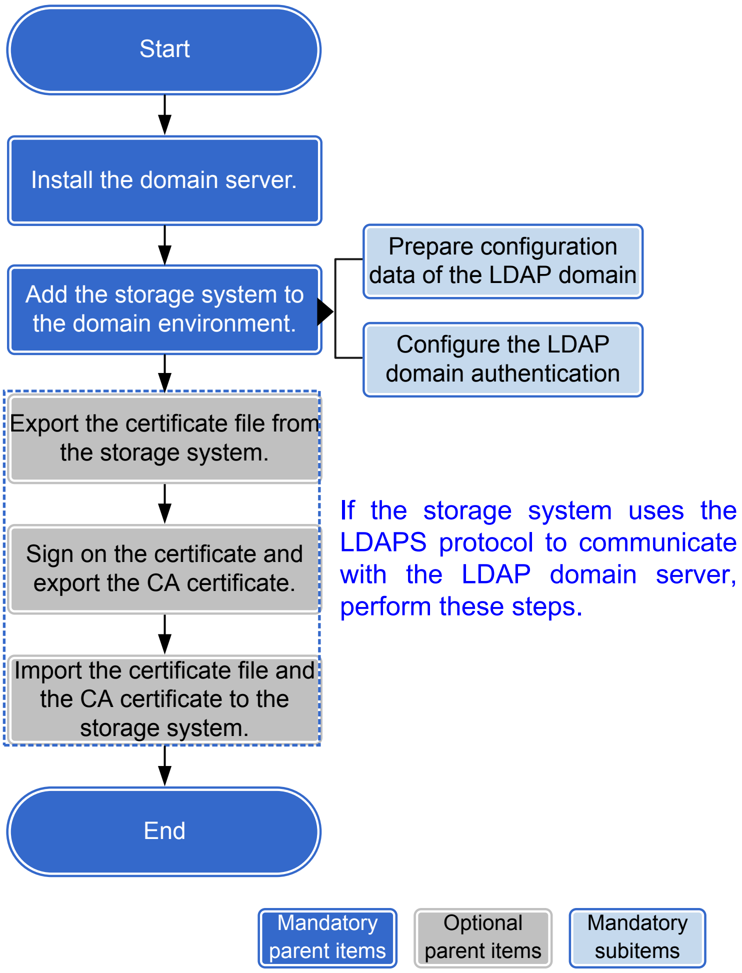
This section describes how to add a storage system to an LDAP domain.

3.9.1.6.1 Configuration Process

This section introduces the process of configuring an LDAP user or user group.

Figure 3-6 shows the process of configuring the LDAP domain authentication.

Figure 3-6 Process of configuring a storage system to add it to an LDAP domain


Start
Install the domain server.
Add the storage system to the domain environment.
Prepare configuration data of the LDAP domain
Configure the LDAP domain authentication
Export the certificate file from the storage system.
Sign on the certificate and export the CA certificate.
Import the certificate file and the CA certificate to the storage system.
If the storage system uses the LDAPS protocol to communicate with the LDAP domain server, perform these steps.
End
Mandatory parent items
Optional parent items
Mandatory subitems

3.9.1.6.2 Preparing the Configuration Data of an LDAP Domain

Collect the configuration data of an LDAP domain server in advance to add storage systems to the LDAP domain.

LDAP Domain Parameters

LDAP data is organized in a tree structure that clearly lays out organizational information. A node on this tree is called as **Entry**. Each **Entry** has a distinguished name (DN). The DN of an Entry is composed of the Base DN and RDN. The Base DN refers to the position of the parent node where the Entry resides on the tree, and the RDN refers to an attribute that distinguishes the Entry from others such as UID or CN.

LDAP directories function as file system directories. For example, directory **dc=redmond,dc=wa,dc=microsoft,dc=com** can be regarded as the following path of a file system directory: **com\microsoft\wa\redmond**. In another example of directory **cn=user1,ou=user,dc=example,dc=com**, **cn=user1** indicates a username and **ou=user** indicates the organization unit of an Active Directory (AD), that is, **user1** is in the user organization unit of the example.com domain.

The following figure shows data structure of an LDAP server:

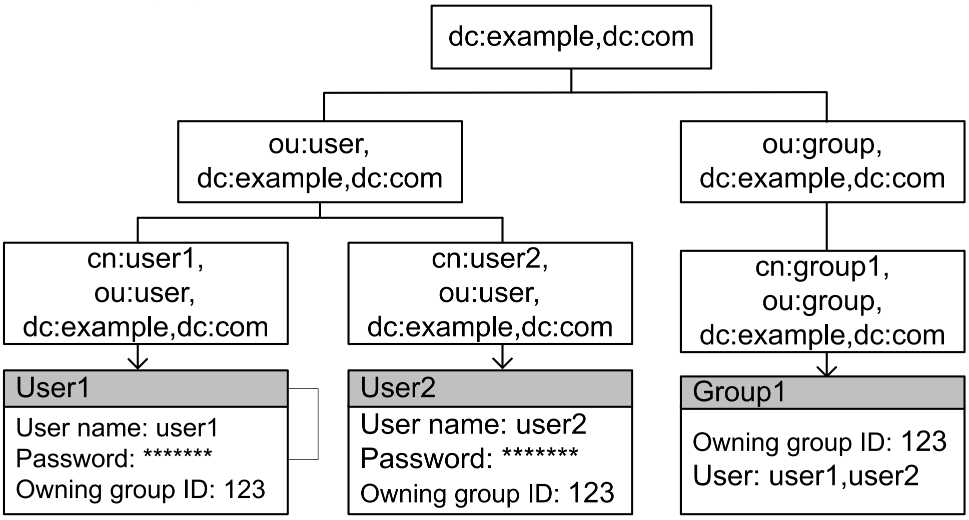


Table 3-18 describes meanings of LDAP entry acronyms.

Table 3-18 Meanings of LDAP entry acronyms

Acronym	Meaning
o	Organization
ou	Organization Unit
c	Country Name
dc	Domain Component
sn	Surname
cn	Common Name

What OpenLDAP Is?

OpenLDAP is a free and open implementation of LDAP that is now widely used in various popular Linux releases. OpenLDAP requires licenses.

OpenLDAP mainly consists of the following four components:

- slapd: an independent LDAP daemon

- slurpd: an independent LDAP update and replication daemon
- Library implementing LDAP
- Tool software and illustration client

The OpenLDAP installation package can be found here on the Userbooster website.

NOTE

The OpenLDAP installation package is not provided on the OpenLDAP website. The installation package supports the following Windows operating systems: Windows XP, Windows Server 2003, Windows Server 2008, Windows Vista, Windows 7, Windows 8, and Windows Server 2012.

Obtaining LDAP Configuration Data in Windows

Using OpenLDAP as an example, the following steps describe how to obtain LDAP configuration data.

1. Open the OpenLDAP installation directory.
2. Find the **slapd.conf** system configuration file.
3. Use the text editing software to open the configuration file and search for the following fields:

```
suffix   "dc=example,dc=com"
rootdn  "cn=Manager,dc=example,dc=com"

rootpw    XXXXXXXXXXXX
```

   - **dc=example,dc=com** corresponds to **Base DN** on the storage system configuration page.
   - **cn=Manager,dc=example,dc=com** corresponds to **Bind DN** on the storage system configuration page.
   - **XXXXXXXXXXXX** corresponds to **Bind Password** on the storage system configuration page. If the password is the ciphertext, contact LDAP server administrators to obtain the password.

4. Find configuration files (with **.ldif** as the file name extension) of users and user groups that need to access storage systems.

   NOTE

   LDAP Interchange Format (LDIF) is one of the most common file formats for LDAP applications. It is a standard mechanism that represents directories in the text format, and it allows users to import data to and export data from the directory server. LDIF files store LDAP configurations and directory contents, and you can obtain parameter information from LDIF files.

5. Use text editing software to open the configuration file and find the DNs of a user and a user group that correspond to **User Directory** and **Group Directory** respectively on the storage system configuration page.

```
#root on the top
dn: dc=example,dc=com
dc: example
objectClass: domain
objectClass: top
#First organization unit name: user
dn: ou=user,dc=example,dc=com
ou: user
objectClass: organizationalUnit
objectClass: top
#Second organization unit name: groups
dn: ou=group,dc=example,dc=com
ou: groups
objectClass: organizationalUnit
objectClass: top
```

```
#The first user represents user1 that belongs to organization unit user in
the organizational structure topology.
dn: cn=user1,ou=user,dc=example,dc=com
cn: user1
objectClass: posixAccount
objectClass: shadowAccount
objectClass: inetOrgPerson
sn: user1
uid: user1
uidNumber: 2882
gidNumber: 888
homeDirectory: /export/home/ldapuser
loginShell: /bin/bash
userPassword: {ssha}eoWxtWNl8YbqsulnwFwKMw90Cx5BSU9DRA==xxxxxx
#The second user represents user2 that belongs to organization unit user in
the organizational structure topology.
dn: cn=user2,ou=user,dc=example,dc=com
cn: user2
objectClass: posixAccount
objectClass: shadowAccount
objectClass: inetOrgPerson
sn: client
uid: client
uidNumber: 2883
gidNumber: 888
homeDirectory: /export/home/client
loginShell: /bin/bash
userPassword: {ssha}eoWxtWNl8YbqsulnwFwKMw90Cx5BSU9DRA==xxxxxx
#The first user group represents group1 that belongs to organization unit
group in the organizational structure topology. The group contains user1 and
user2.
dn: cn=group1,ou=group,dc=example,dc=com
cn: group1
gidNumber: 888
memberUid: user1#Belongs to the group.
memberUid: user2#Belongs to the group.
objectClass: posixGroup
```

Obtaining LDAP Configuration Data in Linux

Using OpenLDAP as an example, the following steps describe how to obtain LDAP configuration data.

1. Log in to an LDAP server as user **root**.
2. Run the **cd /etc/openldap** command to go to the **/etc/openldap** directory.

```
linux-ldap:~ # cd /etc/openldap
linux-ldap:/etc/openldap #
```

3. Run the **ls** command to view system configuration file **slapd.conf** and the configuration file (with **.ldif** as the file name extensions the file name extension) of users and user groups who want to access storage systems.

```
linux-ldap:/etc/openldap #ls
example.ldif ldap.conf schema slap.conf slap.con slapd.conf
```

4. Run the **cat** command to open system configuration file **slapd.conf** where you can view related parameters.

```
linux-ldap:/etc/openldap #cat slapd.conf

suffix   "dc=example,dc=com"
rootdn  "cn=Manager,dc=example,dc=com"

rootpw    XXXXXXXXXXXX
```

   - **dc=example,dc=com** corresponds to **Base DN** on the storage system configuration page.
   - **cn=Manager,dc=example,dc=com** corresponds to **Bind DN** on the storage system configuration page.

  - **XXXXXXXXXXXX** corresponds to **Bind Password** on the storage system configuration page. If the password is in cipher text, contact LDAP server administrators to obtain the password.

5. Run the **cat** command to open the **example.ldif** file. Find the DNs of a user and a user group that correspond to **User Directory** and **Group Directory** respectively on the storage system configuration page. For details about description of parameters, see **Example of LDIF Files in Windows**.

3.9.1.6.3 Configuring LDAP Domain Authentication Parameters

If an LDAP domain server is deployed on the customers' network, add the system to the LDAP domain. After the system is added to the LDAP domain, the LDAP domain server can authenticate NFS clients when they attempt to access the system share resources.

Prerequisites

- An LDAP domain has been set up.
- Associated configurations have been completed, and required data is ready.

NOTE

- The 2000, 5000, and 6000 series storage systems can be connected to the LDAP server through the management network port or the service network port (logical port). If the storage system communicates with the LDAP server through the management network port, the management network port of each controller must be connected properly to the LDAP server. If the storage system communicates with the LDAP server through the service network port, the service network port of each controller under each vStore must be connected properly to the LDAP server, ensuring that the services related to the LDAP server can be normally used. You are advised to use the service network port to connect to the LDAP server.
- The 18000 series storage systems can be connected to the LDAP server through the service port (logical port) only. And it requires all the controllers can communicate with the LDAP server.
- Storage system can be connected to only one LDAP server.

Precautions

You are advised to use physical isolation and end-to-end encryption to ensure security of data transfer between clients and LDAP domain servers.

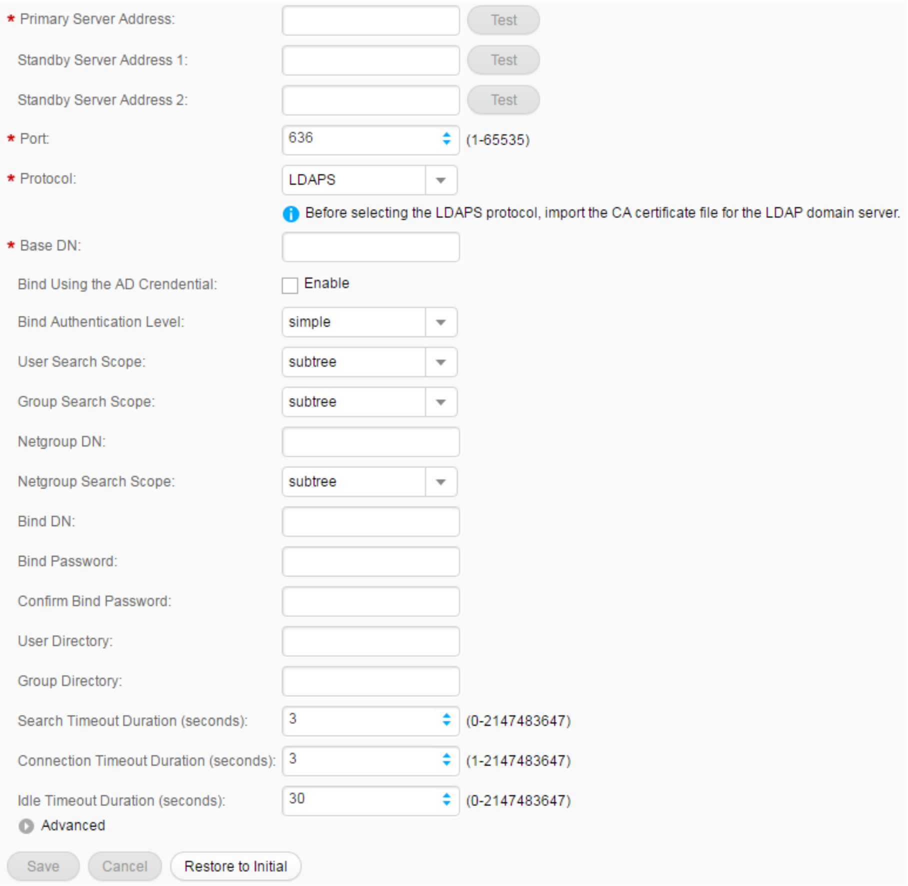
You are advised to configure a static IP address for the Lightweight Directory Access Protocol (LDAP) server. If a dynamic IP address is configured, security risks may exist.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Settings** > **Storage Settings** > **File Storage Service** > **Domain Authentication**.

Step 3 In the **LDAP Domain Settings** area, configure the LDAP domain authentication parameters. The related parameters are shown in **Table 3-19** below.



* Primary Server Address: [ ] Test

Standby Server Address 1: [ ] Test

Standby Server Address 2: [ ] Test

* Port: 636 (1-65535)

* Protocol: LDAPS

Before selecting the LDAPS protocol, import the CA certificate file for the LDAP domain server.

* Base DN:

Bind Using the AD Crendential: □ Enable

Bind Authentication Level: simple

User Search Scope: subtree

Group Search Scope: subtree

Netgroup DN:

Netgroup Search Scope: subtree

Bind DN:

Bind Password:

Confirm Bind Password:

User Directory:

Group Directory:

Search Timeout Duration (seconds): 3 (0-2147483647)

Connection Timeout Duration (seconds): 3 (1-2147483647)

Idle Timeout Duration (seconds): 30 (0-2147483647)

Table 3-19 Parameters of the LDAP domain

Parameter	Description	Value
Primary Server Address	IP address or domain name of an LDAP domain server. **NOTE** ● Ensure that the IP address or domain name is reachable. Otherwise, user authentication commands and network commands will time out. ● Click **Test** to check the connectivity of the entered IP address or domain name.	[Example] 192.168.0.100 www.test.com

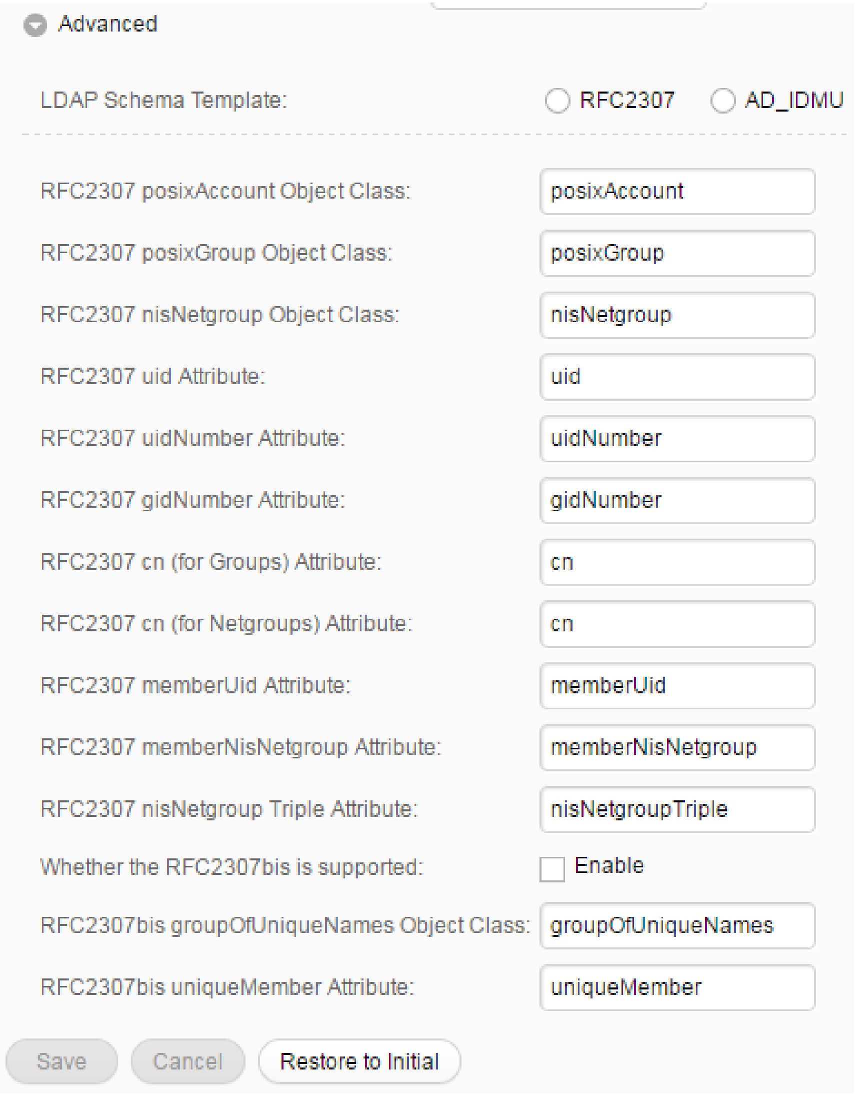
Parameter	Description	Value
Standby Server Address 1	IP address or domain name of standby LDAP server 1. **NOTE** ● Ensure that the IP address or domain name is reachable. Otherwise, user authentication commands and network commands will time out. ● Click **Test** to check the connectivity of the entered IP address or domain name.	[Example] 192.168.0.101 www.test.com
Standby Server Address 2	IP address or domain name of standby LDAP server 2. **NOTE** ● Ensure that the IP address or domain name is reachable. Otherwise, user authentication commands and network commands will time out. ● Click **Test** to check the connectivity of the entered IP address or domain name.	[Example] 192.168.0.102 www.test.com
Port	Port used by the system to communicate with the LDAP domain server. The default port number of the LDAP server is **389**, and the default port number of the LDAPS server is **636**.	[Value Range] A valid port ranges from 1 to 65535. [Example] 636

Parameter	Description	Value
Protocol	Protocol used by the system to communicate with the LDAP domain server. ● **LDAP**: indicates that the system uses the standard LDAP protocol to communicate with the LDAP domain server. ● **LDAPS**: indicates that the system uses the LDAP over SSL to communicate with the LDAP domain server if the LDAP domain server supports the SSL. **NOTE** Before selecting the LDAPS protocol, import the CA certificate file for the LDAP domain server. If an LDAP server is required to authenticate the storage system, import the certificate file and private key file.	[Example] LDAPS
Base DN	DN that specifies LDAP for searching.	[Rule] A DN consists of RDNs, which are separated from each other using commas (,). For example: testDn=testDn,xxxDn=xxx. [Format] xxx=yyy, separated by commas (,). [Example] dc=example,dc=com
Bind Using the AD Credential	Checks whether bind using the AD credential is enabled.	[Example] Disable
Bind Authentication Level	Select bind authentication level. Specifies a bind authentication level for LDAP. ● simple: simple authentication. ● SASL: Simple Authentication and Security Layer	[Example] simple

Parameter	Description	Value
User Search Scope	Specifies the search scope for user queries. ● subtree: Searches the named DN directory and subnodes under the DN. ● onelevel: Searches the subnodes under the DN. ● base: Searches just the named DN directory.	[Example] subtree
Group Search Scope	Specifies the search scope for user group queries. ● subtree: Searches the named DN directory and subnodes under the DN. ● onelevel: Searches the subnodes under the DN. ● base: Searches just the named DN directory.	[Example] subtree
Netgroup DN	Specifies the netgroup DN.	[Format] xxx=yyy, separated by commas (,). [Example] ou=netgroup,dc=example,dc=com
Netgroup Search Scope	Specifies the search scope for netgroup queries. ● subtree: Searches the named DN directory and subnodes under the DN. ● onelevel: Searches the subnodes under the DN. ● base: Searches just the named DN directory.	[Example] subtree

Parameter	Description	Value
Bind DN	Name of a bond directory. **NOTE** To access content, you must use the directory for searching.	[Rule] A DN consists of RDNs, which are separated from each other using commas (,). For example: testDn=testDn,xxxDn=xxx. [Format] xxx=yyy, separated by commas (,). [Example] cn=Manager,dc=example,dc=com
Bind Password	Password for accessing the bond directory. **NOTE** Simple password may cause security risk. Complicated password is recommended, for example, password contains uppercases, lowercases, digits and special characters.	[Example] !QAZ2wsx
Confirm Bind Password	Confirm password used by the system to log in to the LDAP domain server.	[Example] !QAZ2wsx
User Directory	User DN configured by the LDAP domain server.	[Example] ou=user,dc=admin,dc=com
Group Directory	User group DN configured by the LDAP domain server.	[Example] ou=group,dc=admin,dc=com
Search Timeout Duration (seconds)	The timeout duration of client waiting for the search result from server. The default value is 3 seconds.	[Example] 3
Connection Timeout Duration (seconds)	The timeout duration of client connecting with server. The default value is 3 seconds.	[Example] 3
Idle Timeout Duration (seconds)	Duration after which the LDAP server and client have no communication with each other, the connection is down. The default value is 30 seconds.	[Example] 30

Step 4 Click **Advanced** to set the advanced parameters of LDAP server. **Table 3-20** shows relevant parameters.



LDAP Schema Template: ○ RFC2307 ○ AD_IDMU

RFC2307 posixAccount Object Class:	posixAccount
RFC2307 posixGroup Object Class:	posixGroup
RFC2307 nisNetgroup Object Class:	nisNetgroup
RFC2307 uid Attribute:	uid
RFC2307 uidNumber Attribute:	uidNumber
RFC2307 gidNumber Attribute:	gidNumber
RFC2307 cn (for Groups) Attribute:	cn
RFC2307 cn (for Netgroups) Attribute:	cn
RFC2307 memberUid Attribute:	memberUid
RFC2307 memberNisNetgroup Attribute:	memberNisNetgroup
RFC2307 nisNetgroup Triple Attribute:	nisNetgroupTriple
Whether the RFC2307bis is supported:	□ Enable
RFC2307bis groupOfUniqueNames Object Class:	groupOfUniqueNames
RFC2307bis uniqueMember Attribute:	uniqueMember

Table 3-20 Advanced parameters

Parameter	Description	Value
LDAP Schema Template	You can select a type for the LDAP schema template. ● RFC2307: schema based on RFC2307. ● AD_IDMU: schema based on active directory identity management in Unix. **NOTE** ● You can select a schema template for which relevant parameters are entered automatically. You can also customize relevant parameters instead of selecting a schema template. ● Schema defines the structure and rules for LDAP directories and how LDAP servers identify category, attribute, and other information of LDAP directories.	[Example] RFC2307
RFC2307 posixAccount Object Class	Schema defines the name of the RFC2307 posixAccount object class.	[Value range] The value contains 0 to 1024 characters. [Example] posixAccount [Default value] ● posixAccount (displayed by default when RFC2307 is selected for LDAP scheme template) ● User (displayed by default when AD_IDMU is selected for LDAP scheme template)

Parameter	Description	Value
RFC2307 posixGroup Object Class	Schema defines the name of the RFC2307 posixGroup object class.	[Value range] The value contains 0 to 1024 characters. [Example] posixGroup [Default value] ● posixGroup (displayed by default when RFC2307 is selected for LDAP scheme template) ● Group (displayed by default when AD_IDMU is selected for LDAP scheme template)
RFC2307 nisNetgroup Object Class	Schema defines the name of the RFC2307 nisNetgroup object class.	[Value range] The value contains 0 to 1024 characters. [Example] nisNetgroup [Default value] nisNetgroup
RFC2307 uid Attribute	Schema defines the name of the RFC2307 uid attribute.	[Value range] The value contains 0 to 1024 characters. [Example] uid [Default value] uid
RFC2307 uidNumber Attribute	Schema defines the name of the RFC2307 uidNumber attribute.	[Value range] The value contains 0 to 1024 characters. [Example] uidNumber [Default value] uidNumber

Parameter	Description	Value
RFC2307 gidNumber Attribute	Schema defines the name of the RFC2307 gidNumber attribute.	[Value range] The value contains 0 to 1024 characters. [Example] gidNumber [Default value] gidNumber
RFC2307 cn (for Groups) Attribute	Schema defines the name of the RFC2307 cn (for groups) attribute.	[Value range] The value contains 0 to 1024 characters. [Example] cn [Default value] cn
RFC2307 cn (for Netgroups) Attribute	Schema defines the name of the RFC2307 cn (for Netgroups) attribute.	[Value range] The value contains 0 to 1024 characters. [Example] cn [Default value] ● cn (displayed by default when RFC2307 is selected for LDAP scheme template) ● name (displayed by default when AD_IDMU is selected for LDAP scheme template)
RFC2307 memberUid Attribute	Schema defines the name of the RFC2307 memberUid attribute.	[Value range] The value contains 0 to 1024 characters. [Example] memberUid [Default value] memberUid

Parameter	Description	Value
RFC2307 memberNisNetgroup Attribute	Schema defines the name of the RFC2307 memberNisNetgroup attribute.	[Value range] The value contains 0 to 1024 characters. [Example] memberNisNetgroup [Default value] memberNisNetgroup
RFC2307 nisNetgroup Triple Attribute	Schema defines the name of the RFC2307 nisNetgroupTriple attribute.	[Value range] The value contains 0 to 1024 characters. [Example] nisNetgroupTriple [Default value] ● nisNetgroupTriple (displayed by default when RFC2307 is selected for LDAP scheme template) ● NisNetgroupTriple (displayed by default when AD_IDMU is selected for LDAP scheme template)
Whether the RFC2307bis is supported	Whether to enable this function.	[Default value] Disable
RFC2307bis groupOfUniqueNames Object Class	Schema defines the name of the RFC2307bis groupOfUniqueNames object class. This parameter is valid only when **Whether the RFC2307bis is supported** is set to **Enable**.	[Value range] The value contains 0 to 1024 characters. [Example] groupOfUniqueName [Default value] groupOfUniqueName
RFC2307bis uniqueMember Attribute	Schema defines the name of the RFC2307bis uniqueMember attribute. This parameter is valid only when **Whether the RFC2307bis is supported** is set to **Enable**.	[Value range] The value contains 0 to 1024 characters. [Example] uniqueMember [Default value] uniqueMember

Step 5 Click **Save**. The LDAP domain authentication configuration is completed.

NOTE

Click **Restore to Initial** to initialize the LDAP domain authentication.

----End

3.9.1.6.4 (Optional) Generating and Exporting a Certificate on the Storage System

This section describes how to generate and export a certificate required for configuring domain authentication on the storage system.

Context

- The certificate generated on the storage system is not signed and requires to be signed on the signature server.
- If you use a third-party tool to export certificate request files, save the exported private key file as well. These files, together with the signed certificate and CA certificate, are imported to the storage system when the certificates are verified on the storage system.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Settings** > **Storage Settings** > **Value-added Service Settings** > **Credential Management**.

Step 3 Set **Certificate Type** to **Domain authentication certificate** and click **Generate and Export**.

The **Save As** dialog box is displayed. Select a path to save the certificate and click **Save**.

----End

Follow-up Procedure

After the domain authentication certificate is exported, sign the signature on it.

3.9.1.6.5 (Optional) Signing the Authentication Certificate and Exporting the CA Certificate

After a domain authentication certificate is exported, it takes effect only after it is signed by a third-party signing server. The CA certificate should be exported at the same time.

After the domain authentication certificate is exported, sign on the certificate based on actual conditions and export the CA certificate for follow-up procedures.

3.9.1.6.6 (Optional) Importing the Certificate and CA Certificate to the Storage System

This chapter introduces how to import the authentication certificate and CA certificate to the storage system to active the authentication certificate.

Prerequisites

- The signed certificate and CA certificate already exist.
- If the certificate file is exported and signed by a third-party tool, ensure that the private key file exists.

Context

If the certificate file is exported and signed by a third-party tool, import the private key file when you import and activate the certificate and CA certificate.

Procedure

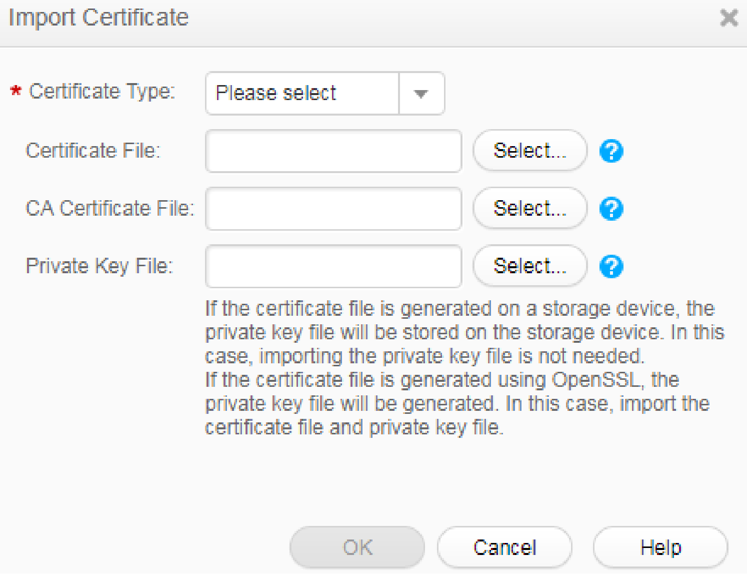
Step 1 Log in to DeviceManager.

Step 2 Choose **Settings** > **Storage Settings** > **Value-added Service Settings** > **Credential Management**.

Step 3 Import and activate the certificate.

1. After the certificate has been signed by the server, click **Import and Activate**.

   The **Import Certificate** dialog box is displayed.



Import Certificate

* Certificate Type: Please select

Certificate File:

CA Certificate File:

Private Key File:

If the certificate file is generated on a storage device, the private key file will be stored on the storage device. In this case, importing the private key file is not needed.
If the certificate file is generated using OpenSSL, the private key file will be generated. In this case, import the certificate file and private key file.

2. Set **Certificate Type** to **Domain authentication certificate** and import the signed certificate and CA certificate. Table 3-21 lists the parameters and the explanations.

Table 3-21 Certificate parameters

Parameter	Description	Value
Certificate Type	Type of a certificate	[Example] Domain authentication certificate
Certificate File	Certificate file that has been exported and signed.	[Example] None
CA Certificate File	Certificate file of a server.	[Example] None
Private Key File	Private key file of a device.	[Example] None

3. Click **OK**.

   The **Warning** dialog box is displayed.

4. Carefully read the content of the dialog box, select **I have read and understand the consequences associated with this operation**, and click **OK**.

   The **Success** dialog box is displayed.

5. Click **OK**.

   The certificate has been successfully imported and activated.

----End

3.9.1.7 Configuring a Storage System to Add It to an NIS Domain

This section describes how to add a storage system to an NIS domain.

3.9.1.7.1 Preparing Data of the NIS Domain Environment

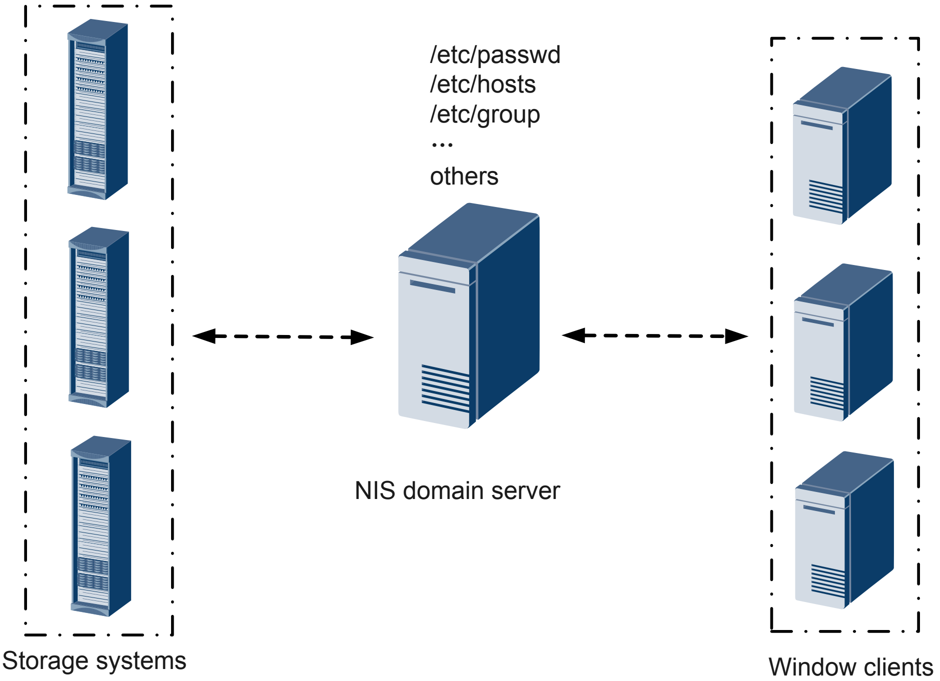
Configuration data of NIS servers needs to be collected in advance to add storage systems to the NIS domain.

Why NIS Domains?

In the UNIX shared mode, all nodes that provide the sharing service need to maintain related configuration files such as **/etc/hosts** and **/etc/passwd**. As a result, great efforts are required to maintain these configuration files. For example, if you add a new node to the shared network, all UNIX-based systems need to update their **/etc/hosts** files to include the name of the new node. The new node may need to access all other nodes, so all the systems need to modify their **/etc/passwd** files. The above operations are time-consuming and tedious when the number of nodes are more than 10.

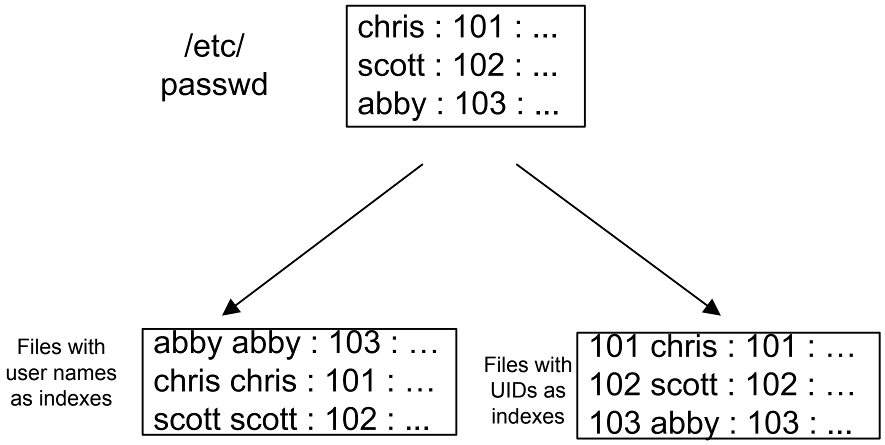
The network information service (NIS) developed by SUN Microsystem uses a single system (NIS server) to manage and maintain the files containing information about host names and user accounts, providing references for all the systems configured as NIS clients. When NIS is used, if you want to add a host to the shared network, you only need to modify a related file on the NIS server and transfer the modification to other nodes on the network.

The following figure shows the relationship between the NIS server and other hosts.



Working Principles

When NIS is configured, the ASCII files in the NIS domain are converted to NIS database files (or mapping table files). Hosts in the NIS domain query and parse the NIS database files to perform operations such as authorized access and updates. For example, common password file **/etc/passwd** of a UNIX host is converted to the following NIS database files:



Parameters

An NIS domain is a logical group of nodes that use the same NIS. A physical network includes multiple NIS domains and nodes with the same domain name belong to one NIS domain.

NIS domain–related files are saved in a subdirectory of **/var/yp** on the NIS server. The subdirectory name corresponds to the NIS domain name, for example, the files mapped to the **research** domain are saved in **/var/yp/research**.

The system super administrator can run the **/usr/bin/domainname** command to rename a domain in interactive mode. Common users can run the **domainname** command without parameters to obtain the default domain name of the local system.

Data Preparation Checklist

In order to add the storage system to NIS domain environment smoothly, for the data that needs to be used in the configuration process, prepare in advance or plan according to the actual situation. **Table 3-22** describes the data to be obtained before configuration.

Table 3-22 Data to be obtained

Item	How to Obtain/Example
Domain Name *Domain name of a server which contains 1 to 63 letters, digits, and hyphens (-), and cannot start or end with a hyphen (-). The domain names of different levels contain a maximum of 63 characters and must be separated by periods (.).*	Contact the administrator of the domain server. [Example] test.com
Primary Server Address *IP address or domain name of primary NIS domain server.*	Contact the administrator of the domain server. [Example] 192.168.0.100 www.test.com
Standby Server Address 1 (Optional) *IP address or domain name of standby NIS server 1.*	Contact the administrator of the domain server. [Example] 192.168.0.101 www.test.com
Standby Server Address 2 (Optional) *IP address or domain name of standby NIS server 2.*	Contact the administrator of the domain server. [Example] 192.168.0.102 www.test.com

3.9.1.7.2 Configuring NIS Domain Authentication Parameters

If an NIS domain server is deployed on the customers' network, add the system to the NIS domain. After the system is added to the NIS domain, the NIS domain server can authenticate NFS clients when they attempt to access the system share resources.

Prerequisites

- An NIS domain has been set up.
- Associated configurations have been completed, and required data is ready.

NOTE

- The 2000, 5000 and 6000 series storage systems can be connected to the NIS server through the management network port or the service network port (logical port). If the storage system communicates with the NIS server through the management network port, the management network port of each controller must be connected properly to the NIS server. If the storage system communicates with the NIS server through the service network port, the service network port of each controller under each vStore must be connected properly to the NIS server, ensuring that the services related to the NIS server can be normally used. You are advised to use the service network port to connect to the NIS server.
- The 18000 series storage systems can be connected to the NIS server through the service port (logical port) only. And it requires all the controllers can communicate with the NIS server.
- The storage system can be connected to only one NIS server.

Precautions

To avoid security risks generated during data transmission between the client and NIS domain server, you are advised to use a highly secure authentication mode, such as LDAP over SSL (LDAPS) or AD domain+Kerberos authentication, or adopt physical isolation or end-to-end encryption.

Procedure

Step 1 Log in to DeviceManager.

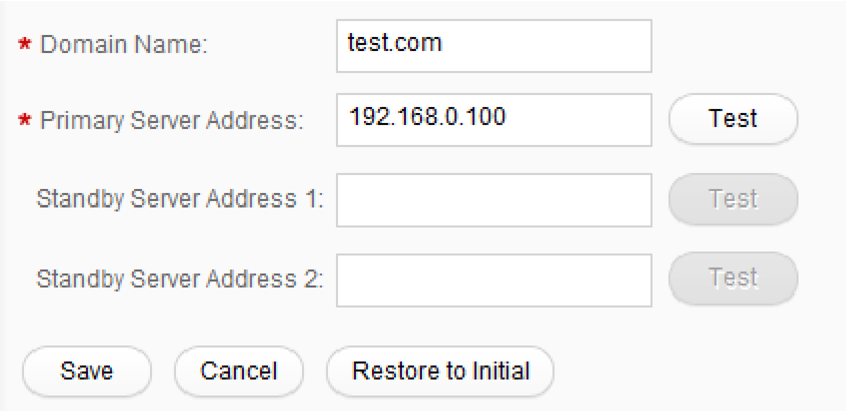
Step 2 Choose **Settings** > **Storage Settings** > **File Storage Service** > **Domain Authentication**.

Step 3 Select **Enable** to enable the NIS domain authentication.

NOTE

NIS domain authentication does not support the transfer of encrypted data. Therefore, NIS domain authentication may cause security risks.

Step 4 In the **NIS Domain Settings** area, configure the NIS domain authentication parameters. The related parameters are shown in **Table 3-23** below.



* Domain Name: test.com

* Primary Server Address: 192.168.0.100

Standby Server Address 1:

Standby Server Address 2:

Table 3-23 Parameters of the NIS domain

Parameter	Description	Value
Domain Name	Domain name of a server.	[Rule] The domain name contains 1 to 63 characters including letters, digits, underscores (_), and hyphens (-), and cannot start or end with a hyphen (-) or an underscore (_). It can contain multiple levels of domain names. A domain name at each level can contain a maximum of 63 characters. Domain names at various levels are separated by periods (.), (.) cannot be at the beginning or end. [Example] test.com
Primary Server Address	IP address or domain name of primary NIS domain server. **NOTE** ● Ensure that the IP address or domain name is reachable. Otherwise, user authentication commands and network commands will time out. ● Click **Test** to check the connectivity of the entered IP address or domain name.	[Example] 192.168.0.100 www.test.com
Standby Server Address 1	IP address or domain name of standby NIS server 1. **NOTE** ● Ensure that the IP address or domain name is reachable. Otherwise, user authentication commands and network commands will time out. ● Click **Test** to check the connectivity of the entered IP address or domain name.	[Example] 192.168.0.101 www.test.com

Parameter	Description	Value
Standby Server Address 2	IP address or domain name of standby NIS server 2. **NOTE** ● Ensure that the IP address or domain name is reachable. Otherwise, user authentication commands and network commands will time out. ● Click **Test** to check the connectivity of the entered IP address or domain name.	[Example] 192.168.0.102 www.test.com

Step 5 Click **Save**. The NIS domain authentication configuration is completed.

NOTE

Click **Restore to Initial** to initialize the NIS domain authentication.

----End

3.9.1.8 (Optional) Configuring the NFSv4 Service to Enable It to Be Used in a Non-Domain Environment

This section describes how to configure the NFSv4 service to enable it to be used in a non-domain environment.

Background

According to the NFSv4 standard protocol, the NFSv4 service must be used in a domain environment to ensure that the NFSv4 service functions properly. However, if you want to use the NFSv4 service in a non-domain environment, configure the **user name@domain name** mapping mechanism used by the NFSv4 service on your client. After the configuration is complete, the NFSv4 service will use UIDs and GIDs to transfer information about files during service transactions between your storage system and client.

Risks

- In scenarios where the NFSv4 service is used in a non-domain environment, the user authentication method of the NFSv4 service is the same as that of the NFSv3 service. The method cannot meet the theoretical security requirements of the NFSv4 standard protocol.
- Users mapped by each client depend on the configuration files of client users and user groups. Users of each client and the configuration file of each user group must be independently maintained for proper mapping.
- UIDs and GIDs must be used when ACLs of non-root users and non-root user groups are configured. Otherwise, the configuration will fail.

You are advised not to use the NFSv4 service on a non-domain environment.

Configuration on the Client

Step 1 Run the **echo 1 > /sys/module/nfs/parameters/nfs4_disable_idmapping** command.

Step 2 Run the **cat /sys/module/nfs/parameters/nfs4_disable_idmapping** command. If **Y** is displayed in the command output, the configuration is successful.

⚠ **NOTICE**

If you have used the NFSv4 service to mount NFS shares before configuring the NFSv4 service to enable compatibility between the service and a non-domain environment, mount the NFS shares again after configuring the NFSv4 service.

----End

3.9.1.9 Creating an NFS Share

This section describes how to create an NFS share. After an NFS share is created, the applicable shared file system is accessible to clients that run the OS such as SUSE, Red Hat, HP-UNIX, Sun Solaris, IBM AIX, and Mac OS.

Prerequisites

- Associated configurations have been completed, and required data is ready.
- Logical port has been created.
- The NFS service has been enabled.

Procedure

Step 1 Log in to DeviceManager.

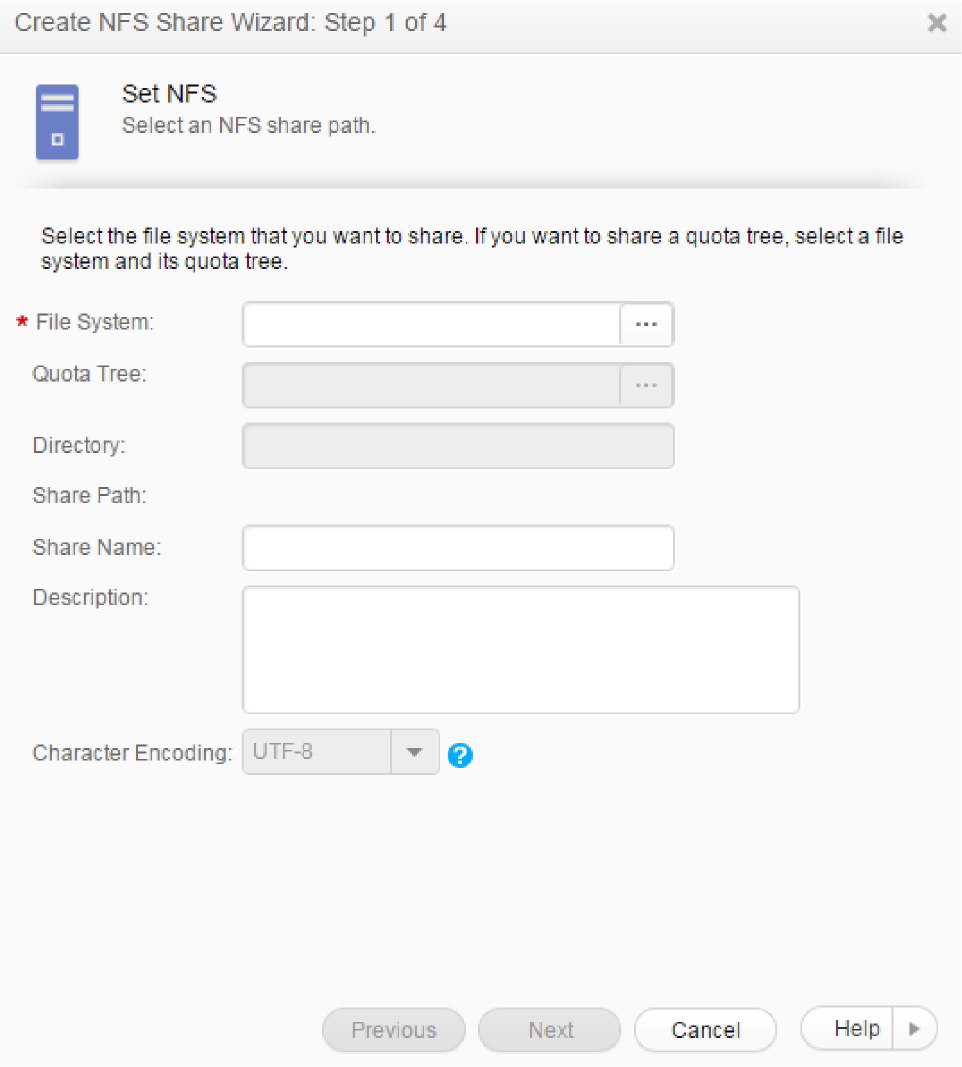
Step 2 Choose **Provisioning** > **Share** > **NFS (Linux/UNIX/MAC)**.

Step 3 Click **Create**.

The **Create NFS Share** dialog box is displayed.

Step 4 Set NFS share path.

Table 3-24 describes the related parameters.



Create NFS Share Wizard: Step 1 of 4

Set NFS

Select an NFS share path.

Select the file system that you want to share. If you want to share a quota tree, select a file system and its quota tree.

* File System:

Quota Tree:

Directory:

Share Path:

Share Name:

Description:

Character Encoding: UTF-8

Table 3-24 Parameters for creating an NFS share

Parameter	Description	Value
File System	File system for which you want to create an NFS share. **NOTICE** If the selected file system is the secondary end of the remote replication or HyperVault, data in the file system is probably being modified when it is accessed. Before performing this operation, confirm that the application allows possible data inconsistency. **NOTE** When global root directory / is selected for **File System**, you can create an NFS GNS share (Applicable to V300R006C10). ● Each vStore can only create one GNS and the share name must be /. ● You must add an independent share for the file system. After the share is added, this file system will not be displayed if a host is only authorized to access / but not the file system. ● GNS root directory / only has read permissions. You cannot create, modify, delete directories or files under /, or modify directory attributes of /. Permission will change to the share permission of a file system once the directory of the file system is entered. ● If GNS is not created, root directory / cannot be mounted to NFSv3. Only shared file systems can be viewed when NFSv4 is mounted with root directory /. ● If GNS is created in the primary vStore of HyperMetro, you can only create a vStore pair when the secondary storage has the same version as that of the primary storage. If a vStore pair is created, you can create a GNS share only when the version of the primary and secondary storage systems is the same and is V3R6C01 or later.	[Example] FileSystem001
Quota Tree	Level-1 directory under the root directory of the file system. **NOTE** Quota Tree is not supported for creating GNS.	To share a quota tree, click ... and select a quota tree you want to share. [Example] share

<table>
<tr><th>Parameter</th><th>Description</th><th>Value</th></tr>
<tr><td>Directory</td><td>Directory or subdirectory under the file system root directory.</td><td>[Example]
Share01</td></tr>
<tr><td>Share Path</td><td>The share path of a file system consists of <b>File System</b>, <b>Quota Tree</b> and <b>Directory</b>.
<b>NOTE</b>
The default share path is / for creating GNS.</td><td>[Example]
/Filesystem001/Share/Share01</td></tr>
<tr><td>Share Name</td><td>Name used by a user for accessing the shared resources.
<b>NOTE</b>
<b>Share Name</b> cannot be set for creating GNS.</td><td>[Value range]
● The share name can contain only letters, digits, spaces, and special characters including !"#$%&'()*+-.,:;<=>?@[\]^`{_|}~. On the CLI, some characters need to be entered as escape characters. For example, \| indicates |, || indicates \, \q indicates ?, and \s indicates spaces.
● The share name must start with a slash (/).
● The share name contains 1 to 255 characters without a slash (/).</td></tr>
<tr><td>Description</td><td>Description of the created NFS share.</td><td>[Value range]
Contains 0 to 255 characters.
[Example]
Share for user 1.</td></tr>
</table>

Parameter	Description	Value
Character Encoding	Clients communicate with the storage system using codes. Codes configured on the NFS share should be the same as that of the client. These codes apply to names and metadata of shared files, but do not change the codes of file data. Codes include: ● UTF-8 International code set ● EUC-JP euc-j*[ja] code set ● JIS JIS code set ● S-JIS cp932*[ja_jp.932] code set ● ZH Simplified Chinese code set, in compliance with GB2312 ● GBK Simplified Chinese code set, in compliance with GB2312 ● EUC-TW Traditional Chinese code set, in compliance with CNS11643 ● BIG5 cp950 traditional Chinese code set ● DE German character set, in compliance with ISO8859-1 ● PT Portuguese character set, in compliance with ISO8859-1 ● ES Spanish character set, in compliance with ISO8859-1 ● FR French character set, in compliance with ISO8859-1 ● IT Italian character set, in compliance with ISO8859-1 ● KO cp949 Korean code set	[Default value] UTF-8

Parameter	Description	Value
	NOTE ● The storage system automatically lists codes supported by the file system. ● The following describes method of querying character encoding on clients (for example, in Linux): run the **locale** command to view character encoding of current system. ● **Character Encoding** cannot be set for creating GNS.	
Audit Log	After the audit function is enabled, the system can record audit logs of the shared directory. The audit log items include **Open**, **Create**, **Read**, **Write**, **Close**, **Delete**, **Rename**, **Obtain properties**, **Set properties**, **Obtain security properties** and **Set security properties**. After the audit function is enabled, by default, the system records **Create**, **Write**, **Delete**, and **Rename** operations of the shared directory. **NOTE** Audit Log is not supported for creating GNS.	[Default value] Disabled

Step 5 Click **Next**.

The **Set Permissions** page is displayed.

Step 6 **Optional:** Set permissions for NFS share.

1. Select a client that you want to set NFS share in **Client List**.

   Click **Add** to create a client if there is no one in the client list. For details, refer to **Adding an NFS Share Client**.

   NOTE

   Permission information cannot be set for creating GNS.

2. Click **Next**.

Step 7 Confirm that you want to create the NFS share.

1. Confirm your settings of the NFS share to be created, and click **Finish**.

   The **Execution Result** dialog box is displayed indicating that the operation succeeded.

2. Click **Close**.

----End

3.9.1.10 Adding an NFS Share Client

An NFS share client enables client users to access shared file systems using a network.

Prerequisites

- Associated configurations have been completed, and required data is ready.
- Create an available host name on the DNS in advance if you need to add a client of **Host** type.
- Create an available network group name on the LDAP or NIS server in advance if you need to add a client of **Network Group** type.

Procedure

Step 1 Log in to DeviceManager.

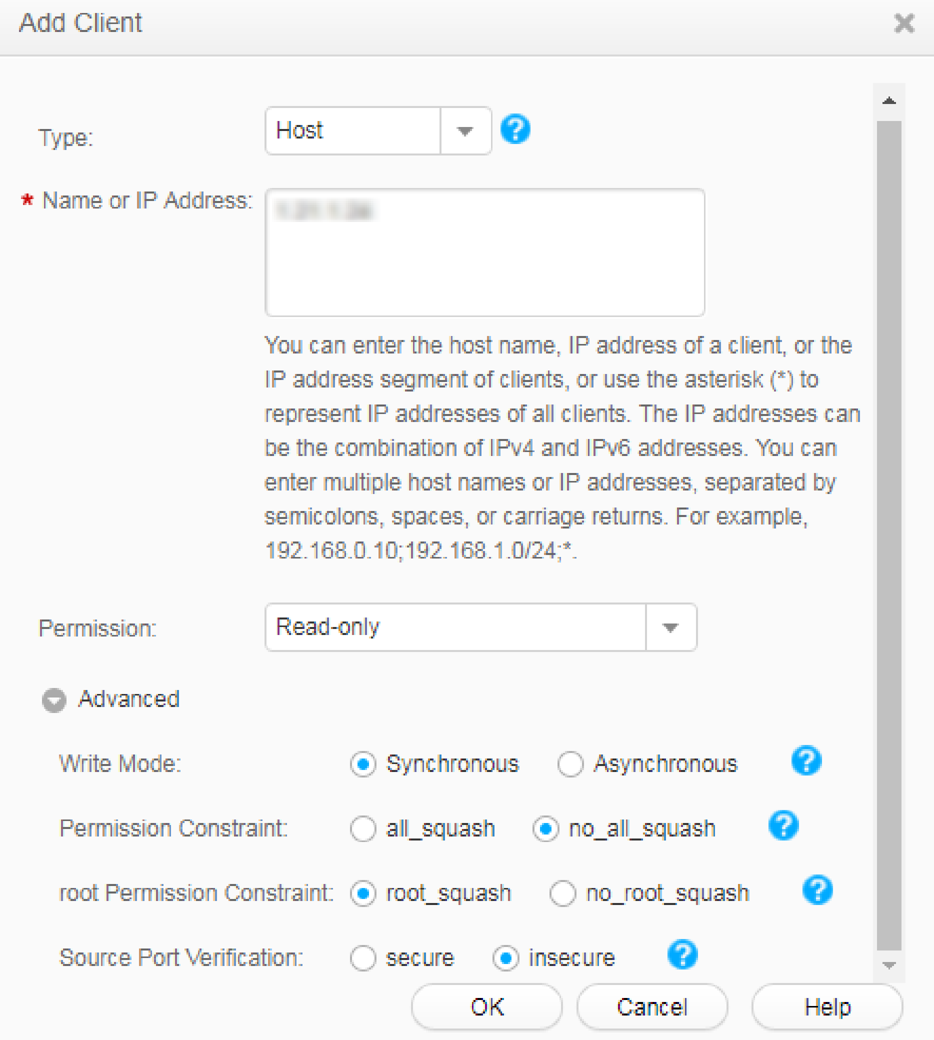
Step 2 Choose **Provisioning** > **Share** > **NFS (Linux/UNIX/MAC)**.

Step 3 Select the NFS share for which you want to add a client.

Step 4 In the **Client List** area, click **Add**.

The **Add Client** dialog box is displayed.

Step 5 Configure the client properties. **Table 3-25** describes related parameters.



Add Client

Type: Host

* Name or IP Address: [redacted]

You can enter the host name, IP address of a client, or the IP address segment of clients, or use the asterisk (*) to represent IP addresses of all clients. The IP addresses can be the combination of IPv4 and IPv6 addresses. You can enter multiple host names or IP addresses, separated by semicolons, spaces, or carriage returns. For example, 192.168.0.10;192.168.1.0/24;*.

Permission: Read-only

Advanced

Write Mode: ● Synchronous ○ Asynchronous

Permission Constraint: ○ all_squash ● no_all_squash

root Permission Constraint: ● root_squash ○ no_root_squash

Source Port Verification: ○ secure ● insecure

Table 3-25 NFS share client properties

Parameter	Description	Value
Type	Client type of the NFS share. Types include: ● Host Applicable to the client in non-domain environment. ● Network group Applicable to client in LDAP or NIS domain. **NOTE** When a client is included in multiple share permissions, the priority of share authentication from high to low is in the following sequence: host name > IP address > IP network > wildcard > network group > * (anonymous).	[Default value] Host

Parameter	Description	Value
Name or IP Address	Name or service IP address of the NFS share client. **NOTE** This parameter is available only when the **Type** is **Host**.	[Value range] You can enter multiple names or IP addresses of clients, separated by semicolons, spaces, or carriage returns. The host name or IP address contains a maximum of 256,000 characters. The name: ● Contains 1 to 255 characters, including letters, digits, hyphens (-), periods (.), and underscores (_). ● The value can begin with only a digit or letter and cannot end with a hyphen (-) or an underscore (_). ● The value cannot contain consecutive periods (.), pure digits, or a period before or after an underscore or hyphen, for example, "_.", "._", ".-", or "-.". The IP address: ● You can enter a single client IP address or a client IP address segment, or use the asterisk (*) to represent IP addresses of all client IP address. ● You can enter IPv4, IPv6 or their mixed IP address. ● The mask of IPv4 ranges from 1 to 32. The prefix of IPv6 ranges from 1 to 128. [Example] 192.168.0.10 192.168.0.10;192.168.1.0/24
Network Group Name	Network group name in LDAP or NIS domain. **NOTE** This parameter is available only when the **Type** is **Network group**.	[Value range] The name: ● Contains 1 to 254 characters. ● Can contain only letters, digits, underscores (_), periods (.), and hyphens (-). [Example] a123456

Parameter	Description	Value
Permission	The permission for client to access the NFS share. The permissions include: ● Read-only Only reading the files in the share is allowed. ● Read-write Any operation is allowed.	[Default value] Read-only
Write Mode (Optional)	Write mode of the NFS share client. The modes include: ● Synchronous: the data written to the share is written into the disk immediately. ● Asynchronous: the data written to the share is written into the cache first, then into the disk. **NOTE** The asynchronous write mode delivers higher write performance. However, if the client and storage system fail at the same time, there are data loss risks.	[Default value] Synchronous
Permission Constraint (Optional)	Determine whether to retain the user identity (UID) and group ID (GID) of a shared directory. ● all_squash: The user ID (UID) and group ID (GID) of a shared directory are mapped to user **nobody** and are applicable to public directories. ● no_all_squash: The UID and GID of a shared directory are reserved.	[Default value] no_all_squash

Parameter	Description	Value
Root Permission Constraint (Optional)	Control the root permission of a client. ● root_squash: The client cannot access the storage system as user **root**. If a client accesses the storage system as user root, the client will be mapped as user **nobody**. ● no_root_squash: A client can access the storage system as user root and user **root** can fully manage and access the root directory. **NOTE** If you want to create VMs in an NFS share, **root Permission Constraint** must be **no_root_squash**. Otherwise, the VMs may not run properly.	[Default value] root_squash
Source Port Verification (Optional)	Determine whether to enable source port verification. ● secure: If secure is selected, clients can use ports 1 to 1023 to access NFS shares. ● insecure: If insecure is selected, clients can use any port to access NFS shares.	[Default value] secure

Step 6 Confirm the addition of the NFS Share Client.

1. Click **OK**.

   The **Execution Result** dialog box is displayed, indicating that the operation succeeded.

2. Click **Close**.

----End

3.9.1.11 Accessing NFS Share

This section describes how a client accesses an NFS share. The operating systems that support the client in accessing NFS shares include SUSE, Red Hat, HP-UX, SUN Solaris, IBM AIX, and Mac OS, etc. Operations used by a client to access an NFS share in an LDAP domain and NIS domain are the same as those used in a non-domain environment.

Accessing an NFS Share by a SUSE or Red Hat Client

NOTE

When Red Hat 7 is used to mount NFS, change the TCP connection cache size to improve NFS transfer performance.

1. Run the **vi /etc/sysctl.conf** command to edit the **sysctl.conf** file.
2. In the **sysctl.conf** file, add the following contents:
```
net.ipv4.tcp_wmem = 10485760 10485760 10485760
net.ipv4.tcp_rmem = 10485760 10485760 10485760
```
3. If the file is modified for the first time, run the **sysctl -p** command or restart the system to make the modification effective.

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

Step 2 Run **showmount -e** *ipaddress* to view available NFS shares of the storage system.

ipaddress represents the logical IP address of the storage system. **172.16.128.10** is used as an example.

```
#showmount -e 172.16.128.10
Export list for 172.16.128.10
/nfstest *
#
```

NOTE

- **/nfstest** in the output represents the **Share Name** of the NFS share created in the storage system. If GNS is created, you can see /.
- If SmartMulti-Tenant is configured for a storage system and the type of service IP addresses is IPv6, the **showmount -e** *ipaddress* command cannot be executed on a client to check the NFS shares of the storage system. You must log in to the management interface of the storage system to query the NFS shares.

Step 3 Run **mount -t nfs -o vers=n,proto=m,rsize=o,wsize=p,hard,intr,timeo=q** *ipaddress*:*sharename* **/mnt** to mount the NFS share. Table 3-26 describes the related parameters.

sharename represents the **Share Name** of the NFS share created in the storage system.

```
#mount -t nfs -o vers=3,proto=tcp,rsize=1048576,wsize=1048576,hard,intr,timeo=600
172.16.128.10:/nfstest /mnt
```

NOTE

You can run the following commands to mount GNS:

```
#mount -t nfs -o vers=3,proto=tcp,rsize=1048576,wsize=1048576,hard,intr,timeo=600
172.16.128.10:/ /mnt
```

Table 3-26 SUSE/Red Hat mount NFS shares parameters

Parameter	Description	Example
o	Option that nfs mount, including **ro**, **rw** and so on. ● ro: Mount a share that is read-only. ● rw: Mount a share that can be read and written.	The default value is **rw**.

Parameter	Description	Example
vers	The NFS version. The value can be **3** or **4**.	In a scenario where the NFSv4 sharing protocol is used, a single-controller switchover may interrupt services. In environment that requires high reliability, you are advised to use NFSv3.
proto	The transfer protocol. The value can be **tcp** or **udp**.	tcp
rsize	The number of bytes NFS uses when reading files from an NFS server. The unit is byte.	**1048576** and **16384** for Red Hat 7 are recommended.
wsize	The number of bytes NFS uses when writing files to an NFS server. The unit is byte.	Recommended to use **1048576**
timeo	The retransmission interval upon timeout. The unit is one tenth of a second.	Recommended to use **600**

Step 4 Run **mount** to verify that the NFS share has been mounted to the local computer.

```
#mount
172.16.128.10:/nfstest on /mnt type nfs
(rw,vers=3,proto=tcp,rsize=1048576,wsize=1048576,hard,intr,timeo=600,addr=172.16.1
28.10)
```

NOTE

If GNS is mounted, the following information is displayed:

```
#mount
172.16.128.10:/ on /mnt type nfs
(rw,vers=3,proto=tcp,rsize=1048576,wsize=1048576,hard,intr,timeo=600,addr=172.16.1
28.10)
```

When the previous output appears, the NFS share has been successfully mounted to the local computer. If the actual output differs from the previous output, contact technical support engineers.

----End

Accessing an NFS Share by an HP-UX or SUN Solaris Client

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

Step 2 Run **showmount -e** *ipaddress* to view available NFS shares of the storage system.

ipaddress represents the logical IP address of the storage system. **172.16.128.10** is used as an example.

```
#showmount -e 172.16.128.10
Export list for 172.16.128.10
/nfstest *
#
```

NOTE

- **/nfstest** in the output represents the **Share Name** of the NFS share created in the storage system. If GNS is created, you can see /.
- If SmartMulti-Tenant is configured for a storage system and the type of service IP addresses is IPv6, the **showmount -e** *ipaddress* command cannot be executed on a client to check the NFS shares of the storage system. You must log in to the management interface of the storage system to query the NFS shares.

Step 3 Run **mount** [**-F nfs**|**-f nfs**] **-o vers=n,proto=m** *ipaddress*:*sharename* **/mnt** to mount the NFS share. **Table 3-27** describes the related parameters.

sharename represents the **Share Name** of the NFS share created in the storage system.

```
#mount -f nfs -o vers=3,proto=tcp 172.16.128.10:/nfstest /mnt
```

NOTE

You can run the following commands to mount GNS:

```
#mount -f nfs -o vers=3,proto=tcp 172.16.128.10:/ /mnt
```

Table 3-27 HP-UX or SUN Solaris mount NFS shares parameters

Parameter	Description	Example
-F nfs or -f nfs	Optional.	**-F nfs** is available to the HP-UX client and **-f nfs** to the Solaris client.
vers	The NFS version. The value can be **3** or **4**.	In a scenario where the NFS v4 sharing protocol is used, a single-controller switchover may interrupt services. In environment that requires high reliability, you are advised to use NFSv3.
proto	The transfer protocol. The value can be **tcp** or **udp**.	tcp

Step 4 Run **mount** to verify that the NFS share has been mounted to the local computer.

```
#mount
172.16.128.10:/nfstest on /mnt type nfs (rw,vers=3,proto=tcp,addr=172.16.128.10)
```

NOTE

If GNS is mounted, the following information is displayed:

```
#mount
172.16.128.10:/ on /mnt type nfs (rw,vers=3,proto=tcp,addr=172.16.128.10)
```

When the previous output appears, the NFS share has been successfully mounted to the local computer. If the actual output differs from the previous output, contact technical support engineers.

----End

Accessing an NFS Share by an IBM AIX Client

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

Step 2 Run **showmount -e** *ipaddress* to view available NFS shares of the storage system.

ipaddress represents the logical IP address of the storage system. **172.16.128.10** is used as an example.

```
#showmount -e 172.16.128.10
Export list for 172.16.128.10
/nfstest *
#
```

NOTE

- **/nfstest** in the output represents the **Share Name** of the NFS share created in the storage system. If GNS is created, you can see /.
- If SmartMulti-Tenant is configured for a storage system and the type of service IP addresses is IPv6, the **showmount -e** *ipaddress* command cannot be executed on a client to check the NFS shares of the storage system. You must log in to the management interface of the storage system to query the NFS shares.

Step 3 Run **mount** *ipaddress*:*sharename* **/mnt** to mount the NFS share.

sharename represents the **Share Name** of the NFS share created in the storage system.

```
#mount 172.16.128.10:/nfstest /mnt
mount: 1831-008 giving up on:
172.16.128.10:/nfstest
Vmount: Operation not permitted.
#
```

NOTE

You can run the following commands to mount GNS:

```
#mount 172.16.128.10:/ /mnt
mount: 1831-008 giving up on:
172.16.128.10:/
Vmount: Operation not permitted.
#
```

NOTE

If the AIX client fails to mount the NFS share after the command is executed, this is because the default NFS ports of AIX and Linux are inconsistent. Run the following command to solve this problem.

```
#nfso -o nfs_use_reserved_ports=1
Setting nfs_use_reserved_ports to 1
```

Step 4 Run **mount** to verify that the NFS share has been mounted to the local computer.

```
#mount
172.16.128.10:/nfstest on /mnt type nfs (rw,addr=172.16.128.10)
```

NOTE

If GNS is mounted, the following information is displayed:

```
#mount
172.16.128.10:/ on /mnt type nfs (rw,addr=172.16.128.10)
```

When the previous output appears, the NFS share has been successfully mounted to the local computer. If the actual output differs from the previous output, contact technical support engineers.

----End

Accessing an NFS Share by a Mac OS Client

Step 1 Run **showmount -e** *ipaddress* to view available NFS shares of the storage system.

ipaddress represents the logical IP address of the storage system. **172.16.128.10** is used as an example.

```
Volumes root# showmount -e 172.16.128.10
/nfstest *
```

NOTE

- **/nfstest** in the output represents the **Share Name** of the NFS share created in the storage system. If GNS is created, you can see /.
- If SmartMulti-Tenant is configured for a storage system and the type of service IP addresses is IPv6, the **showmount -e** *ipaddress* command cannot be executed on a client to check the NFS shares of the storage system. You must log in to the management interface of the storage system to query the NFS shares.

Step 2 Run **sudo /sbin/mount_nfs -P** *ipaddress*:*sharename* **/Volumes/mount1** to mount the NFS share.

sharename represents the **Share Name** of the NFS share created in the storage system.

```
Volumes root# sudo /sbin/mount_nfs -P 172.16.128.10:/nfstest /Volumes/mount1
```

NOTE

You can run the following commands to mount GNS:

```
Volumes root# sudo /sbin/mount_nfs -P 172.16.128.10:/ /Volumes/mount1
```

Step 3 Run **mount** to verify that the NFS share has been mounted to the local computer.

```
Volumes root# mount
/dev/disk0s2 on / (hfs, local, journaled)
devfs on /dev (devfs, local)
fdesc on /dev (fdesc, union)
map -hosts on /net (autofs, automounted)
map auto_home on /home (autofs, automounted)
172.16.128.10:/nfstest on /Volumes/mount1 (nfs)
```

NOTE

If GNS is mounted, the following information is displayed:

```
Volumes root# mount
/dev/disk0s2 on / (hfs, local, journaled)
devfs on /dev (devfs, local)
fdesc on /dev (fdesc, union)
map -hosts on /net (autofs, automounted)
map auto_home on /home (autofs, automounted)
172.16.128.10:/ on /Volumes/mount1 (nfs)
```

When the previous output appears, the NFS share has been successfully mounted to the local computer. If the actual output differs from the previous output, contact technical support engineers.

----End

Accessing an NFS Share by a VMware Client

NOTE

When you want to create virtual machines on the NFS share, The **Root Permission Constraint** of the NFS share must be **no_root_squash**.

Step 1 Log in to **VMware vSphere Client**.

Step 2 Choose **Localhost** > **Configuration** > **Storage** > **Add Storage**.

The **Add Storage** wizard is displayed.

Step 3 In **Select Storage Type**, select **Network File System**. Then, click **Next**.

The **Locate Network File System** page is displayed.

Step 4 Set parameters. **Table 3-28** describes related parameters.

Table 3-28 Parameters for adding an NFS share in VMware

Parameter	Description	Value
Server	Logical IP address of the storage system.	Example 172.16.128.10
Folder	**Share Name** of the NFS share created in the storage system.	Example /nfstest **NOTE** Since the GNS root directory / only has read permissions. GNS does not apply to VMware.
Datastore Name	Name of the NFS share in VMware.	Example data

Step 5 Click **Next**.

Step 6 Confirm the information and click **Finish**.

Step 7 On the **Configuration** tab page, view the newly added NFS share.

----End

Follow-up Procedure

If you modify NFS user information when using the client to access NFS shares, new user authentication information cannot take effect immediately. Wait 30 minutes for the modification to take effect.

3.9.1.12 NFS Share Configuration Example

This section uses an example to explain how to configure an NFS share.

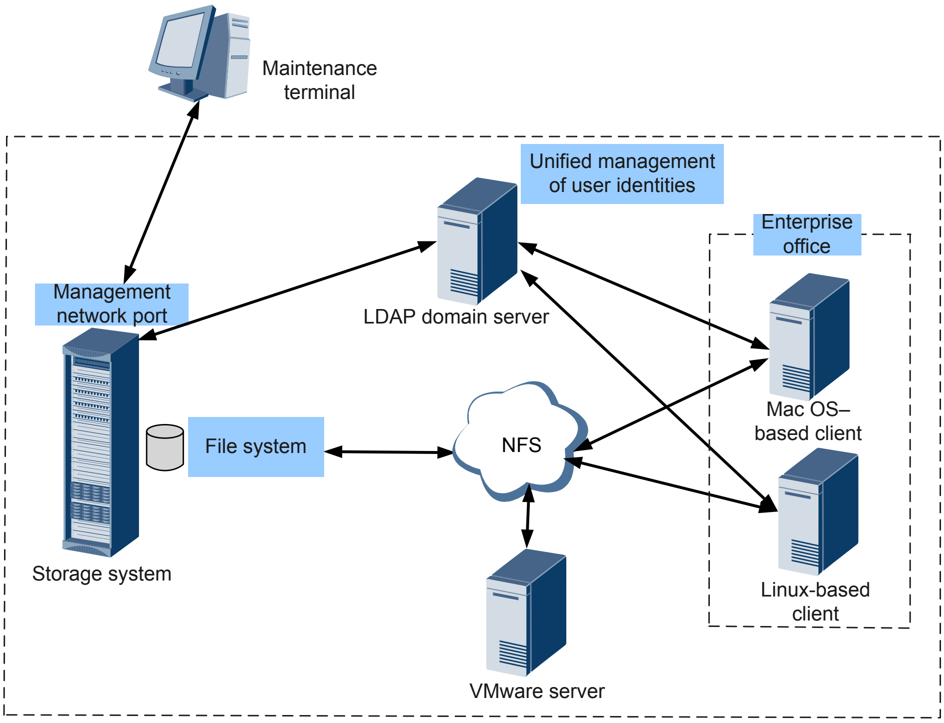
3.9.1.12.1 Scenario

A research institute has an enterprise office system and a virtual machine (VM) system. Specific storage space must be allocated to different service systems. This section describes the customer's existing environment and requirements.

Network Diagram

Figure 3-7 shows the customer's network diagram.

Figure 3-7 Customer's network diagram



The status quo of the customer's live network can be concluded as follows:

- The enterprise office system runs Linux and Mac OS, which are connected to an LDAP domain server.
- Linux-based hosts belong to network group **ldapgrouplinux**, whereas Mac OS-based hosts belong to network group **ldapgroupmac**.
- The enterprise office system, LDAP domain server, VMware server, and storage system reside on the same LAN.

Customer Requirements

The research institute wants to purchase a storage system for the enterprise office system and VM system. The storage space must be allocated as follows:

- There are two network groups (Mac and Linux) in the enterprise office system and only one network group on a VM. Each network group requires 1 TB dedicated storage space that can be read and written.
- The Mac network group and Linux network group can only access their own storage space.

3.9.1.12.2 Requirement Analysis

This section analyzes the customer's requirements and provides a solution.

The customer's requirements are analyzed as follows:

- All clients use the Linux operating system, so the storage system can employ NFS sharing to provide storage space for the two systems respectively.

- The storage system supports NFS share management in a non-domain and an LDAP domain environment.

Based on the previous analysis, a solution as follows is provided:

- Use OceanStor 5800 V3 as the storage system.
- Configure each service system as shown in **Table 3-29**.

Table 3-29 Basic information of service systems

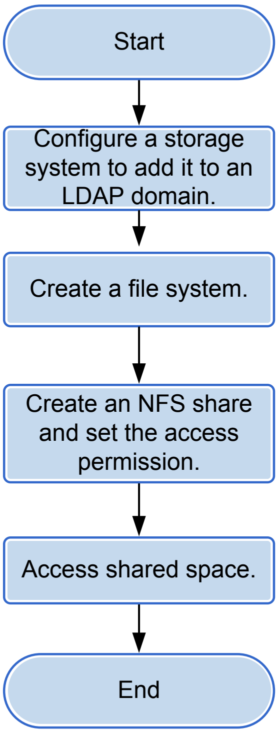
Service System	Share Path	Shared Space	User Group	IP Address
Linux-based host of the office system	/FileSystem0000	1 TB	ldapgrouplinux	-
Mac OS-based host of the office system	/FileSystem0001	1 TB	ldapgroupmac	-
VM	/FileSystem0003	1 TB	-	172.16.211.200
LDAP Server	-	-	-	172.16.211.201

3.9.1.12.3 Configuration Process

The preceding solutions and the following configuration flowchart help you understand the subsequent configuration.

Figure 3-8 shows the configuration process.

Figure 3-8 Configuration process


Start
Configure a storage system to add it to an LDAP domain.
Create a file system.
Create an NFS share and set the access permission.
Access shared space.
End

NOTE

This configuration process is only applicable to this configuration example. For the complete configuration process of NFS share, see **3.9.1.1 Configuration Process**.

3.9.1.12.4 Creating an NFS Share

After requirement analysis and service planning, you need to configure an NFS share on DeviceManager.

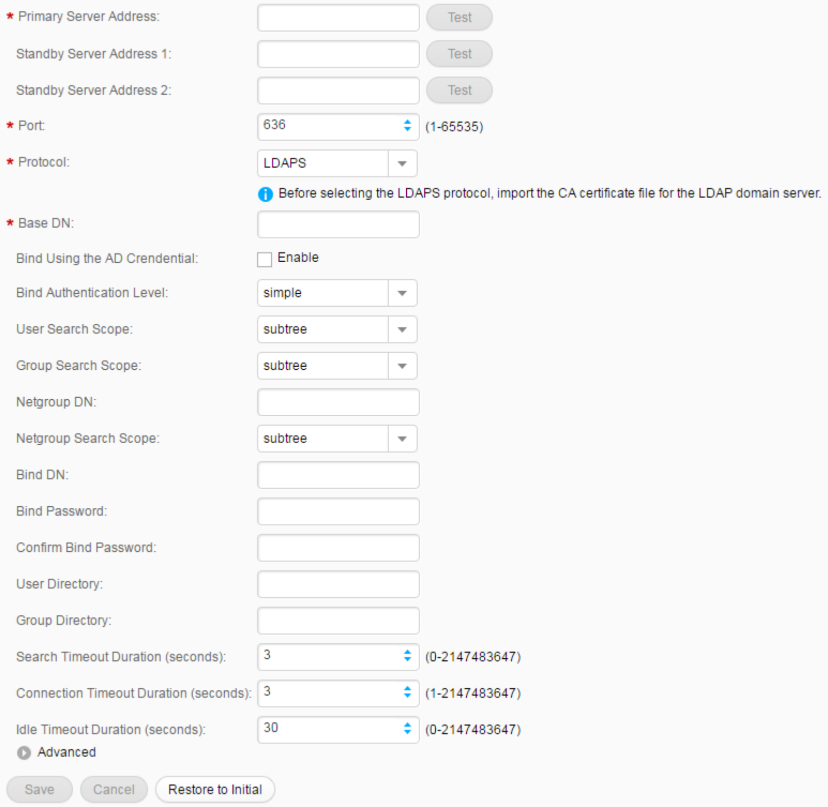
Prerequisites

The storage system and application servers can communicate with each other.

Procedure

Step 1 Configure a storage system to add it to an LDAP Domain.

On the navigation bar of the DeviceManager, select ⚙ **Settings** > **Storage Settings** > **File Storage Service** > **Domain Authentication**. Input the parameters of the LDAP domain in the **LDAP Domain Settings** area.



* Primary Server Address:

Standby Server Address 1:

Standby Server Address 2:

* Port: 636 (1-65535)

* Protocol: LDAPS

Before selecting the LDAPS protocol, import the CA certificate file for the LDAP domain server.

* Base DN:

Bind Using the AD Crendential: □ Enable

Bind Authentication Level: simple

User Search Scope: subtree

Group Search Scope: subtree

Netgroup DN:

Netgroup Search Scope: subtree

Bind DN:

Bind Password:

Confirm Bind Password:

User Directory:

Group Directory:

Search Timeout Duration (seconds): 3 (0-2147483647)

Connection Timeout Duration (seconds): 3 (1-2147483647)

Idle Timeout Duration (seconds): 30 (0-2147483647)

NOTE

Before selecting the LDAPS protocol, import the CA certificate file for the LDAP domain server.

Step 2 Create a file system.

The file system provides shared space for an NFS share.

1. On the DeviceManager page, choose **Provisioning** > **File System**.

   The **File System** page is displayed.

2. Click **Create**.

   The **Create File System** dialog box is displayed.

3. In the **Create File System** dialog box, configure planned parameters. **Table 3-30** describes related parameters.

Table 3-30 Create File System parameters

Parameter	Planned Value
Name	FileSystem
Capacity	1 TB
File System Block Size	8 KB
Quantity	3
Owning Storage Pool	StoragePool000

NOTE

– When creating multiple file systems, the storage system automatically appends a number to each file system name based on the number of file systems to be created for identification. Therefore, the file systems that are created are named FileSystem0000, FileSystem0001, and FileSystem0002 respectively.

– Because the scene is used as a virtual machine and a database, the file system block size can be set to 8KB.

4. Click **OK**.

Step 3 Create an NFS share and set the access permission. Such as share the **FileSystem001** with a Linux-based host.

1. On the DeviceManager page, choose **Provisioning** > **Share** > **NFS (Linux/UNIX/MAC)**. Click **Create**.

   The **Create NFS Share Wizard: Step 4-1** page is displayed.

2. In **File System**, select file system **FileSystem0000**.
3. Click **Next**.

   The **Create NFS Share Wizard: Step 4-2** page is displayed.

4. Click **Add**.

   The **Add Client** dialog box is displayed.

5. Set **Type** to **Network Group** and enter **ldapgrouplinux** in **Network Group Name**.
6. Click **OK**.

   The **Create NFS Share Wizard: Step 4-2** page is displayed.

7. Click **Next**.

   The **Create NFS Share Wizard: Step 4-3** page is displayed.

8. Click **Finish**.

   The **Create NFS Share Wizard: Step 4-4** page is displayed.

9. Click **Close**.

Step 4 Repeat **Step 3** to share **FileSystem0001** and **FileSystem0002** respectively with a Mac OS-based host and a VMware host.

NOTE

If **FileSystem0001** is shared with a Mac OS-based host, enter **ldapgroupmac** in **Network Group Name** in **Step 3.5**.

If **FileSystem0002** is shared with a VMware ESX-based host, enter **172.16.211.200** in **Name or IP Address** in **Step 3.5**.

----End

3.9.1.12.5 Accessing Shared Space

This section describes how the departments access shared space. After an NFS share is configured, users need to map the shared space provided by the storage system to the network drive on the client.

Procedure

Step 1 Mount the NFS share using the LDAP client that belongs to network group **ldapgrouplinux** in the LDAP domain.

1. Run the **mount -t nfs -o vers=3,proto=tcp,rsize=1048576,wsize=1048576,hard,intr,timeo=600 172.16.211.20:/FileSystem0000 /mnt** command on the Linux-based client to mount the NFS share.

```
linux-client:~ #mount -t nfs -o
vers=3,proto=tcp,rsize=1048576,wsize=1048576,hard,intr,timeo=600
172.16.211.20:/FileSystem0000 /mnt
```

   linux-client indicates the name of the LDAP client. **timeo** indicates retransmission time-out (unit: 1/10 seconds, recommended value: 600). **172.16.211.20** indicates the IP address of the logical port. **/FileSystem0000** indicates the NFS share name to be mounted. **/mnt** indicates the mount point.

2. Run the **mount** command to view the mounted share.

```
linux-client:~ # mount
172.16.211.20:/FileSystem0000 on /mnt type nfs (ro,addr=172.16.211.20)
```

   The command output indicates that the NFS share of the storage system has been successfully mounted to the Linux-based client that belongs to network group **ldapgrouplinux**.

Step 2 Mount the NFS share using the LDAP client that belongs to network group **ldapgroupmac** in the LDAP domain.

1. Run the **sudo /sbin/mount_nfs -P 172.16.211.20:/FileSystem0001 /volumes/mnt** command on the Mac OS based client to mount the NFS share.

```
Volumes root# sudo /sbin/mount_nfs -P 172.16.211.20:/FileSystem0001 /volumes/
mnt
```

   Volumes root indicates the name of the Mac OS based client that belongs to network group **ldapgroupmac**. **172.16.211.20** indicates the IP address of the logical port. **/FileSystem0001** indicates the NFS shared file system to be mounted. **/volumes/mnt** indicates the mount point.

2. Run the **mount** command to view the mounted share.

```
Volumes root# mount
/dev/disk0s2 on / (hfs, local, journaled)
devfs on /dev (devfs, local)
fdesc on /dev (fdesc, union)
map -hosts on /net (autofs, automounted)
map auto_home on /home (autofs, automounted)
172.16.211.20:/FileSystem0001 on /Volumes/mnt (nfs)
```

   The command output indicates that the NFS share of the storage system has been successfully mounted to the Mac OS-based client that belongs to network group **ldapgroupmac**.

Step 3 Mount an NFS share in VMware.

1. Log in to **VMware vSphere Client**.
2. Choose **Localhost** > **Configuration** > **Storage** > **Add Storage**.

   The **Add Storage** wizard is displayed.
3. In **Select Storage Type**, select **Network File System**. Then, click **Next**.

   The **Locate Network File System** page is displayed.
4. Set parameters. **Table 3-31** describes related parameters.

Table 3-31 Parameters for adding an NFS share in VMware

Parameter	Planned Value
Server	172.16.211.200
Folder	/FileSystem0002
Datastor Name	data

5. Click **Next**.
6. Confirm the information and click **Finish**.
7. On the **Configuration** tab page, view the newly added NFS share.

----End

3.9.1.13 NFS GNS Share Configuration Example (Applicable to V300R006C10 and Later Versions)

This section uses an example to explain how to configure an NFS GNS share.

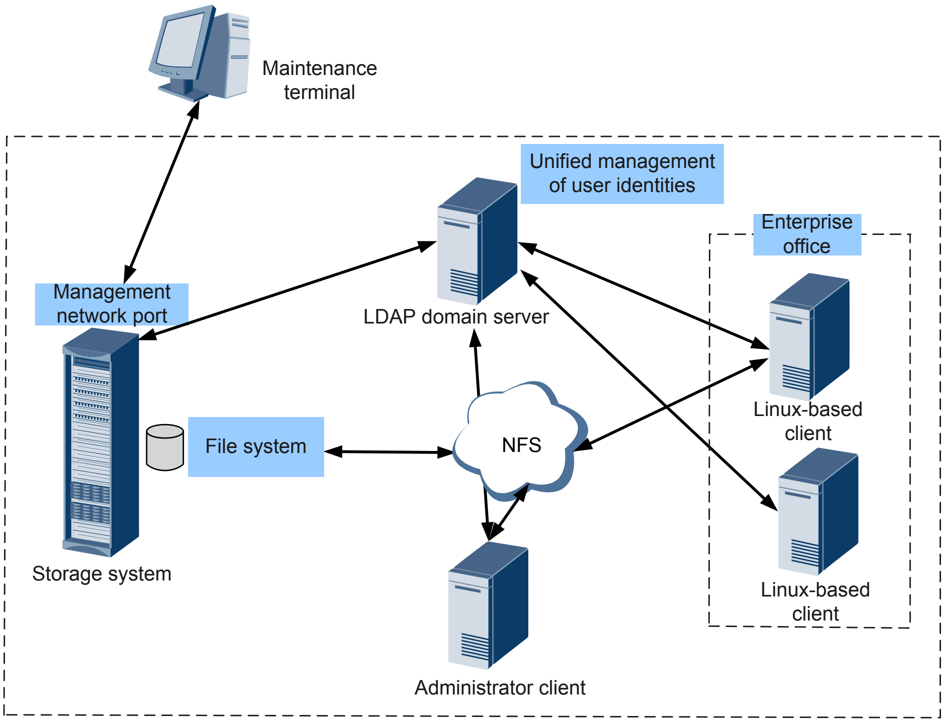
3.9.1.13.1 Scenario

To enable the administrator of an enterprise to manage all NFS share file systems in a centralized manner, the administrator must be configured with GNS share. This section describes the customer's live network environment and detailed requirements.

Network Diagram

Figure 3-9 shows the customer's network diagram.

Figure 3-9 Customer's network diagram



The status quo of the customer's live network can be concluded as follows:

- The enterprise office system and administrator system run Linux, which are connected to an LDAP domain server.
- Linux-based hosts of the office system belong to three network groups in the LDAP domain, ldapgroup1, ldapgroup2, and ldapgroup3. Administrator's hosts belong to the same network group in the LDAP domain, ldapmgr.
- The enterprise office system, administrator's host, LDAP domain server, and storage system reside on the same LAN.

Customer Requirements

The storage system purchased by the enterprise is used for the enterprise office system. The storage space must be allocated as follows:

- In the enterprise office system, there are three network groups (Linux network groups). Each network group needs 1 TB dedicated storage space and has read and write permissions.
- The administrator needs to manage all storage space.

3.9.1.13.2 Requirement Analysis

This section analyzes the customer's requirements and provides a solution.

The customer's requirements are analyzed as follows:

- All clients use the Linux operating system, so the storage system can employ NFS sharing to provide storage space for clients.
- If the administrator's host runs a Linux operating system, the NFS GNS share provided by the storage system can be used to enable the administrator to manage all NFS shared file systems directly.
- The storage system supports NFS share management in a non-domain and an LDAP domain environment.

Based on the previous analysis, a solution as follows is provided:

- Use OceanStor 5800 V3 as the storage system.
- Configure each service system as shown in **Table 3-32**.

Table 3-32 Basic information of service systems

Service System	Share Path	Shared Space	User Group	IP Address
Linux-based host of the office system	/FileSystem0000	1TB	ldapgroup1	-
Linux-based host of the office system	/FileSystem0001	1TB	ldapgroup2	-

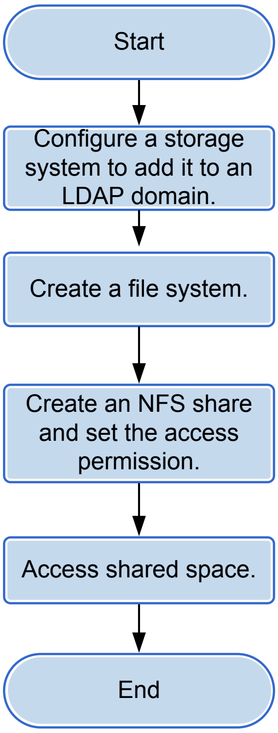
Service System	Share Path	Shared Space	User Group	IP Address
Linux-based host of the office system	/FileSystem0002	1TB	ldapgroup3	-
Administrator's Linux-based host	All shared file systems	-	ldapmgr	-
LDAP server	-	-	-	172.16.211.201

3.9.1.13.3 Configuration Process

The preceding solutions and the following configuration flowchart help you understand the subsequent configuration.

Figure 3-10 shows the configuration process.

Figure 3-10 Configuration process


Start
Configure a storage system to add it to an LDAP domain.
Create a file system.
Create an NFS share and set the access permission.
Access shared space.
End

NOTE

This configuration process is only applicable to this configuration example. For the complete configuration process of NFS share, see **3.9.1.1 Configuration Process**.

3.9.1.13.4 Creating an NFS Share

After requirement analysis and service planning, you need to configure an NFS share on DeviceManager.

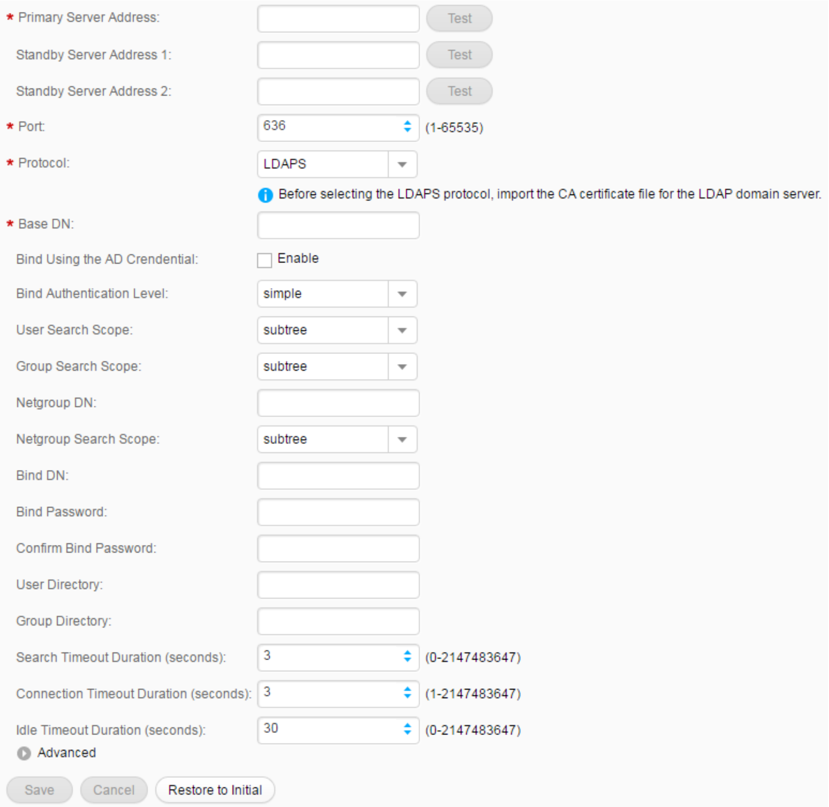
Prerequisites

The storage system and application servers can communicate with each other.

Procedure

Step 1 Configure a storage system to add it to an LDAP Domain.

On the navigation bar of the DeviceManager, select **Settings** > **Storage Settings** > **File Storage Service** > **Domain Authentication**. Input the parameters of the LDAP domain in the **LDAP Domain Settings** area.



* Primary Server Address:		Test
Standby Server Address 1:		Test
Standby Server Address 2:		Test
* Port:	636	(1-65535)
* Protocol:	LDAPS Before selecting the LDAPS protocol, import the CA certificate file for the LDAP domain server.	
* Base DN:		
Bind Using the AD Crendential:	□ Enable	
Bind Authentication Level:	simple	
User Search Scope:	subtree	
Group Search Scope:	subtree	
Netgroup DN:		
Netgroup Search Scope:	subtree	
Bind DN:		
Bind Password:		
Confirm Bind Password:		
User Directory:		
Group Directory:		
Search Timeout Duration (seconds):	3	(0-2147483647)
Connection Timeout Duration (seconds):	3	(1-2147483647)
Idle Timeout Duration (seconds):	30	(0-2147483647)

NOTE

Before selecting the LDAPS protocol, import the CA certificate file for the LDAP domain server.

Step 2 Create a file system.

The file system provides shared space for an NFS share.

1. On the DeviceManager page, choose **Provisioning** > **File System**.

   The **File System** page is displayed.

2. Click **Create**.

   The **Create File System** dialog box is displayed.

3. In the **Create File System** dialog box, configure planned parameters. **Table 3-33** describes related parameters.

Table 3-33 Create File System parameters

Parameter	Planned Value
Name	FileSystem
Capacity	1 TB
File System Block Size	8 KB
Quantity	3
Owning Storage Pool	StoragePool000

NOTE

- When creating multiple file systems, the storage system automatically appends a number to each file system name based on the number of file systems to be created for identification. Therefore, the file systems that are created are named FileSystem0000, FileSystem0001, and FileSystem0002 respectively.
- Assume the size of most files in the file system is between 100 KB and 1 MB. the file system block size can be set to 8KB.

4. Click **OK**.

Step 3 Create an NFS share and set the access permission. Such as share the **FileSystem001** with a Linux-based host.

1. On the DeviceManager page, choose **Provisioning** > **Share** > **NFS (Linux/UNIX/MAC)**. Click **Create**.

   The **Create NFS Share Wizard: Step 4-1** page is displayed.
2. In **File System**, select file system **FileSystem0000**.
3. Click **Next**.

   The **Create NFS Share Wizard: Step 4-2** page is displayed.
4. Click **Add**.

   The **Add Client** dialog box is displayed.
5. Set **Type** to **Network Group** and enter **ldapgroup1** in **Network Group Name**.
6. Click **OK**.

   The **Create NFS Share Wizard: Step 4-2** page is displayed.
7. Click **Next**.

   The **Create NFS Share Wizard: Step 4-3** page is displayed.
8. Click **Finish**.

   The **Create NFS Share Wizard: Step 4-4** page is displayed.
9. Click **Close**.

Step 4 Repeat **Step 3** to enable corresponding network groups to share **FileSystem0001** and **FileSystem0002**.

NOTE

When enabling the host of ldapgourp2 to share **FileSystem0001**, enter **ldapgroup2** for **Network Group Name** in **Step 3.5**.

When enabling the host of ldapgourp2 to share **FileSystem0002**, enter **ldapgroup3** for **Network Group Name** in **Step 3.5**.

Step 5 Repeat **Step 3** to enable the network group **ldapmgr** to share **FileSystem0000**, **FileSystem0001**, and **FileSystem0002**.

Step 6 Create an NFS GNS share.

1. On the DeviceManager, choose **Provisioning** > **Share** > **NFS (Linux/UNIX/MAC)**, and click **Create**.

   The **Create NFS Share Wizard: Step 1 of 4** dialog box is displayed.
2. Click / next to **File System**.
3. Click **Next**.

   The **Create NFS Share Wizard: Step 2 of 4** dialog box is displayed.
4. Click **Next**.

   The **Create NFS Share Wizard: Step 3 of 4** dialog box is displayed.
5. Click **Finish**.

   The **Create NFS Share Wizard: Step 4 of 4** dialog box is displayed.
6. Click **Close**.

----End

3.9.1.13.5 Accessing Shared Space

This section describes how the departments access shared space. After an NFS share is configured, users need to map the shared space provided by the storage system to the network drive on the client.

Procedure

Step 1 Mount the NFS share using the LDAP client that belongs to network group **ldapgroup1** in the LDAP domain.

1. Run the **mount -t nfs -o vers=3,proto=tcp,rsize=1048576,wsize=1048576,hard,intr,timeo=600 172.16.211.20:/FileSystem0000 /mnt** command on the Linux-based client to mount the NFS share.

```
linux-client:~ #mount -t nfs -o
vers=3,proto=tcp,rsize=1048576,wsize=1048576,hard,intr,timeo=600
172.16.211.20:/FileSystem0000 /mnt
```

   linux-client indicates the name of the LDAP client. **timeo** indicates retransmission time-out (unit: 1/10 seconds, recommended value: 600). **172.16.211.20** indicates the IP address of the logical port. **/FileSystem0000** indicates the NFS share name to be mounted. **/mnt** indicates the mount point.
2. Run the **mount** command to view the mounted share.

```
linux-client:~ # mount
172.16.211.20:/FileSystem0000 on /mnt type nfs (ro,addr=172.16.211.20)
```

The command output indicates that the NFS share of the storage system has been successfully mounted to the Linux-based client that belongs to network group **ldapgroup1**.

Step 2 Repeat **Step 1** to mount the NFS share using the LDAP client belonging to network groups **ldapgroup2** and **ldapgroup3** in the LDAP domain.

Step 3 Mount the NFS GNS share using the administrator's host belonging to the network group **ldapmgr** in the LDAP domain.

1. Mount the NFS share by running **mount -t nfs -o vers=3,proto=tcp,rsize=1048576,wsize=1048576,hard,intr,timeo=600 172.16.211.20:/ /mnt** on the administrator's Linux-based client.

```
linux-mgr:~ # mount -t nfs -o 
vers=3,proto=tcp,rsize=1048576,wsize=1048576,hard,intr,timeo=600 
172.16.211.20:/ /mnt
```

   linux-mgr indicates the name of the LDAP client, **timeo** indicates the retransmission timeout period, the unit is **1/10s** (recommended value is **600**), **172.16.211.20** indicates the IP address of the logical port in the storage system, / indicates the NFS GNS share in the storage system, and **/mnt** indicates the mounting point where the share is mounted to the client.

2. Run **mount** to check the mounted share.

```
linux-mgr:~ # mount 172.16.211.20:/ on /mnt type nfs (ro,addr=172.16.211.20)
```

3. The command output shows that the NFS GNS share has been mounted to the administrator's Linux-based client. If you access the mounted directory, you can access and view all NFS shared file systems.

```
linux-mgr:~ # ll /mnt
total 12
drwxrwxrwx 3 root root 3 Jan  9 20:08 FileSystem0000
drwxrwxrwx 3 root root 3 Jan  9 20:08 FileSystem0001
drwxrwxrwx 3 root root 3 Jan  9 20:08 FileSystem0002
```

----End

3.9.2 Configuring a CIFS Share

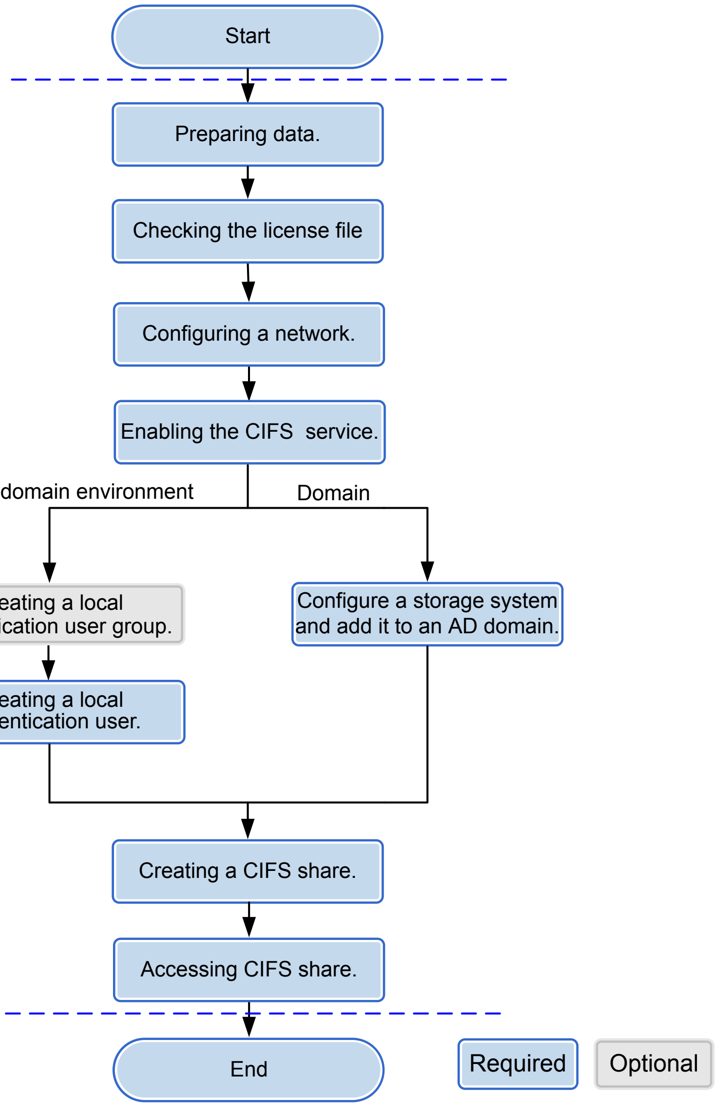
Storage system supports the CIFS share mode. By configuring a CIFS share, a user can access the shared directory.

3.9.2.1 Configuration Process

This section describes the CIFS share configuration process.

Figure 3-11 shows the CIFS share configuration process.

Figure 3-11 CIFS share configuration process


Start
Preparing data.
Checking the license file
Configuring a network.
Enabling the CIFS service.
Non-domain environment
Domain
Creating a local authentication user group.
Configure a storage system and add it to an AD domain.
Creating a local authentication user.
Creating a CIFS share.
Accessing CIFS share.
End
Required
Optional

3.9.2.2 Preparing Data

Before configuring a CIFS share, obtain information about storage system IP address, local users, quotas, permissions, and AD domain to assist in the follow-up configuration.

Table 3-34 describes preparations required for configuring a CIFS share.

Table 3-34 Preparations required for configuring a CIFS share

Item	Description	Example
Logical IP address of the storage system *Indicates a logical IP address used by a storage system to provide shared space for a client.*	-	172.16.128.10
File system *Indicates the file system for which a CIFS share is configured.*	The storage system enables you to configure a file system or its quota tree[a] as a CIFS share.	FileSystem001
Share name *Indicates the name of a CIFS share.*	The share name: ● Must contain 1 to 80 characters. ● Share name cannot contain space, double quotation mark ("), slash (/), backslash (\), square brackets ([]), larger than (<), less than (>), plus (+), colon (:), semicolon (;), comma (,), question mark (?), asterisk (*), vertical bar (|),and equal mark (=).	share_for_user1
Permission *Permission of a user or user group to access a share.*	The permission includes: ● Full control: the user can full control the CIFS share. ● Read-only: the user can only read the CIFS share. ● Read and write: the user can read and write the CIFS share. ● Forbidden: the user cannot access the CIFS share.	Read-only

Item	Description	Example
User *User that employs local authentication.*	The user name: ● Cannot contain space, double quotation mark ("), slash (/), backslash (\), square brackets ([]), less than (<), larger than (>), plus (+), colon (:), semicolon (;), comma (,), question mark (?), asterisk (*), vertical bar (|), equal mark (=), (@), or end with a period (.). ● The user name can contain case-insensitive letters. Therefore, **aaaaaaaa** and **AAAAAAAA** cannot be created at the same time. ● The user name cannot be the same as the name of the local authentication user group. ● Contains 8 to 32 characters by default. NOTE You can modify the minimum length of user name in **More** > **Set Security Policies**. NOTE You cannot use the user accounts retained in the system, including: ● User accounts retained in Windows: **Everyone**, **Local**, **Creator Owner**, **Creator Group**, **Creator Owner Server**, **Creator Group Server**, **Owner Rights**, **Group Rights**, **NT Pseudo Domain**, **Dialup**, **Network**, **Batch**, **Interactive**, **Service**, **Anonymous Logon**, **Proxy**, **Enterprise Domain Controllers**, **Self**, **Authenticated Users**, **Restricted**, **Terminal Server User**, **Remote Interactive Logon**, **This Organization**, **System**, **Local Service**, **Network Service**, **Write Restricted**, **Other Organization**, **Builtin**, **Internet$**, **Members can fully administer the computer/domain**, **Users**, **Guests**, **Power Users**, **Members can share directories**, **Account Operators**, **Server Operators**, **Print Operators**, **Backup Operators**, **Members can bypass file security to back up files**, **Replicator**, **Current Owner**, **Current Group**. ● User accounts retained in Linux: **root**, **nogroup**, **nobody**, **ftp**, **anonymous**, **daemon**, **nobody**, **news**, **sshd**, **messagebus**. ● User accounts retained in a storage system: **ibc_os_hs**.	test_user01

Item	Description	Example
User group *User group that employs local authentication.*	The user group name: ● For V300R006C00: – Must contain 1 to 32 characters. – Cannot contain space, double quotation mark ("), slash (/), backslash (\), square brackets ([]), larger than (<), less than (>), plus (+), colon (:), semicolon (;), comma (,), question mark (?), asterisk (*), vertical bar (|), equal mark (=), (@), or end with a period (.). – The user group name can contain case-insensitive letters. Therefore, **aa** and **AA** cannot be created at the same time. – The user group name cannot be the same as the name of the local authentication user. ● For V300R006C10: – The user group name cannot contain the quotation mark ("), slash (/), backslash (\), square brackets ([]), less than sign (<), larger than sign (>), plus sign (+), colon (:), semicolon (;), comma (,), question mark (?), asterisk (*), vertical bar (|), equal sign (=), at sign (@) or end with a period (.). If the user group name start and end with spaces, the spaces are not displayed after the user group name is created. – The user group name can contain case-insensitive letters. Therefore, **aa** and **AA** cannot be created at the same time. – The user group name cannot be the same as the name of the local authentication user. – The user group name contains 1 to 63 characters.	default_group

Item	Description	Example
	NOTE You cannot use the user accounts retained in the system, including: ● User accounts retained in Windows: ● For V300R006C00: **Everyone**, **Local**, **Creator Owner**, **Creator Group**, **Creator Owner Server**, **Creator Group Server**, **Owner Rights**, **Group Rights**, **NT Pseudo Domain**, **Dialup**, **Network**, **Batch**, **Interactive**, **Service**, **Anonymous Logon**, **Proxy**, **Enterprise Domain Controllers**, **Self**, **Authenticated Users**, **Restricted**, **Terminal Server User**, **Remote Interactive Logon**, **This Organization**, **System**, **Local Service**, **Network Service**, **Write Restricted**, **Other Organization**, **Builtin**, **Internet$**, **Members can fully administer the computer/domain**, **Users**, **Guests**, **Power Users**, **Members can share directories**, **Account Operators**, **Server Operators**, **Print Operators**, **Backup Operators**, **Members can bypass file security to back up files**, **Replicator**, **Current Owner**, **Current Group**. ● For V300R006C10: **Everyone**, **Local**, **Creator Owner**, **Creator Group**, **Creator Owner Server**, **Creator Group Server**, **Owner Rights**, **Group Rights**, **NT Pseudo Domain**, **Dialup**, **Network**, **Batch**, **Interactive**, **Service**, **Anonymous Logon**, **Proxy**, **Enterprise Domain Controllers**, **Self**, **Authenticated Users**, **Restricted**, **Terminal Server User**, **Remote Interactive Logon**, **This Organization**, **System**, **Local Service**, **Network Service**, **Write Restricted**, **Other Organization**, **Builtin**, **Internet$**, **Members can fully administer the computer/domain**, **Members can share directories**, **Backup Operators**, **Members can bypass file security to back up files**, **Current Owner**, **Current Group**. ● User accounts retained in Linux: **root**, **nogroup**, **nobody**, **ftp**, **anonymous**, **bin**, **daemon**, **sys**, **tty**, **disk**, **lp**, **www**, **kmem**, **wheel**, **mail**, **news**, **uucp**, **shadow**, **dialout**, **audio**, **floppy**, **cdrom**, **console**, **utmp**, **public**, **video**, **games**, **xok**, **trusted**, **modem**, **man**, **users**, **nobody**, **nogroup**, **sshd**, **postfix**, **maildrop**. ● User accounts retained in a storage system: **ibc_os_hs**.	

Item	Description	Example
AD domain information *AD domain information for domain authentication.*	AD domain information includes: ● User name of the domain administrator: The AD domain can provide an account that has the rights to add storage systems to the domain. ● Password: password of the user. ● Full domain name: name of the AD domain ● Organization Unit: Organization unit of a type of directory objects in a domain. These objects include users, computers, and printers. After an object is added to a domain, it will be a member in the organization unit. If you do not enter anything, the storage system is added to organization unit as **Computers** by default. ● System name: name of a storage system that is added to the AD domain. ● Overwrite System Name: After this option is selected, the system name that is the same as the name of the domain control server is overwritten. Then the authentication of the devices and domain control servers related to the system name is affected.	-
DNS *DNS information for domain authentication.*	IP address of DNS server.	-
a: Quota tree refers to the quota tree and is a special directory of the file system. You can set a directory quota on the quota tree to manage the space used by all files under the directory.		

NOTE

You can contact your network administrator to obtain desired data.

3.9.2.3 Checking the License File

Each value-added feature requires a license file for activation. Before configuring a value-added feature, ensure that its license file is valid for the feature.

Context

On the DeviceManager interface, CIFS feature is displayed in **Feature** of **CIFS Protocol**.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Settings** > **License Management**.

Step 3 Check the active license files.

1. In the navigation tree on the left, choose **Active License**.
2. In the middle information pane, verify the information about active license files.

----End

Follow-up Procedure

- If the information about the license of the feature is not displayed on the **Active License** page, apply for and import a license file as instructed in the *Installation Guide* of the corresponding product model.
- If the storage system generates an alarm indicating that the license expired, purchase and import another license file.

3.9.2.4 Configuring a Network

This section describes how to use DeviceManager to configure a logical IP address for a storage system. The logical IP address is used for accessing shares.

3.9.2.4.1 (Optional) Configuring DNS-based Load Balancing Parameters (Applicable to V300R006C10 and Later Versions)

Storage arrays' DNS-based load balancing feature can detect the IP address load on the arrays in real time and use a proper IP address as the DNS response to achieve load balancing among IP addresses. This section describes how to configure DNS-based load balancing and DNS zones.

Context

Working principle:

1. When a host accesses the NAS service of a storage array using the domain name, the host first sends a DNS request to the built-in DNS server of the storage array and the DNS server obtains the IP address according to the domain name.
2. When a domain name contains multiple IP addresses, the storage array selects the IP address with a light load as the DNS response based on the configured load balancing policy and returns the DNS response to the host.
3. After receiving the DNS response, the host sends a service request to the destination IP address.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Settings** > **Storage Settings** > **File Storage Service** > **DNS-based Load Balancing**.

Step 3 Table 3-35 lists parameters related to DNS-based load balancing.

Table 3-35 DNS-based load balancing parameters

Parameter	Description	Value
DNS-based Load Balancing	Enables or disables DNS-based load balancing. **NOTE** ● When enabling the DNS-based load balancing function, you are advised to disable the global namespace forwarding function. This function affects DNS-based load balancing. ● After the DNS-based load balancing function is disabled, the domain name resolution service is unavailable and file systems cannot use the function. ● This parameter can be set only in the system view, not in the vStore view. The setting takes effect for the entire storage system.	[Example] Enable

Parameter	Description	Value
Load Balancing Policy	This parameter enables you to configure DNS-based load balancing policies. A storage system supports the following load balancing policies: ● Weighted round robin: When a client uses a domain name to initiate an access request, the storage system calculates the weight based on the performance data. Under the same domain name, IP addresses that are required to process loads have the same probability to be selected to process client services. ● CPU usage: When a client uses a domain name to initiate an access request, the storage system calculates the weight based on the CPU usage of each node. Using the weight as the probability reference, the storage system selects a node to process the client's service request. ● Bandwidth usage: When a client uses a domain name to initiate an access request, the storage system calculates the weight based on the total bandwidth usage of each node. Using the weight as the probability reference, the storage system selects a node to process the client's service request. ● Open connections: When a client uses a domain name to initiate an access request, the storage system calculates the weight based on the NAS connections of each node. Using the weight as the probability reference, the storage system selects a node to process the client's service request. ● Overall load: When a client uses a domain name to initiate an access request, the storage system selects a node to process the client's service request based on the comprehensive load. The comprehensive node load is calculated based on the CPU usage, bandwidth usage, and number of NAS connections. Less	[Example] Weighted round robin

Parameter	Description	Value
	loaded nodes are more likely to be selected. **NOTE** This parameter can be set only in the system view, not in the vStore view. The setting takes effect for the entire storage system.	

Step 4 Configure a DNS zone.

A DNS zone contains IP addresses of a group of logical ports. A host can use the name of a DNS zone to access shared services provided by a storage system. Services can be evenly distributed to logical ports.

NOTE

Only the logical ports whose **Role** is **Service** or **Management+Service** can be added into a DNS zone. The logical ports whose **Role** is **Management** cannot be added in to a DNS zone.

1. Add a DNS zone.
   a. Click **Add**.
   b. The **Add DNS Zone** dialog box is displayed. In **Domain Name**, type the domain name of the DNS zone you want to add and click **OK**.

      NOTE

      The domain name complexity requirements are as follows:

      - A domain name contains 1 to 255 characters and consists of multiple labels separated by periods (**.**).
      - A label contains 1 to 63 characters including letters, digits, hyphens (-), and underscores (_), and must start and end with a letter or a digit.
      - The domain name must be unique.
2. Remove a DNS zone.
   a. In the DNS zones that are displayed, select a DNS zone you want to remove.
   b. Click **Remove**.
3. Modify a DNS zone.
   a. In the DNS zones that are displayed, select a DNS zone you want to modify.
   b. Click **Modify**.
   c. The <**Modify DNS Zone** dialog box is displayed. In **Domain Name**, type the domain name of the DNS zone you want to modify and click **OK**.
4. View a DNS zone.
   a. In **DNS Zone**, type a keyword and click **Search**.
   b. In **DNS Zone**, the DNS zone names relevant to the keyword will be displayed.

      NOTE

      You can select a DNS zone to modify or remove it.

Step 5 Click **Save**. The **Warning** dialog box is displayed.

Step 6 Confirm the information in the dialog box and select **I have read and understand the consequences associated with performing this operation**.

Step 7 Click **OK**. The **Execution Result** page is displayed.

Step 8 On the **Execution Result** page, confirm the modification and click **Close**. The DNS zone configuration is complete.

----End

Follow-up Procedure

Choose **Provisioning** > **Port** > **Logical Ports** to configure **Listen DNS Query Request** and **DNS Zone** information for logical ports.

3.9.2.4.2 Creating a Logical Port

This operation enables you to create a logical port for managing and accessing file based on Ethernet ports, bond ports, or VLANs.

Precautions

The number of logical ports created for each controller is recommended not more than 64. If the number exceeds 64 and a large number of ports do not work properly, logical ports drift towards the small number of ports available. As a result, service performance deteriorates.

Procedure

Step 1 Log in to DeviceManager.

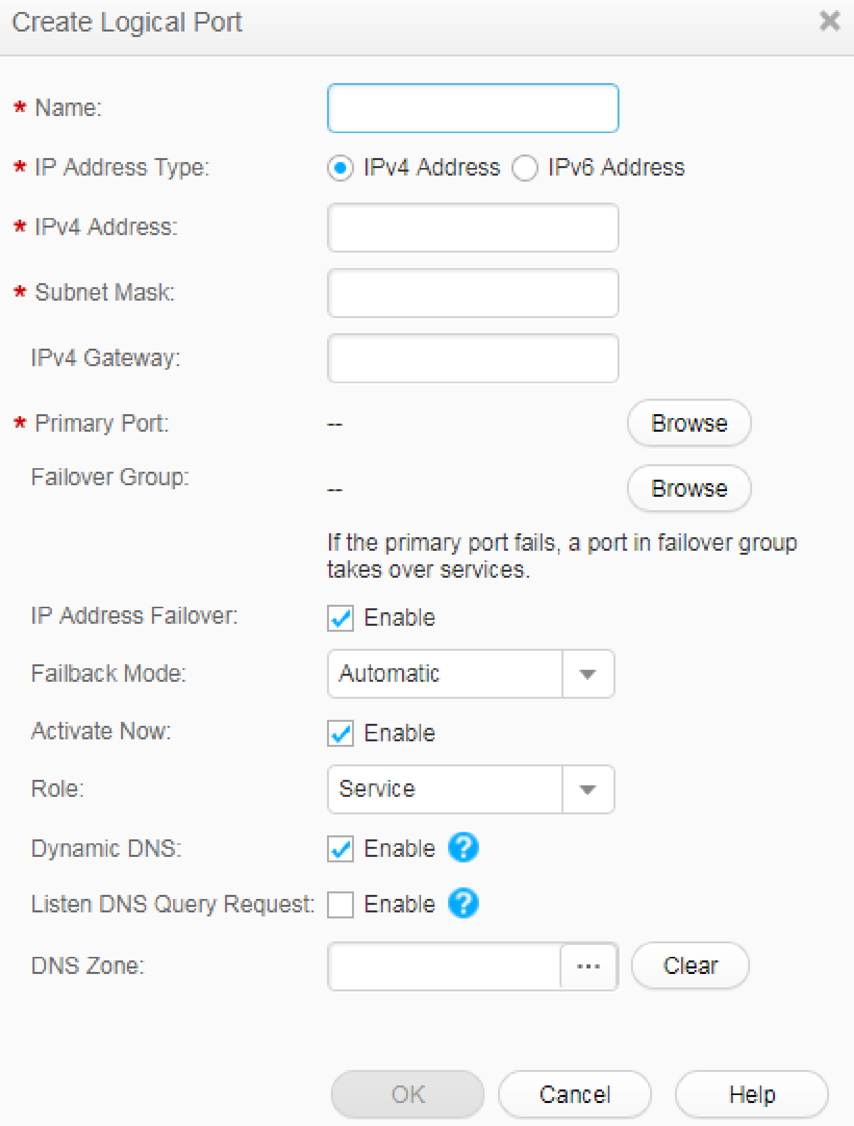
Step 2 Choose **Provisioning** > **Port** > **Logical Ports**.

Step 3 Click **Create**.

The **Create Logical Port** dialog box is displayed.

Step 4 In the **Create Logical Port** dialog box, configure related parameters.

Table 3-36 describes related parameters.



Create Logical Port

* Name:
* IP Address Type: ● IPv4 Address ○ IPv6 Address
* IPv4 Address:
* Subnet Mask:
IPv4 Gateway:
* Primary Port: --
Failover Group: --
If the primary port fails, a port in failover group takes over services.
IP Address Failover: ☑ Enable
Failback Mode: Automatic
Activate Now: ☑ Enable
Role: Service
Dynamic DNS: ☑ Enable
Listen DNS Query Request: □ Enable
DNS Zone:

Table 3-36 Logical port parameters

Parameter	Description	Value
Name	Name of the logical port. The name must meet the following requirements so that the logical port is available to compatible applications: ● The name must be unique. ● The name can contain only letters, digits, underscores (_), periods (.), and hyphens (-). ● The name contains 1 to 31 characters.	[Example] lif01
IP Address Type	IP address type of the logical port, including IPv4 or IPv6.	[Example] IPv4
IPv4 Address	IPv4 address of the logical port.	[Example] 192.168.100.11
Subnet Mask	IPv4 subnet mask of the logical port.	[Example] 255.255.0.0
IPv4 Gateway	IPv4 gateway of the logical port.	[Example] 192.168.100.1
IPv6 Address	IPv6 address of the logical port.	[Example] fc00::1234
Prefix	IPv6 prefix length of the logical port.	[Example] 64
IPv6 Gateway	IPv6 gateway of the logical port.	[Example] fc00::1
Primary Port	Port to which the logical port belongs, including the Ethernet port, Bond port, and VLAN.	[Example] None

Parameter	Description	Value
Failover Group	Failover group name. **NOTE** ● If a failover group is specified, services on the failed primary port will be taken over by a port in the specified failover group. ● If no failover group is specified, services on the failed primary port will be taken over by a port in the default failover group.	[Example] None
IP Address Failover	After IP address failover is enabled, services are failed over to other normal ports within the failover group if the primary port fails. However, the IP address used by services remains unchanged. **NOTE** Shares of file systems do not support the multipathing mode. IP address failover is used to improve reliability of links.	[Example] Enable
Failback Mode	Mode in which services fail back to the primary port after the primary port is recovered. The mode can be manual or automatic. **NOTE** ● If **Failback Mode** is **Manual**, ensure that the link to the primary port is normal before the failback. Services will manually fail back to the primary port only when the link to the primary port keeps normal for over five minutes. ● If **Failback Mode** is **Automatic**, ensure that the link to the primary port is normal before the failback. Services will auto fail back to the primary port only when the link to the primary port keeps normal for over five minutes.	[Example] Automatic

Parameter	Description	Value
Activate Now	To activate the logical port immediately.	[Example] Enable
Role	Roles of logical ports include the following: ● Management: The port is used by a super administrator to log in to the system for management. ● Service: The port is used by a super administrator to access services such as file system CIFS shares. ● Management+Service: The port is used by a super administrator to log in to the system to manage the system and access services.	[Example] Service
Dynamic DNS	When the dynamic DNS is enabled, the DNS server will automatically and periodically update the IP address configured for the logical port.	[Example] Enable
Listen DNS Query Request	After this function is enabled, external NEs can access the DNS service provided by the storage system by using the IP address of this logical port.	[Example] Enable

Parameter	Description	Value
DNS Zone	Name of a DNS zone. **NOTE** ● If the value is blank, the logical port is not used for DNS-based load balancing. ● Only the logical ports whose **Role** is **Service** or **Management+Service** can be added into a DNS zone. The logical ports whose **Role** is **Management** cannot be added in to a DNS zone. ● One logical port can be associated with only one DNS zone. One DNS zone can be associated with multiple logical ports. ● A DNS zone can be associated with both IPv4 and IPv6 logical ports. ● The load balancing effect varies with the distribution of logical ports associated with a DNS zone. To obtain a better load balancing effect, ensure that logical ports associated with a DNS zone are evenly distributed among controllers.	[Example] None

Step 5 Click **OK**.

The **Success** dialog box is displayed indicating that the logical port has been successfully created.

Step 6 Click **OK**.

----End

3.9.2.4.3 (Optional) Creating a Bond Port

This section describes how to bond Ethernet ports on a same controller.

Prerequisites

Ethernet ports that have IP addresses cannot be bound. The IP addresses of the bonded host ports need to be cleared before bonding.

Context

- Port bonding provides more bandwidth and redundancy for links. Although ports are bonded, each host still transmits data through a single port and the total bandwidth can

be increased only when there are multiple hosts. Determine whether to bond ports based on site requirements.

- The port bond mode of a storage system has the following restrictions:
  - On the same controller, a bond port is formed by a maximum of eight Ethernet ports.
  - Only the interface modules with the same port rate (GE or 10GE) can be bonded.
  - The port cannot be bonded across controllers. Non-Ethernet network ports cannot be bonded.
  - SmartIO interface modules cannot be bonded if they work in cluster or FC mode or run FCoE service in FCoE/iSCSI mode.
  - Read-only users are unable to bind Ethernet ports.
  - Each port only allows to be added to one bonded port. It cannot be added to multiple bonded ports.
  - Ports are bonded to create a bond port that cannot be added to the port group.
- After Ethernet ports are bonded, **MTU** changes to the default value and you must set the link aggregation mode for the ports. For example, on Huawei switches, you must set the ports to the static LACP mode.

  NOTE

  The detailed link aggregation mode varies with the switches' manufacturer.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Provisioning** > **Port** > **Bond Ports**.

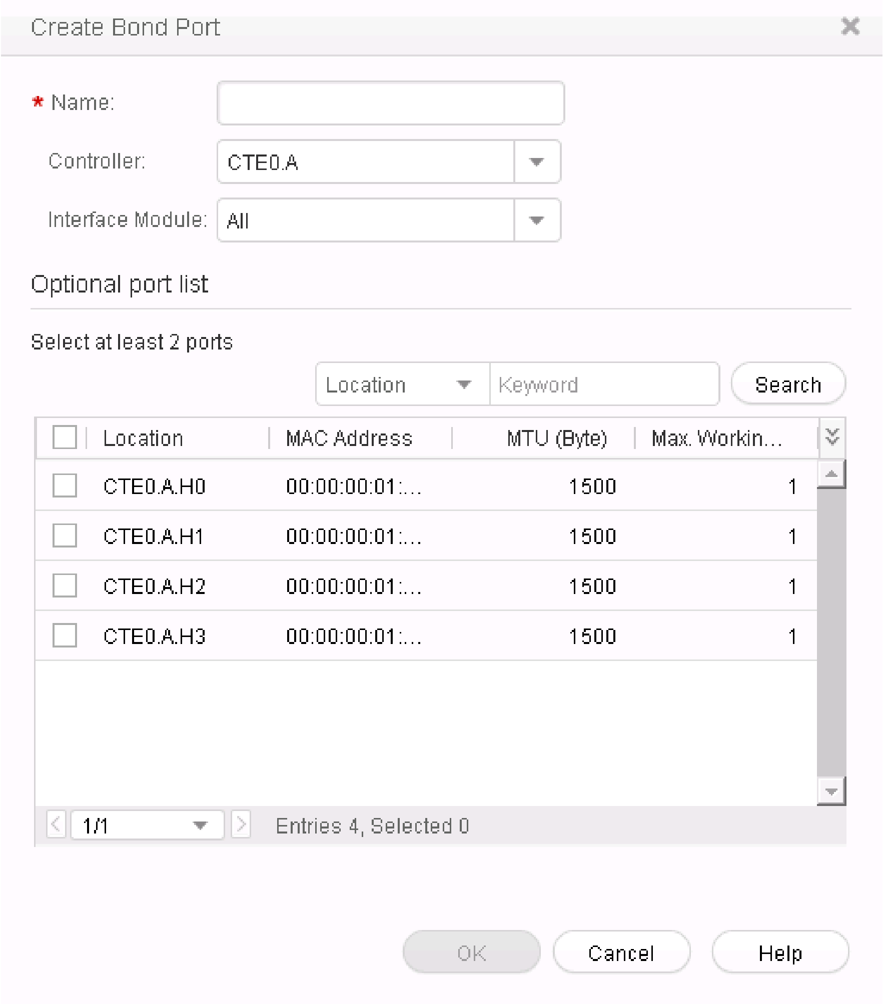
Step 3 Click **Create**.

The **Create Bond Port** dialog box is displayed.

NOTE

The port name format is **controller enclosure ID.interface module ID.port ID**.

Step 4 Set the name, interface module, and optional ports that can be bonded with the current Ethernet port.



Create Bond Port

* Name:

Controller: CTE0.A

Interface Module: All

Optional port list

Select at least 2 ports

□	Location	MAC Address	MTU (Byte)	Max. Workin...
□	CTE0.A.H0	00:00:00:01:...	1500	1
□	CTE0.A.H1	00:00:00:01:...	1500	1
□	CTE0.A.H2	00:00:00:01:...	1500	1
□	CTE0.A.H3	00:00:00:01:...	1500	1

1/1 Entries 4, Selected 0

1. In **Name**, enter a name for the bond port.

   The name:

   - Contains only letters, digits, underscores (_), periods (.), and hyphens (-).
   - Contains 1 to 31 characters.

2. From the **Controller**, select the controller the Ethernet ports own to.
3. Select the **Interface Module**.
4. From the **Optional port list**, select the Ethernet ports you want to bond.

   NOTE

   Select at least two ports.

5. Click **OK**.

   The security alert dialog box is displayed.

Step 5 Confirm that you want to bond these Ethernet ports.

1. Confirm the information of the dialog box and select **I have read and understand the consequences associated with performing this operation.**.
2. Click **OK**.

   The **Success** dialog box is displayed indicating that the operation succeeded.

3. Click **OK**.

----End

3.9.2.4.4 (Optional) Managing a Route of Logical Port

You need to configure a route when the CIFS server and the storage system are not on the same network. When a domain controller server exists, ensure that the logical IP addresses, domain controller server, and DNS can ping each other. If they cannot ping each other, add routes from the logical IP addresses to the network segment of the domain controller server and the DNS. When configuring CIFS share access, if the CIFS server and logical IP addresses cannot ping each other, add a route from the logical IP addresses to the network segment of the CIFS server.

Prerequisites

The logical port has been assigned an IP address.

Procedure

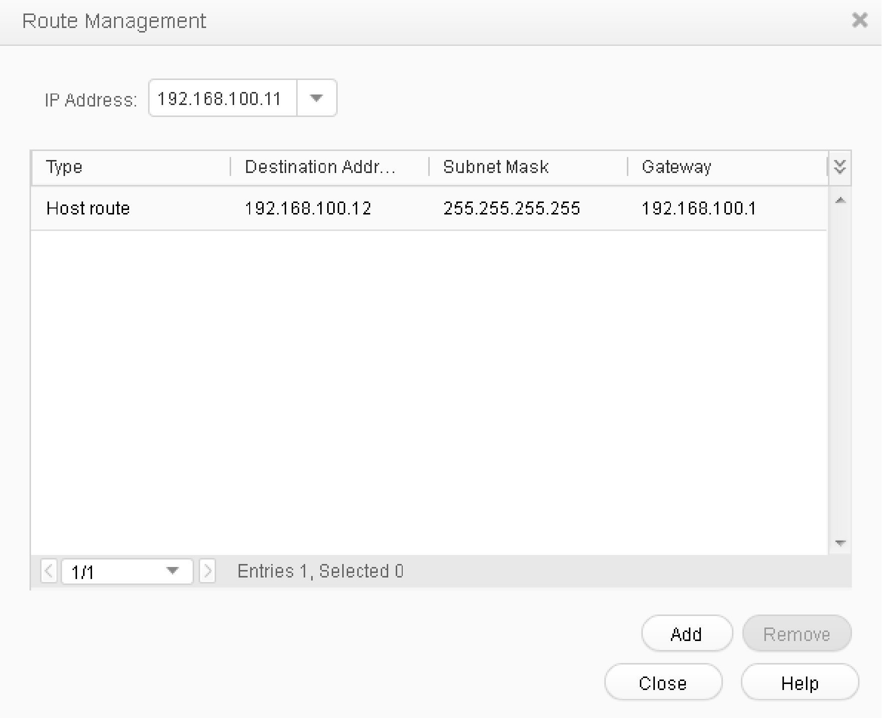
Step 1 Log in to DeviceManager.

Step 2 Go to the route management page.

You can go to the route management page by using either of the following methods:

- Choose **Provisioning** > **Port** > **Logical Ports**. Select a logical port for which you want to add a route and click **Route Management**. The **Route Management** dialog box is displayed.
- Choose **System** and click to switch to the rear view of the controller enclosure. Select the Ethernet port that you want to configure and click **Logical Port Management**. In the **Logical Port Management** dialog box that is displayed, select a logical port for which you want to add a route and click **Route Management**. The **Route Management** dialog box is displayed.

Step 3 Configure the route information for the logical port.



Route Management

IP Address: 192.168.100.11

Type	Destination Addr...	Subnet Mask	Gateway
Host route	192.168.100.12	255.255.255.255	192.168.100.1

1/1 Entries 1, Selected 0

1. In **IP Address**, select the IP address of the logical port.
2. Click **Add**.

   The **Add Route** dialog box is displayed.

   NOTICE

   The default IP addresses of the internal heartbeat on the dual-controller storage system are **127.127.127.10** and **127.127.127.11**, and the default IP addresses of the internal heartbeat on the four-controller storage system are **127.127.127.10**, **127.127.127.11**, **127.127.127.12**, and **127.127.127.13**. Therefore, the IP address of the router cannot fall within the 127.127.127.XXX segment. Besides, the IP address of the gateway cannot be **127.127.127.10**, **127.127.127.11**, **127.127.127.12**, or **127.127.127.13**. Otherwise, routing will fail. (Internal heartbeat links are established between controllers for these controllers to detect each other's working status. You do not need to separately connect cables. In addition, internal heartbeat IP addresses have been assigned before delivery, and you cannot change these IP addresses).

3. In **Type**, select the type of the route to be added.

   Possible values of **Type** are **Default route**, **Host route**, and **Network segment route**.
4. Set **Destination Address**.
   - If **IP Address** is an IPv4 address, set **Destination Address** to the IPv4 address or network segment of the application server's service network port or that of the other storage system's logical port.
   - If **IP Address** is an IPv6 address, set **Destination Address** to the IPv6 address or network segment of the application server's service network port or that of the other storage system's logical port.
5. Set **Destination Mask** (IPv4) or **Prefix** (IPv6).
   - If a **Destination Mask** is set for an IPv4 address, this parameter specifies the subnet mask of the IP address for the service network port on the application server or storage device.
   - If a **Prefix** is set for an IPv6 address, this parameter specifies the prefix of the IPv6 address for application server's service network port or that of the other storage system's logical port.
6. In **Gateway**, enter the gateway of the local storage system's logical port IP address.

Step 4 Click **OK**. The route information is added to the route list.

The security alert dialog box is displayed.

Step 5 Confirm the information of the dialog box and select **I have read and understand the consequences associated with performing this operation.**.

Step 6 Click **OK**.

The **Success** dialog box is displayed indicating that the operation succeeded.

NOTE

To remove a route, select it and click **Remove**.

Step 7 Click **Close**.

----End

3.9.2.5 Setting the CIFS Service (Applicable to V300R006C00)

Before creating a share, enable and configure the CIFS service.

Prerequisites

The license for CIFS protocol has been imported and activated.

Procedure

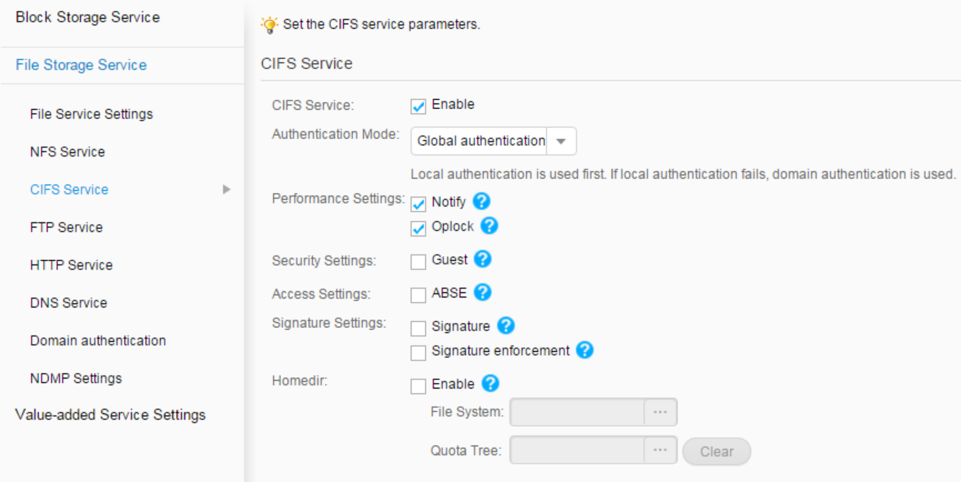
Step 1 Log in to DeviceManager.

Step 2 Choose **Settings** > **Storage Settings** > **File Storage Service** > **CIFS Service**.

Step 3 In **CIFS Service**, check whether **Enable** is selected. If not, select **Enable**.

Step 4 Configure CIFS service parameters.

1. Configure parameters described in **Table 3-37** based on site conditions.



Set the CIFS service parameters.

CIFS Service

CIFS Service: ☑ Enable

Authentication Mode: Global authentication

Local authentication is used first. If local authentication fails, domain authentication is used.

Performance Settings: ☑ Notify ☑ Oplock

Security Settings: □ Guest

Access Settings: □ ABSE

Signature Settings: □ Signature □ Signature enforcement

Homedir: □ Enable

File System:

Quota Tree:

Table 3-37 CIFS service parameters

Parameter	Description	Setting
Authentication Mode	Authentication mode for accessing a CIFS share. – **Local authentication**: Applies to scenarios where a local authentication user accesses a CIFS share in a non-domain environment. – **Domain authentication**: Applies to scenarios where a domain user accesses a CIFS share in an AD domain. – **Global authentication**: Local authentication is used first. If local authentication fails, domain authentication is used.	[Default value] Global authentication

Parameter	Description	Setting
Performance Settings	You can configure performance parameters to improve the CIFS share access efficiency. – Oplock: Opportunistic locking (Oplock) is a mechanism used to adjust cache policies of clients, improving performance and network utilization. This function is not recommended in the following scenarios: ■ Scenarios that have high requirements for data integrity: Local cache loss will occur if your network is interrupted or your client breaks down after Oplock is enabled. If the upper-layer service software does not have a mechanism to ensure data integrity, recovery, or retry, data loss may occur. ■ Scenarios where multiple clients access the same file: If Oplock is enabled, the system performance will be adversely affected. – Notify: After this parameter is enabled, a client's operations on a directory, such as adding a sub-directory, adding a new file, modifying the directory, and modifying a file, can be sensed by other clients that are accessing this	[Default value] Enabled

Parameter	Description	Setting
	directory or the parent directory of this directory.	
Security Settings	After the guest service is enabled, users can access shared directories without user names or passwords. Besides, users have the same permission as the **Everyone** local authentication group. **NOTE** After this function is enabled, unauthorized users can access shared directories as a guest user, which may cause information security issues. You are advised to disable this function.	[Default value] Disabled
Access Settings	After ABSE (Access based share enumeration) has been enabled, when user view the CIFS share information, only the CIFS shares that the user has permission to access displays. **NOTE** – It takes 10 to 20 minutes to load the CIFS share permission information after the storage system is powered on. During this period, the function does not take effect. – You are advised to enable this function. If this function is disabled, users can find all shares (including the shares for which the users do not have access permission), which may cause security threats to other shares.	[Default value] Disabled

Parameter	Description	Setting
Signature Settings	You can set signatures to enhance CIFS share access security. – Signature: This item is available for a client that employs Server Message Block (SMB) 1.0. After this item is selected, the client supports the signature function. For a client that employs an SMB later than SMB 1.0, the client supports the signature function by default. Whether the signature function is enabled also depends on the client registry settings. By default, the registry settings do not support the signature function. – Signature enforcement: After this option is selected, servers must adopt the signature function no matter the signature function is enabled by clients or not. **NOTE** If the signature function is disabled, the storage system may encounter man-in-the-middle (MITM) attacks, resulting in security risks.	[Default value] Disabled

Parameter	Description	Setting
Homedir	The Homedir share provides specific users with directories exclusively shared to them. An exclusive directory can only be accessed by its owner. – File system: file system that is shared in CIFS Homedir mode (mandatory) – Quota Tree: level-1 directory of a file system (optional) **NOTE** After Homedir is enabled, a user can directly access the directory (the directory is the same as the user name) under the specified the file system directory.	[Default value] Disabled

2. After the parameters are configured, click **Save**.

   The **Success** dialog box is displayed indicating that the operation succeeded.

3. Click **OK** to finish configuring CIFS service parameters.

----End

3.9.2.6 Setting the CIFS Service (Applicable to V300R006C10 and Later Versions)

Before creating a share, enable and configure the CIFS service.

Prerequisites

The license for CIFS protocol has been imported and activated.

Procedure

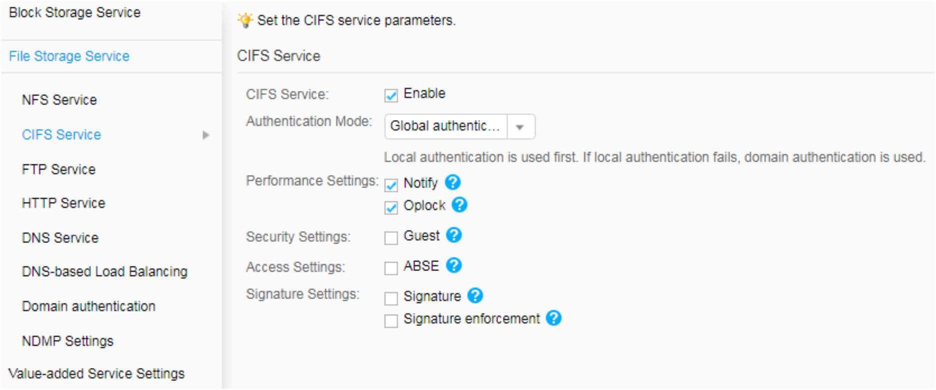
Step 1 Log in to DeviceManager.

Step 2 Choose **Settings** > **Storage Settings** > **File Storage Service** > **CIFS Service**.

Step 3 In **CIFS Service**, check whether **Enable** is selected. If not, select **Enable**.

Step 4 Configure CIFS service parameters.

1. Configure parameters described in **Table 3-38** based on site conditions.



Set the CIFS service parameters.

CIFS Service

CIFS Service: ☑ Enable

Authentication Mode: Global authentic...

Local authentication is used first. If local authentication fails, domain authentication is used.

Performance Settings: ☑ Notify ☑ Oplock

Security Settings: □ Guest

Access Settings: □ ABSE

Signature Settings: □ Signature □ Signature enforcement

Table 3-38 CIFS service parameters

Parameter	Description	Setting
Authentication Mode	Authentication mode for accessing a CIFS share. – **Local authentication**: Applies to scenarios where a local authentication user accesses a CIFS share in a non-domain environment. – **Domain authentication**: Applies to scenarios where a domain user accesses a CIFS share in an AD domain. – **Global authentication**: Local authentication is used first. If local authentication fails, domain authentication is used.	[Default value] Global authentication

Parameter	Description	Setting
Performance Settings	You can configure performance parameters to improve the CIFS share access efficiency. – Oplock: Opportunistic locking (Oplock) is a mechanism used to adjust cache policies of clients, improving performance and network utilization. This function is not recommended in the following scenarios: ■ Scenarios that have high requirements for data integrity: Local cache loss will occur if your network is interrupted or your client breaks down after Oplock is enabled. If the upper-layer service software does not have a mechanism to ensure data integrity, recovery, or retry, data loss may occur. ■ Scenarios where multiple clients access the same file: If Oplock is enabled, the system performance will be adversely affected. – Notify: After this parameter is enabled, a client's operations on a directory, such as adding a sub-directory, adding a new file, modifying the directory, and modifying a file, can be sensed by other clients that are accessing this directory or the parent directory of this directory.	[Default value] Enabled

Parameter	Description	Setting
Security Settings	After the guest service is enabled, users can access shared directories without user names or passwords. Besides, users have the same permission as the **Everyone** local authentication group. **NOTE** After this function is enabled, unauthorized users can access shared directories as a guest user, which may cause information security issues. You are advised to disable this function.	[Default value] Disabled
Access Settings	After ABSE (Access based share enumeration) has been enabled, when user view the CIFS share information, only the CIFS shares that the user has permission to access displays. **NOTE** – It takes 10 to 20 minutes to load the CIFS share permission information after the storage system is powered on. During this period, the function does not take effect. – You are advised to enable this function. If this function is disabled, users can find all shares (including the shares for which the users do not have access permission), which may cause security threats to other shares.	[Default value] Disabled

Parameter	Description	Setting
Signature Settings	You can set signatures to enhance CIFS share access security. – Signature: This item is available for a client that employs Server Message Block (SMB) 1.0. After this item is selected, the client supports the signature function. For a client that employs an SMB later than SMB 1.0, the client supports the signature function by default. Whether the signature function is enabled also depends on the client registry settings. By default, the registry settings do not support the signature function. – Signature enforcement: After this option is selected, servers must adopt the signature function no matter the signature function is enabled by clients or not. **NOTE** If the signature function is disabled, the storage system may encounter man-in-the-middle (MITM) attacks, resulting in security risks.	[Default value] Disabled

2. After the parameters are configured, click **Save**.

   The **Success** dialog box is displayed indicating that the operation succeeded.

3. Click **OK** to finish configuring CIFS service parameters.

----End

3.9.2.7 Configuring a Local Authentication User (Group)

In a non-domain environment, you must configure a local authentication user (group). Storage system enables you to allocate different CIFS share access permissions to different user (group).

3.9.2.7.1 (Optional) Creating a Local Authentication User Group

This section describes how to create a local authentication user group. Local authentication user groups help you control the share access permissions of local authentication users.

Context

A storage system has four local authentication user groups that are automatically created. The four local authentication user groups are reserved for the system and cannot be deleted.

- **default_group**: default user group. When the group members access the shared file system in the storage systems, they must be authenticated to obtain their permissions.
- **Administrators**: administrator group. When the group members access the shared file system in the storage system, they do not need to be authenticated by share level ACL and directory&file level NT ACL. They can operate any file in any share with administrator permissions.
- **AntivirusGroup**: antivirus user group. The group members can use third-party antivirus software to scan for shared file systems. They have administrator permissions.
- **Backup Operators**: backup user group. The group members can use third-party backup software to back up and recover shared file systems. They do not have administrator permissions.

NOTE

Access Control List (ACL): a collection of permissions that are authorized to users or user groups to operate shared files. ACL permissions are classified into ACL permission storage and ACL permission authentication. After a user logs in to a share, the user determines the share permissions, reads the ACL permissions, and determines whether files can be read and written. For storage, each ACL permission is called Access Control Entry (ACE). After CIFS shares are mounted to a Windows client, the client sends NT ACLs to a server (storage system that provides CIFS shares).

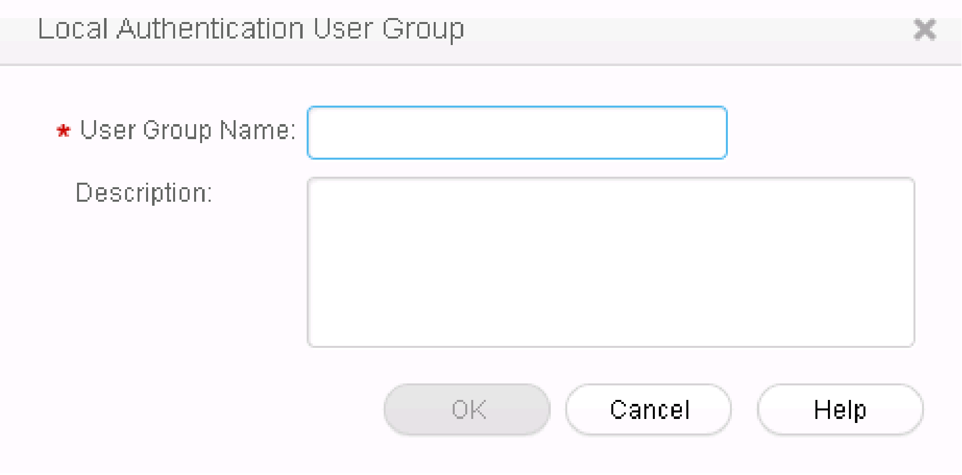
Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Provisioning** > **User Authentication** > **Local Authentication User Group**.

Step 3 Click **Create**.

The **Local Authentication User Group** dialog box is displayed.



Step 4 In **User Group Name**, enter a new user group name.

NOTE

- For V300R006C00:
  - Must contain 1 to 32 characters.
  - Cannot contain space, double quotation mark ("), slash (/), backslash (\), square brackets ([]), larger than (<), less than (>), plus (+), colon (:), semicolon (;), comma (,), question mark (?), asterisk (*), vertical bar (|), equal mark (=), (@), or end with a period (.).
  - The user group name can contain case-insensitive letters. Therefore, **aa** and **AA** cannot be created at the same time.
  - The user group name cannot be the same as the name of the local authentication user.
- For V300R006C10:
  - The user group name cannot contain the quotation mark ("), slash (/), backslash (\), square brackets ([]), less than sign (<), larger than sign (>), plus sign (+), colon (:), semicolon (;), comma (,), question mark (?), asterisk (*), vertical bar (|), equal sign (=), at sign (@) or end with a period (.). If the user group name start and end with spaces, the spaces are not displayed after the user group name is created.
  - The user group name can contain case-insensitive letters. Therefore, **aa** and **AA** cannot be created at the same time.
  - The user group name cannot be the same as the name of the local authentication user.
  - The user group name contains 1 to 63 characters.

Step 5 **Optional:** In **Description**, add the description of the user group.

Step 6 Click **OK**.

Step 7 In the **Success** dialog box that is displayed, click **OK**.

----End

3.9.2.7.2 Creating a Local Authentication User

This section describes how to create a local user. For applications that use local authentication, local user accounts are used to access a share. You can add a local user to a user group and access a share as the user group.

Procedure

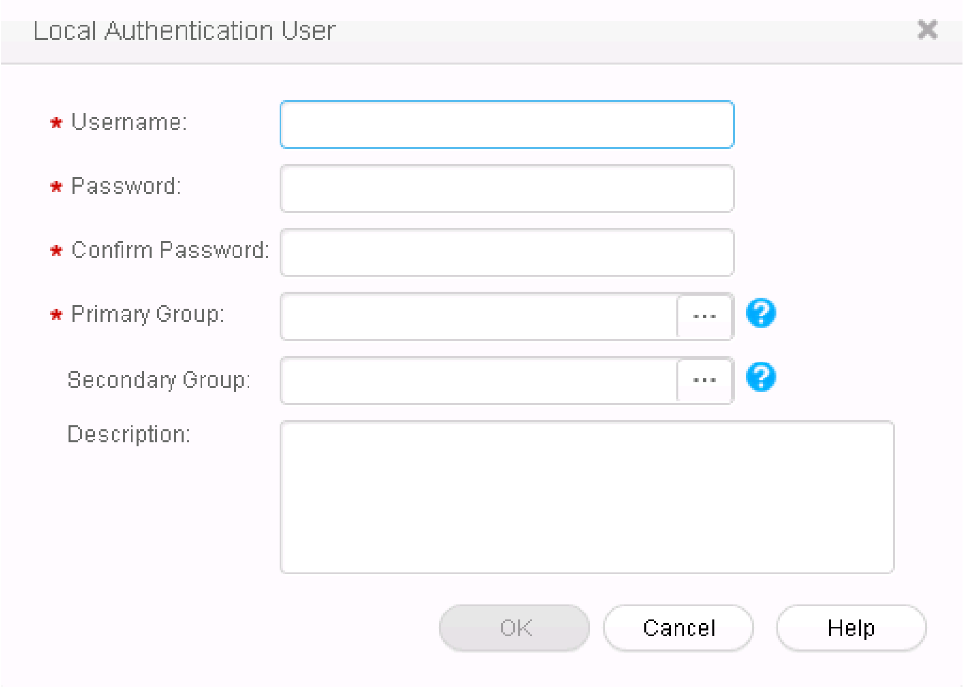
Step 1 Log in to DeviceManager.

Step 2 Choose **Provisioning** > **User Authentication**.

Step 3 Click **Local Authentication User** tab.

Step 4 Click **Create**.

The **Local Authentication User** dialog box is displayed.



Step 5 In **Username**, enter a new user name.

The user name:

- Cannot contain space, double quotation mark ("), slash (/), backslash (\), square brackets ([]), less than (<), larger than (>), plus (+), colon (:), semicolon (;), comma (,), question mark (?), asterisk (*), vertical bar (|), equal mark (=), (@), or end with a period (.).
- The user name can contain case-insensitive letters. Therefore, **aaaaaaaa** and **AAAAAAAA** cannot be created at the same time.
- The user name cannot be the same as the name of the local authentication user group.
- Contains 8 to 32 characters by default.

  NOTE

  You can modify the minimum length of user name in **More** > **Set Security Policies**.

Step 6 In **Password**, enter the password of the user.

The system default password requirements are:

- Contain 8 to 16 characters.
- Contain special characters. Special characters include: !"#$%&'()*+,-./:;<=>?@[\]^`{_|}~ and space.
- Contain any two types of the uppercase letters, lowercase letters, and digits.
- Cannot contain three consecutive same characters.
- Be different from the user name or the user name typed backwards.

NOTE

Click **More** and choose **Set Security Policies** to set a security policy for the password of the local authentication user in the file system. If **Password Validity Period (days)** is not selected, your password will never expire. For the security purpose, you are advised to select **Password Validity Period (days)** and set a validity period. The default validity period is 180 days. After the password expires, you cannot access shares, but you can set a password again and modify the password security policy.

Step 7 In **Confirm Password**, enter the new password again.

Step 8 Select **Primary Group**.

The **Select Primary Group** dialog box is displayed.

NOTE

The primary group to which users belong controls the users' permission for CIFS shares. A user must and can only belong to one primary group.

Step 9 Select the user group to which the user belongs to and click **OK**.

Step 10 (Optional) Select **Secondary Group**.

The **Select Secondary Group** dialog box is displayed.

NOTE

The concepts of primary group and secondary group are for local authentication users and have no relationship with each other. A local authentication user must belong to a primary group but not to a secondary group.

Step 11 Click **Add**.

The **Select User Group** dialog box is displayed.

Step 12 Select one or multiple groups which the user belongs to and click **OK**.

The system goes back to **Select Secondary Group** dialog box.

Step 13 Click **OK**.

The system goes back to **Local Authentication User** dialog box.

Step 14 **Optional:** In **Description** text box, enter the description for the local authentication user, for later management or search.

Step 15 Click **OK**.

Step 16 In the **Success** dialog box that is displayed, click **OK**.

----End

3.9.2.8 Configuring a Storage System to Add It to an AD Domain

After the storage system is added to an AD domain, domain users can access CIFS shares that are allocated to the domain. This section describes how to add a storage system to an AD domain.

3.9.2.8.1 Preparing AD Domain Configuration Data

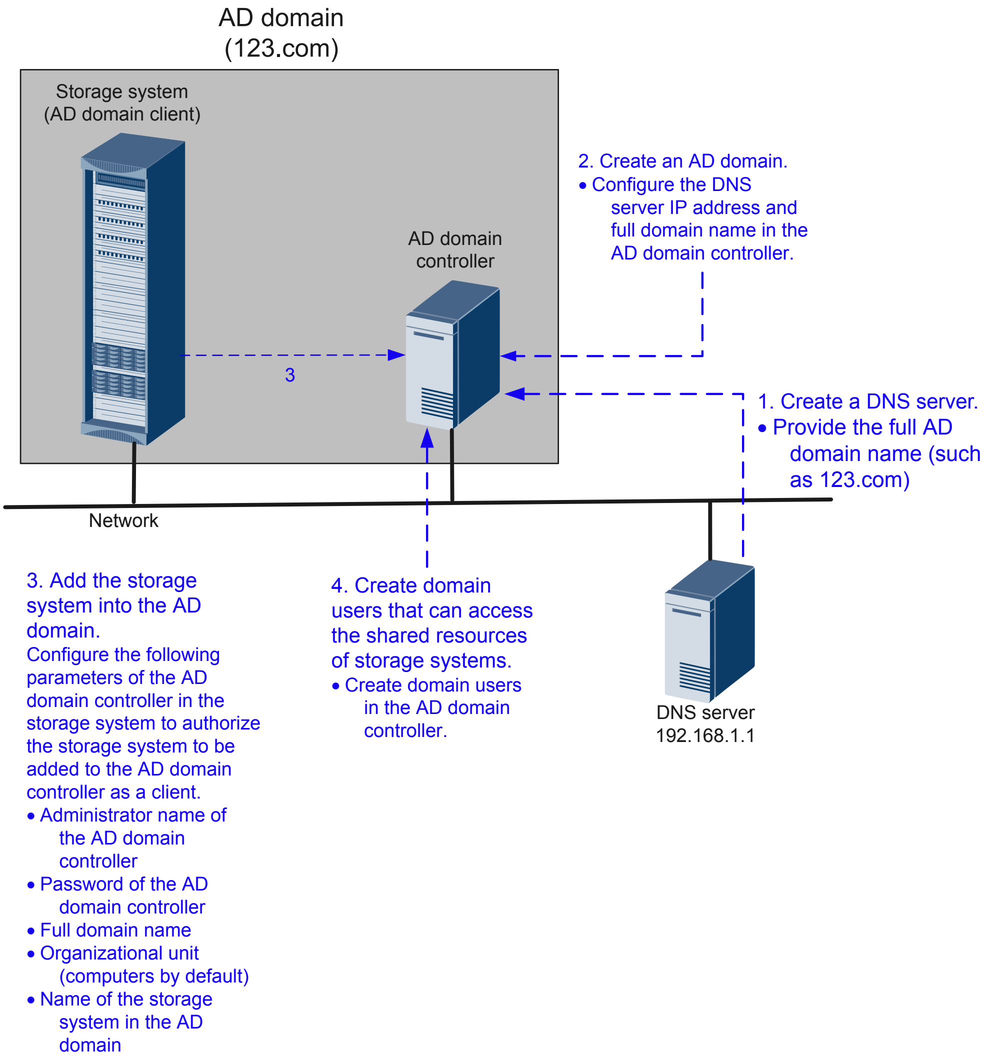
Why AD Domains?

In the Windows shared mode, every Windows host is an independent node. The account and permission information about users allowed to access the shares are stored on each node. As a result, the information maintenance is complex and uncontrollable. For example, to grant a user the access permission, you need to add the configuration information about this user to every node.

If an AD domain is used, however, the domain controller manages all the user configuration information and authenticates the access to the domain. The domain controller incorporates a database that stores information about the domain account, password, and nodes in the domain. A user can access all the shared content in the domain after passing the authentication by the domain controller.

Working Principles and Panorama

1. Create a DNS server and provide a full AD domain name (such as 123.com) using the server. Other servers only need to input the full domain name and pass the authentication to access the shares.
2. Set up an AD domain on the domain controller side.
3. Add the storage systems that need to provide sharing services to the AD domain.
4. Create a domain user on the domain controller side. Log in to the servers in the AD domain using the domain user account. The shares in the domain can be accessed.


AD domain
(123.com)
Storage system
(AD domain client)
AD domain
controller
3
Network
DNS server
192.168.1.1
2. Create an AD domain.
• Configure the DNS server IP address and full domain name in the AD domain controller.
1. Create a DNS server.
• Provide the full AD domain name (such as 123.com)
3. Add the storage system into the AD domain.
Configure the following parameters of the AD domain controller in the storage system to authorize the storage system to be added to the AD domain controller as a client.
• Administrator name of the AD domain controller
• Password of the AD domain controller
• Full domain name
• Organizational unit (computers by default)
• Name of the storage system in the AD domain
4. Create domain users that can access the shared resources of storage systems.
• Create domain users in the AD domain controller.

Data Preparation

The data to be prepared is as follows: **Domain Administrator Username**, **Password**, **Full Domain Name**, **Organization Unit** (optional), and **System Name**. For details about how to obtain the data, see the parameter description in section "Configuring AD Domain Authentication Parameters".

3.9.2.8.2 Configuring a Storage System to Add It to a DNS Server

After a storage system is connected to a DNS server, you can access the storage system through the IP address or domain name. This operation enables you to configure a system management IP address for the active or standby DNS.

Prerequisites

- The DNS has been configured and is running properly.
- Port 53 of the TCP/UDP protocol between the storage system and the DNS server is enabled.

Context

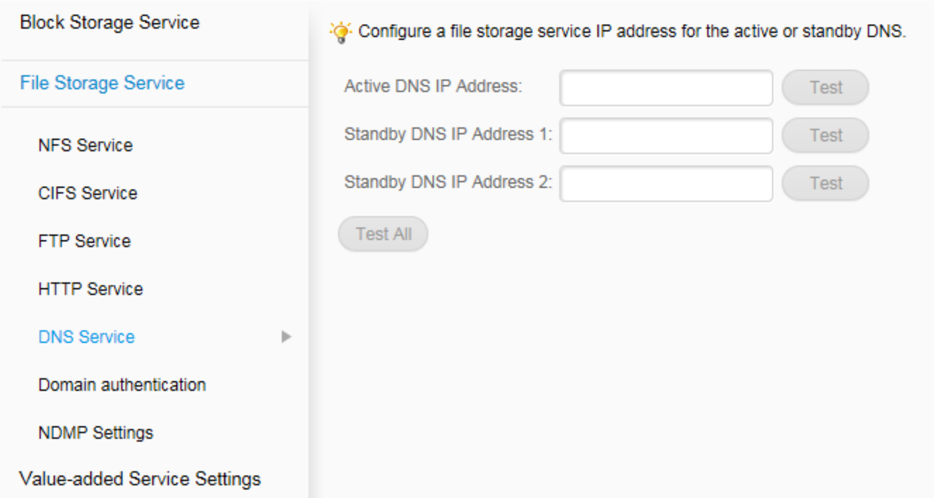
- A DNS server is used to resolve host names in a domain.
- If you want to configure a standby DNS server, keep the domain names of the active and standby servers consistent.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Settings** > **Storage Settings** > **File Storage Service** > **DNS Service**.

Step 3 Set the DNS information.



Configure a file storage service IP address for the active or standby DNS.

Active DNS IP Address:

Standby DNS IP Address 1:

Standby DNS IP Address 2:

1. Set **Active DNS IP Address**.

   NOTE

   You can click **Test** of DNS IP address to test its availability.

2. **Optional:** Set **Standby DNS IP Address 1**.

   NOTE

   You can click **Test** of DNS IP address to test its availability.

3. **Optional:** Set **Standby DNS IP Address 2**.

NOTE

- Configure the standby DNS IP address 1 first and then the standby DNS IP address 2.
- You can click **Test** of DNS IP address to test its availability.

NOTE

You can click **Test All** to test the connection between the DNS server and storage system.

Step 4 Click **Save**.

The **Success** dialog box is displayed, indicating that the operation succeeded.

Step 5 Click **OK**.

----End

3.9.2.8.3 Configuring AD Domain Authentication Parameters

In an AD domain, add a storage system to the AD domain. Then the AD server can authenticate CIFS clients when they try to access shared resources. The administrator can manage the share access permission and quotas of domain users. If the storage system is not added to the AD domain, domain users cannot use share services provided by the share server.

Prerequisites

- An AD domain has been set up.
- The storage system has been connected to the DNS server.
- AD domain server and DNS server have time synchronization with the storage system. The time difference must be no larger than 5 minutes.
- Ports 88, 389, 445, and 464 of the TCP/UDP protocol between the storage system and the AD domain environment are enabled.

NOTE

- The 2000, 5000, and 6000 series storage systems can be connected to the AD domain server and DNS server through the management network port or the service network port (logical port). If the storage system communicates with the AD domain server and DNS server through the management network port, the management network port of each controller must be connected properly to the AD domain server and DNS server. If the storage system communicates with the AD domain server and DNS server through the service network port, the service network port of each controller under each vStore must be connected properly to the AD domain server and DNS server, ensuring that the CIFS services related to the AD domain can be normally used. You are advised to use the service network port to connect to the AD domain server.
- For 6000 series storage systems, every two controllers share one management network port. When the management network port is used to connect to the AD domain server and DNS server, only one controller can be connected to the AD domain server and DNS server. Therefore, in 6000 series storage systems, you are not advised to use the management network port to connect to the AD domain server and DNS server.
- The 18000 series storage systems can be connected to the AD domain and DNS server through the service network port (logical port) only. And it requires all the controllers can communicate with the AD server.
- AD domain servers support the primary/secondary domain, parent/child domain, active/standby domain, or trust domain.

Precautions

- Before adding a storage system to an AD domain, ensure that the primary controller of the storage system has connected to a DNS server and an AD domain server. If it has not, enable the AD domain forwarding function and connect a service port of the storage system to a DNS server and an AD domain server.

NOTE

- Run **show controller general** to query information about all controllers.**Role** indicates the cluster role of a controller. When **Role** is **Master**, this controller is the primary controller of the storage system.
- You can run the **change domain ad_config controller_forwarding_enable=yes** command to enable the AD domain forwarding function. For details, see the **Command Reference** of the corresponding product model.

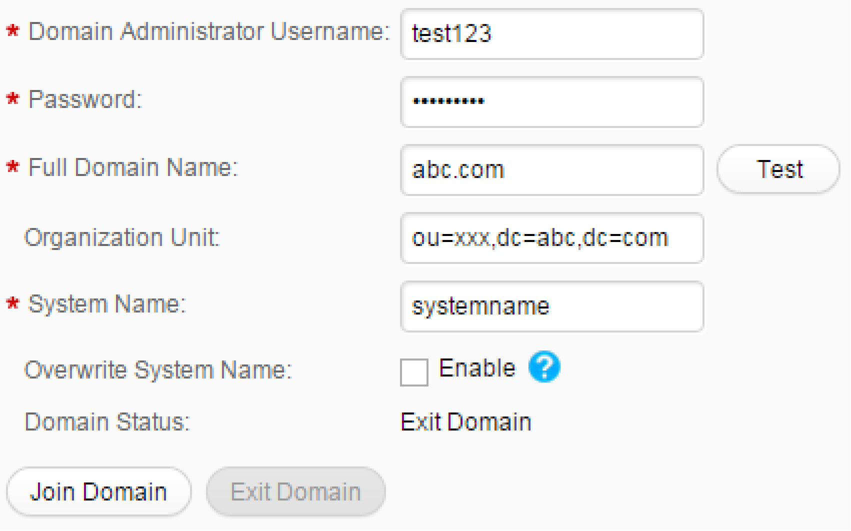
- If **OverWrite System Name** is enabled and the entered system name is the same as that on the AD domain server, information of the existing system will be overwritten by that of the new system.
- Simple password may cause security risk. Complicated password is recommended, for example, password contains uppercases, lowercases, digits and special characters.
- You are advised to use physical isolation and end-to-end encryption to ensure security of data transfer between clients and AD domain servers.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Settings** > **Storage Settings** > **File Storage Service** > **Domain Authentication**.

Step 3 In the **AD Domain Settings** area, configure the AD domain authentication. The related parameters are as shown in **Table 3-39**.



* Domain Administrator Username: test123

* Password: ••••••••••

* Full Domain Name: abc.com

Organization Unit: ou=xxx,dc=abc,dc=com

* System Name: systemname

Overwrite System Name: □ Enable

Domain Status: Exit Domain

Table 3-39 Parameters of the AD domain

Parameter	Description	Value
Domain Administrator Username	User name of an administrator who logs in to the AD domain server.	[Rule] Contains 1 to 63 letters. [Example] test123 [How to Obtain] Contact the administrator of the AD domain controller.
Password	Password of an administrator who logs in to the AD domain server.	[Rule] Contains 1 to 127 letters. [Example] !QAZ2wsx [How to Obtain] Contact the administrator of the AD domain controller.
Full Domain Name	Full domain name of the AD domain server	[Rule] Contains 1 to 127 characters. [Example] abc.com [How to Obtain] Contact the administrator of the AD domain controller.
Organization Unit	Organization unit of a type of directory objects in a domain. These objects include users, computers, and printers. After an object is added to a domain, it will be a member in the organization unit. If you do not enter anything, the storage system is added to organization unit as Computers by default.	If the **Type** of organization units of a domain controller is **Container**, enter **cn=xxx,dc=abc,dc=com**. Otherwise, enter **ou=xxx,dc=abc,dc=com**. [Example] ou=xxx,dc=abc,dc=com [How to Obtain] 1. On the Windows AD domain server, open **Active Directory Users and Computers** or **ADSI Edit**. 2. Select the folder directory on the left and right-click the directory. Choose **Properties**. 3. In the Properties dialog box that is displayed, click **Attribute Editor**. The value of **distinguishedName** is the organization unit.

Parameter	Description	Value
System Name	Name of the storage system in the AD domain. After being added to the domain, the client can use the name to access storage systems.	[Rule] It can contain only letters, digits, and hyphens (-), and must not contain digits only, and contains 1 to 15 letters. [Example] systemname
Overwrite System Name	If a same system name already exists on the domain control server, the existing system name is overwritten after this option is selected.	[Example] Enable
Domain Status	Whether storage system has been added to the domain.	[Example] Exited domain

Step 4 Click **Join Domain**. The AD domain authentication configuration is completed.

----End

Follow-up Procedure

If you want to exit domain, perform the following operations:

1. In **AD Domain Settings**, input **Domain Administrator Username** and **Password**.
2. Click **Exit domain**.

   The **Success** dialog box is displayed indicating that the operation succeeded.
3. Click **OK** to finish exiting the storage system to AD domain.

3.9.2.9 Creating a CIFS share

You may share the file system through CIFS, and user can access the shared storage space.

Prerequisites

- The CIFS service is enabled.
- If it is a non-domain environment, the CIFS authentication mode is configured as local authentication or global authentication.
- If it is an AD domain environment, the CIFS authentication mode is configured as domain authentication or global authentication.

Procedure

Step 1 Log in to DeviceManager.

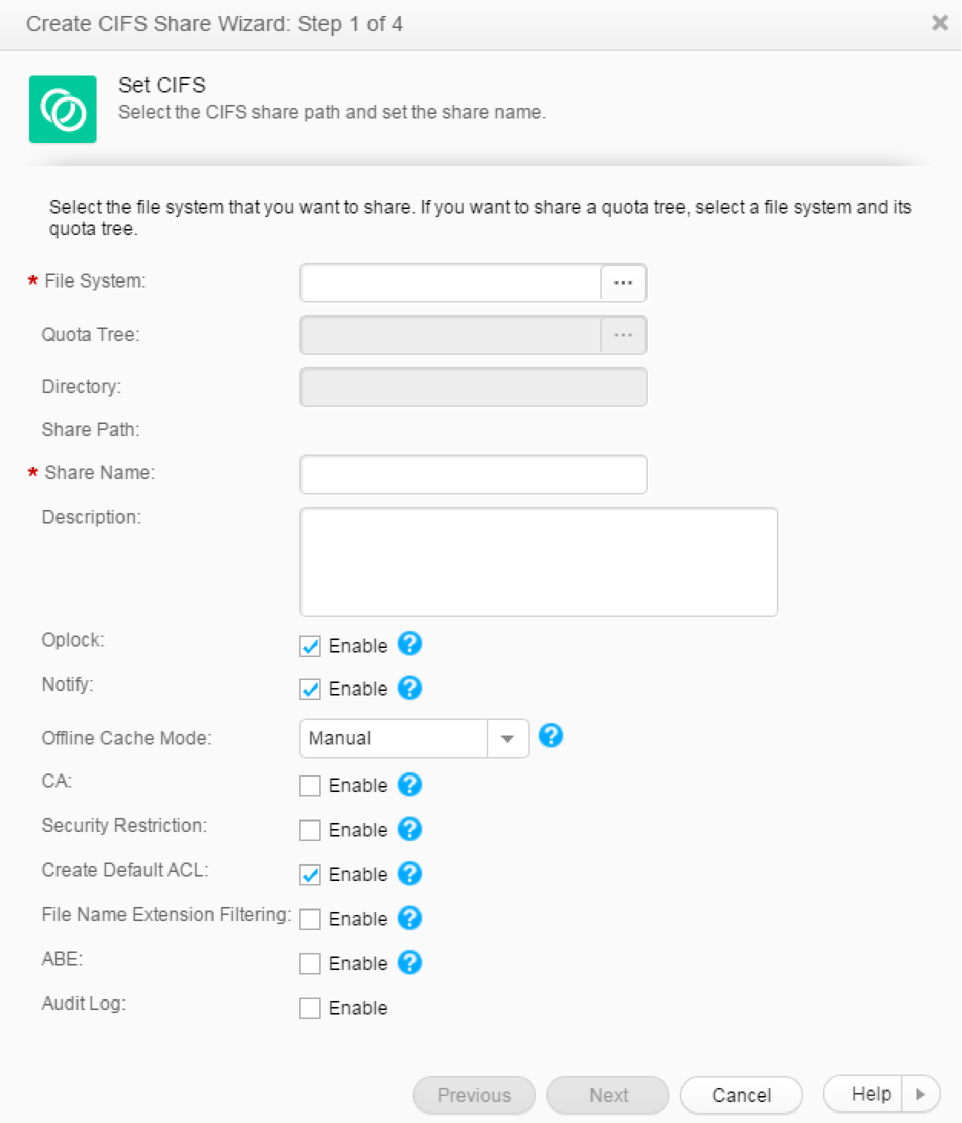
Step 2 Choose **Provisioning** > **Share** > **CIFS (Windows/MAC)**.

Step 3 Click **Create**.

The **Create CIFS Share Wizard** dialog box is displayed.

Step 4 Set CIFS parameters.

1. On the CIFS setting page, configured required parameters.



Create CIFS Share Wizard: Step 1 of 4

Set CIFS

Select the CIFS share path and set the share name.

Select the file system that you want to share. If you want to share a quota tree, select a file system and its quota tree.

* File System:

Quota Tree:

Directory:

Share Path:

* Share Name:

Description:

Oplock: ☑ Enable

Notify: ☑ Enable

Offline Cache Mode: Manual

CA: □ Enable

Security Restriction: □ Enable

Create Default ACL: ☑ Enable

File Name Extension Filtering: □ Enable

ABE: □ Enable

Audit Log: □ Enable

Table 3-40 describes the related parameters.

Table 3-40 Parameters for creating a CIFS share

Parameter	Description	Value
File System	File system for which you want to create a CIFS share. **NOTICE** If the selected file system is the secondary end of the remote replication or HyperVault, data in the file system is probably being modified when it is accessed. Before performing this operation, confirm that the application allows possible data inconsistency. **NOTE** – When global root directory / is selected for **File System**, you can create a CIFS GNS share (Applicable to V300R006C10). ■ You can create multiple GNS shares with different share names for each vStore. ■ After GNS CIFS shares are created, all file systems are mounted to the root directory / by default. By enabling the access based enumeration (ABE) function, you can allow users to or not to visit unauthorized files and file folders. By setting ACL permissions on the file system, you can control user access to a specific file system. ■ GNS root directory / only has read permissions. You cannot create, modify, delete directories or files under /, or modify directory attributes of /. Files or directories cannot be moved across level-1 directories (file systems). ■ Directory names of the CIFS protocol are case insensitive. If file systems have duplicate names with different capitalization, for example file systems **AA** and **aa**, only the file system created earlier or with a smaller file system ID is added to GNS. Change the names of the files with duplicate names and ensure that the names are unique. After the modification is successful, the file system is automatically added to GNS. ■ SMB1 does not support GNS. ■ If GNS is created in the primary vStore of HyperMetro, you can only create a vStore pair when the secondary storage has the same version as that of the primary storage. If a vStore pair is created, you can create a GNS share only when the version of the primary and secondary storage systems is the same and is V3R6C01 or later.	[Example] Filesystem001

Parameter	Description	Value
	NOTE When the internal network of the LAN is stable, you can run the **change service cifs global_namespace_forward_enabled=yes** command to enable the GNS forwarding function so that the performance can be improved when the non-owning controller of the file system is accessed. For details, see the *Command Reference* of the corresponding product model. When the internal network of the LAN is unstable (for example, node fault, upgrade, or IP address failover), you are not advised to enable the GNS forwarding function, which may interrupt services. – After the GNS forwarding function is enabled or disabled, the client needs to remount the share for the client to take effect. In addition, the client may fail to access certain directories. In this case, the client needs to stop services and wait until the client cache times out, and then mount the share. You can also use the dfsutil.exe tool (provided by Microsoft) to clear the client cache and then mount the share. – To use the GNS forwarding function, you need to configure an IP address that can be accessed by the client for the logical port and enable the IP address failover. – If the GNS forwarding function is enabled, the DNS-based load balancing function is affected. To enable the function, you are advised to disable the DNS-based load balancing function. **NOTE** **c$** is the default GNS share whose Share Path is the root directory / and Permission is Full control by Administrators. – Share **c$** cannot be deleted but its properties and permission can be modified. – After a new vStore is created, a **c$** share is automatically created for this vStore. – After the **c$** share is created, you can choose a file system as the share path when creating shares on MMC and do not need to manually enter the share path.	
Quota Tree	Level-1 directory under the root directory of the file system. **NOTE** Quota Tree is not supported for creating GNS.	To share a quota tree, click ... and select a quota tree you want to share. [Example] Share
Directory	Directory or subdirectory under the file system root directory.	[Example] Share01

Parameter	Description	Value
Share Path	The share path of a file system consists of **File System**, **Quota Tree** and **Directory**. **NOTE** The default share path is / for creating GNS.	[Example] /Filesystem001/Share/Share01
Share Name	Name used by a user for accessing the shared resources. **NOTE** If the system has multiple CIFS shares with case-sensitive names in multi-languages (for example, two CIFS shares whose names are **AA** and **aa**), new CIFS shares with the same case-sensitive names as those shares can be created after some of those shares are deleted (for example, after share **AA** is deleted, a new share **AA** can be created). If the system has no CIFS shares with case-sensitive names in multi-languages, new CIFS share names in multi-languages will be case-insensitive (for example, CIFS shares whose names are **AA** and **aa** cannot coexist).	[Value range] - The share name can be letters of any language. - Contain 1 to 80 characters. - Cannot contain special characters "/\ []:|<>+;,?*=. - Cannot be the name reserved by the system. The names reserved by the system are: **ipc$**, **autohome**, **~** and **print$**. [Example] share_for_user1
Description	Description of the created CIFS share.	[Value range] The name contains 0 to 255 characters. [Example] Share for user 1.

Parameter	Description	Value
Oplock	Opportunistic lock (Oplock) is a mechanism used to adjust cache policies of clients, improving performance and network utilization. This function is not recommended in the following scenarios: – Scenarios that have high requirements for data integrity: Local cache loss will occur if your network is interrupted or your client breaks down after Oplock is enabled. If the upper-layer service software does not have a mechanism to ensure data integrity, recovery, or retry, data loss may occur. – Scenarios where multiple clients access the same file: If Oplock is enabled, the system performance will be adversely affected.	[Default value] Enabled
Notify	After this parameter is enabled, a client's operations on a directory, such as adding a sub-directory, adding a new file, modifying the directory, and modifying a file, can be sensed by other clients that are accessing this directory or the parent directory of this directory.	[Default value] Enabled

Parameter	Description	Value
Offline Cache Mode	Cache files to be accessed in different offline cache modes to local clients so that files can be operated offline. The following offline cache modes are supported: – Manual Specified files and programs in the shared directory can be cached to local clients and operated offline. – Documents If a user accesses the shared directory and opens a file or program in the shared directory, the file or program is automatically cached to a local client so that the user can operate it offline. Files and programs that can be operated offline are saved in the cache of clients and they are synchronized with those in the shared directory until the cache is full or users delete them. Files and programs that have not been opened cannot be cached locally. – Programs Performance is optimized based on the Documents mode. If an executable file (EXE or DLL) in the shared directory is executed by a local client, the file is automatically cached to the client. If the client needs to run the executable file online or offline next time, it accesses the cached file instead of that in the shared directory. – None Files and programs in the shared directory cannot be cached to local clients. Therefore, these files and programs cannot be operated offline. This mode prevents the offline file function of clients from creating duplicates of files in the shared directory. **NOTE** The offline file function of clients must be enabled so that files and programs can be automatically cached.	[Default value] Manual
CA	This option is for SMB3.0 continuous availability, only applied to the share for Hyper-V. This feature depends on Oplock, ensure that Oplock is enabled.	[Default value] Disabled

Parameter	Description	Value
Security Restriction	After security restriction is enabled, only the added IP addresses can be used to access devices. If security restriction is not enabled, all IP addresses can be used to access devices.	[Default value] Disabled
Create Default ACL	This function creates a default ACL (full control rights to everyone; applied to the current directory, its subdirectories, and files in them) for a shared CIFS root directory if the directory has no ACL. You can change the default ACL in follow-up operations. If you want to retain the UNIX MODE rights, disable this function. **NOTE** This function cannot be enabled for creating GNS.	[Default value] Enabled
File Name Extension Filtering	After file name extension filtering is enabled, the types of files that users access on a CIFS share are controlled. **NOTE** – SMB2 and SMB3 support file name extension filtering while SMB1 does not support it. – File name extension filtering is used for common CIFS share, excluding Homedir share.	[Default value] Disabled
ABE	After Access Based Enumeration (ABE) is enabled, files and folders that users have no access permission are not displayed. **NOTE** – SMB2 and SMB3 support ABE while SMB1 does not support it. – ABE is used for common CIFS share, excluding Homedir share.	[Default value] Disabled

Parameter	Description	Value
Audit Log	After the audit function is enabled, the system can record audit logs of the shared directory. The audit log items include **Open**, **Create**, **Read**, **Write**, **Close**, **Delete**, **Rename**, **Obtain properties**, **Set properties**, **Obtain security properties**, **Set security properties**, **Obtain extension properties**, and **Set extension properties**. After the audit function is enabled, by default, the system records **Create**, **Write**, **Delete**, and **Rename** operations of the shared directory. **NOTE** Before configuring this function, choose ⚙ **Settings** > 🖥 **Monitor Settings** > **Audit Log Settings**, and enable the **Audit Log Settings** function.	[Default value] Disabled

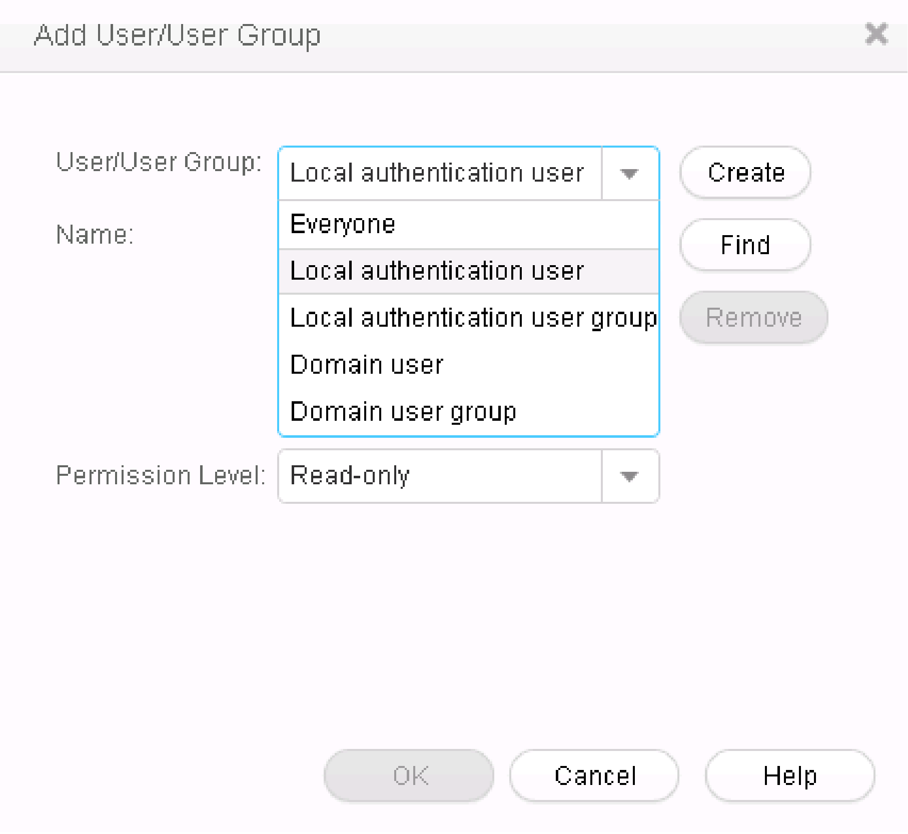
2. Click **Next**.

   The **Set Permissions** page is displayed.

Step 5 Set the permissions of user or user group accessing the CIFS share.

1. In **Users/User Groups** area, click **Add**.

   The **Add User/User Group** dialog box is displayed.



Add User/User Group

User/User Group: Local authentication user

Name:

Permission Level: Read-only

2. In **User/User Group**, select user type or user group type.

   The values include: **Everyone**, **Local authentication user**, **Local authentication user group**, **Domain user** and **Domain user group**.

   - If you select **Everyone**, click **Add**.
   - If you select **Local authentication user** or **Local authentication user group**, click **Find**, in the pop-up **Add User** or **Add User Group** dialog boxes to select the user or user group you want to add. Click **OK**.
   - If the desired local authentication user or user group does not exist, click **Create** to create and add a new authentication user or user group.
   - If you select **Domain user** or **Domain user group**, enter the corresponding name in **Name**, and click **Add**.

     NOTE

     - **Everyone** means every user has the access permission.
     - The name format is **Domain name\Domain user name** or **Domain name\Domain user group name**.

3. In **Permission Level**, select the CIFS access permission for the user or user group added.

   Table 3-41 provides details about the permissions.

Table 3-41 Description of CIFS share permissions

Operation	Forbidden	Read-Only	Read and Write	Full Control
Viewing files and subdirectories	Not allowed	Allowed	Allowed	Allowed
Viewing the contents of files	Not allowed	Allowed	Allowed	Allowed
Running executable files	Not allowed	Allowed	Allowed	Allowed
Adding files or subdirectories	Not allowed	N/A	Allowed	Allowed
Modifying the contents of files	Not allowed	N/A	Allowed	Allowed
Deleting files and subdirectories	Not allowed	N/A	Allowed	Allowed
Renaming	Not allowed	N/A	Allowed	Allowed
Changing the ACL of files or directories	Not allowed	N/A	N/A	Allowed

NOTE

- Priorities in the descending order are **Forbidden**, **Full control**, **Read and write** , and **Read-only**. The permission with the highest priority prevails. When a user's access permission is extended, the new permission takes effect immediately. For example, if a user's original access permission is **Read-only** but the user is added to a user group with **Full control** permission later, the user's access permission changes to **Full control** and it does not need to be re-authenticated to access the CIFS share.
- When the primary group of a local authentication user is the local authentication user group of **Administrators**, the group members can access the shared file system in the storage system without being authenticated by share level ACL and directory and file level NT ACL. They can operate any file in any share with administrator permissions.

4. Click **OK**.

   The system adds the user or user group you select to the **Users/User Groups** list.
5. Click **Next**.

Step 6 (Optional) Set security restriction. This parameter is valid only after security restriction is enabled.

1. In the **Accessible IP Address/Address Segment** area, click **Add**.

   The **Add IP Address or IP Address Segment** dialog box is displayed.
2. In **IP Address/Address Segment**, specify the IP addresses or IP address segments.

   NOTE

   - The IP address segment is in the format of IP address/mask, for example, 192.168.1.100/16. The mask of IPv4 ranges from 1 to 32, and the mask of IPv6 ranges from 1 to 128. A mixed IP address segment (IPv4 and IPv6) is not supported.
   - The IP rule can be:
     - A single IPv4 or IPv6 address, for example, 192.168.1.100.
     - An IP address segment, for example, 192.168.1.100/16 or 192.168.1.10~192.168.1.11/30.
   - A maximum of 32 IP addresses or IP address segments can be added.
3. Click **OK**.

   The added IP addresses or IP address segments are displayed in the list.
4. Click **Next**.

Step 7 (Optional) Set the file name extension filter rule. The rule can be set only after the file name extension filtering function is enabled.

NOTE

File name extension filtering rules are valid only for the current share.

1. In **File Name Extension Filtering Rule**, click **Add**.

   The **Add File Name Extension Filtering Rule** dialog box is displayed.
2. In **File Name Extension**, specify the file name extension (file type) to be filtered.

NOTE

- The file name extension contains 1 to 127 visible ASCII characters, and contains only digits, letters, space, and special characters (!\"#$%&\'()*+\,-.\/\:;\<=\>?@[\\]^_`{\|}~). Wildcard character * can only be the last character. For example, the file name extension can be txt, TXT, T?X, or Tx*.
- The maximum number of filtering items supported by a share is 128.
- The maximum number of filtering items supported by a storage system is 120,000.
- The following are recommended configurations: One share has a maximum of seven file name extension filtering rules, and one file name extension contains 1 to 32 characters (excluding wildcards). The recommended configurations minimize the adverse impact on CIFS service performance. If the recommended configurations are not used, CIFS performance may greatly deteriorate.
- When configuring a file name extension filtering rule, ensure that the rule does not affect the storage of temporary files that may be generated when application software is running. For example, some application software may generate files with the .tmp file name extension. In this case, add the .tmp extension to the file name extension filtering rule. For details about specific temporary file name extension of application software, contact the corresponding software vendor.

3. Select the permission rule from the **Rule Type** drop-down list.

   NOTE

   - **Denied only**: Files with the specified extension do not have access permission.
   - **Allowed only**: Only files with the specified extension have access permission.

4. Click **OK**.

   The added file name extension filter rule is displayed in the list.

5. Click **Next**.

Step 8 The **Summary** page is displayed. On the **Summary** page, check whether the CIFS information is correct. Click **Finish**.

Step 9 On the **Execution Result** page, view the execution result. Click **Close** to finish creating a CIFS share.

You can view the created share in the CIFS share list.

----End

3.9.2.10 Accessing CIFS Shares

This section describes how to access CIFS shares. By accessing a CIFS share, different users can access the shared directory.

Procedure

Step 1 Right-click **Computer** on a Windows-based client.

Step 2 Select **Map Network Drive**.

Step 3 In **Folder**, enter the path of the mapped folder, and select **Connect using different credentials**.

The path format is **\\*logical ip address*\*sharename***, *logical ip address* indicates the logical IP address of the storage system, and *sharename* indicates the name of the CIFS share.

Step 4 Click **Finish**.

Step 5 In **Windows Security**, enter the user name and password of the local user and click **OK**.

- If you use a domain authentication user, enter the domain user name in the **Domain name/Domain user name** format in **User Name** and enter the password of the domain user in **Password**.

  NOTE

  After CIFS shares are allocated to domain users, do not modify the domain user information. Otherwise, the CIFS shares cannot be accessed.

- If you use a local authentication user, enter the user name and password of the local authentication user in **User Name** and **Password** respectively.

Step 6 View the mapped network drive.

Double-click **Computer**. The **Computer** window is displayed, listing mapped network drives.

Step 7 Double-click the mapped network drive to access the CIFS share.

----End

Follow-up Procedure

- To cancel the sharing, run the command **net use [DeviceName] /del** in the Windows CLI. *DeviceName* indicates the disk drive that needs to be disconnected, such as **z:**.
- If the information about a local authentication user or domain user is changed (for example, the user is forbidden, the password is changed or expires, the relationship is changed, or the user is deleted) when a client accesses the file system of CIFS and FTP shares, the changed information will take effect after authentication is passed in the next time (by mounting shares again).
- The storage system supports offline sharing. When a client is mounted and shared, you can still read and write on a local duplicate on the client even when it is disconnected with the storage system. When the connection resumes, data modified offline is synchronized automatically to the storage system. (If the shared data in the storage system is changed, you need to manually start the synchronization.)
- If GNS is created, run command **admin:/>change service cifs global_namespace_capacity=** to set the size of GNS.

3.9.2.11 Connecting Microsoft Management Console to the Storage System

A Windows client refers to a client that runs the Windows operating system. The Microsoft Management Console (MMC) of the Windows client can be used to manage users, user groups, shares, sessions, and open files for storage systems.

3.9.2.11.1 Introduction

This section provides information about the Microsoft Management Console (MMC).

Microsoft Management Console (MMC) is a Windows tool that can provide a unified and standard management interface and operation platform for Windows administrators. With CIFS used, MMC can manage users, user groups, and shares for storage systems.

In large- and medium-sized NAS applications, there exist multiple NAS servers of different vendors. If a NAS administrator has to log in to each NAS server to manage it, the management task is not efficient and error-prone. As a management platform, MMC can manage these servers in a unified way. For this reason, MMC becomes a general-purpose NAS server management tool in the industry.

The following versions of Windows operating systems allow you to use MMC to manage users, user groups, and shares.

- Windows XP
- Windows 7
- Windows Server 2003
- Windows Server 2008
- Windows Server 2012

Table 3-42 lists the supported management functions.

Table 3-42 Management function list

Category	Function	Description
CIFS sharing management	Enumerating shares	Operators must have administrator privileges.
	Adding shares	Restricted by the Windows client, the folder path length cannot be longer than 255 characters when creating shares on Microsoft Management Console. Otherwise, the shares cannot be successfully created.
	Viewing shares	The maximum connection count is fixed at 1 at present.
	Modifying shares	Description, permissions, ACL, and offline cache of shares can be modified.
	Stopping sharing	-
User management	Enumerating users	-
	Viewing user information	The user group to which users belong can be viewed.
	Changing the user group to which users belong	-
User group management	Creating user groups	-
	Enumerating user groups	-
	Viewing user group information	Group members including domain users can be viewed.

Category	Function	Description
	Changing group members	Local users, domain users, and domain user groups can be added to or removed from user groups.
	Modifying user group description	-
	Deleting user groups	-
Session management	Enumerating sessions	-
	Closing sessions	-
Open files management	Enumerating open files	-
	Closing open files	-

3.9.2.11.2 Logging In to Microsoft Management Console

After logging in to the Microsoft Management Console (MMC), you can manage users, user groups, and shares.

Prerequisites

- When you log in to a Windows client as a local user, another local user with the same user name and password has been created on the storage system and added to the **administrators** user group.
- When you log in to a Windows client as a domain user, the storage system has been added to the same domain and the domain user has been added to the **administrators** user group on storage system.
- The client and storage system have joined the same AD domain so that users and user groups can be managed using Windows Management Console.

Procedure

Step 1 Choose **Start** > **Run**. In the text box that is displayed, enter **mmc**.

Step 2 In the pop-up window, choose **File** > **Add/Remove Snap-ins**. In the dialog box that is displayed, select **Shared Folders** and click **Add**.

Step 3 In the dialog box that is displayed, select **Another computer**, enter the front-end service IP address of the storage system, and click **Finish**.

The IP address can be an IPv4 or IPv6 address. Alternatively, you can enter **System Name** that is used when storage system joins the AD domain.

Step 4 Click **OK**.

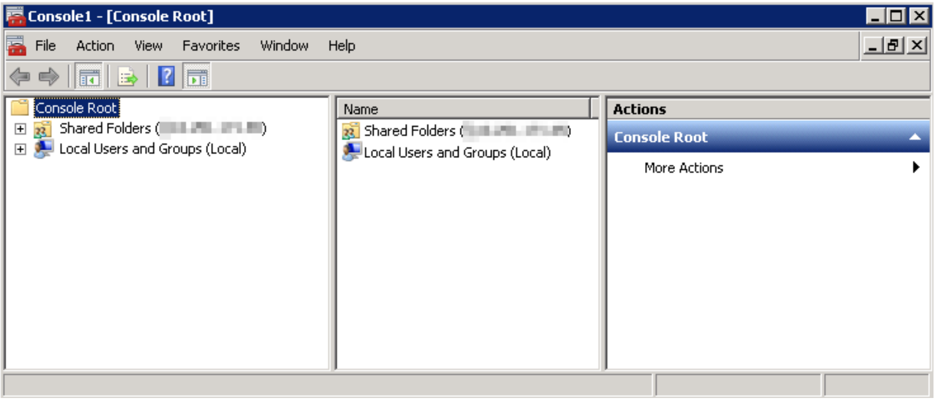
After the addition, you can manage the shares of the storage system.

Step 5 Choose **File** > **Add/Remove Snap-ins**. In the dialog box that is displayed, select **Local Users and Groups** and click **Add**.

Step 6 In the dialog box that is displayed, select **Another computer**, enter the front-end service IP address of the storage system, and click **Finish**.

Step 7 Click **OK**.

After the addition, you can manage the users and user groups.


Console1 - [Console Root]
File
Action
View
Favorites
Window
Help
Console Root
Shared Folders ([redacted])
Local Users and Groups (Local)
Name
Shared Folders ([redacted])
Local Users and Groups (Local)
Actions
Console Root
More Actions

----End

3.9.2.11.3 Managing Shares

After logging in to the Microsoft Management Console (MMC), you can manage users, user groups, and shares.

Prerequisites

- You have logged in to MMC.
- The local administrator has been disabled on the client.

Procedure

- Create a share.
  a. Double-click **Share Folders**.
  b. Right-click **Shares** and choose **NewShare**.
  c. In the **Create A Shared Folder Wizard** dialog box, select a folder that you want to share from storage system.
     - Restricted by the Windows client, the folder path length cannot be longer than 255 characters when creating shares on Microsoft Management Console. Otherwise, the shares cannot be successfully created.
     - Using **Browse** to select a folder from storage system is supported.
  d. Click **Next** and enter a **Share Name** and **Description**.
  e. Click **Next** and select permissions for the folder.
  f. Click **Finish**. In the **Sharing was Successful** dialog box, click **Finish**.
     The created folder will display on MMC.
- View a share.
  a. Choose **Share Folders** > **Shares**.
     - In the window on the right, all CIFS shares of the storage system are listed.

- The client connection count of the share is fixed at 1. The actual value cannot be displayed at present.

b. Right-click the share that you want to view and choose **Properties**. In the dialog box that is displayed, select **Share Permissions** to view the access permission for the share.

- Modify a share.

  a. Choose **Share Folders** > **Shares**.

  In the window on the right, all CIFS shares of the storage system are listed.

  b. Right-click the share that you want to modify and choose **Properties**.

  c. In the dialog box that is displayed, select **General**. In **Description**, change the description.

  d. In the dialog box that is displayed, select **Share Permissions** and modify the permission for the share.

- Stop sharing.

  a. Choose **Share Folders** > **Shares**.

  In the window on the right, all CIFS shares of the storage system are listed.

  b. Right-click the folder that you want to stop sharing and choose **All Tasks** > **Stop Sharing**.

  c. In the dialog box that is displayed, click **Yes**.

----End

3.9.2.11.4 Managing Users and User Groups

After logging in to the Microsoft Management Console (MMC), you can manage users, user groups, and shares.

Prerequisites

- You have logged in to MMC.
- The local administrator has been disabled on the client.
- The client and storage system have joined the same AD domain.

Procedure

- Create user groups.

  a. Choose **Local Users and Groups(Local)** > **Groups**.

  b. Right-click **Groups** and choose **New Group**. Enter user information as instructed and click **Create**.

  NOTE

  It is not supported to create a Windows reservation account through MMC.

- View the user and user group.

  a. Choose **Local Users and Groups(Local)** > **Users**.

  All users will be displayed in the window on the right.

  b. Right-click the user that you want to view and choose **Properties** to view the user details.

c. Choose **Local Users and Groups(Local)** > **Groups**.

All user groups will be displayed in the window on the right.

d. Right-click the user group that you want to view and choose **Properties** to view the user group details.

- Modify users and user groups.
  a. Choose **Local Users and Groups(Local)** > **Users**.
  b. Right-click the user that you want to modify and choose **Properties** > **Member of**.
  c. Select the user group to which the user belongs and click **Remove**.
  d. Click **OK** for the change to take effect.
  e. Choose **Local Users and Groups(Local)** > **Groups**.
  f. Right-click the user group that you want to modify, choose **Properties**, and click **Add** to add users to the user group.
  g. Select the user that you want to remove from the user group and click **Remove**.
  h. Change the user group description in **Description**.
  i. Click **OK** for the change to take effect.

NOTE

The description of a Windows reserved user group cannot be modified through MMC.

- Delete user groups.
  a. Choose **Local Users and Groups(Local)** > **Groups**.
  b. Right-click the user group that you want to delete and select **Delete**.
  c. Read and confirm the risk disclosure statement. In the dialog box that is displayed, click **Yes**. Then the user group is deleted.

----End

3.9.2.11.5 Managing Sessions (Applicable to V300R006C10 and Later Versions)

You can use Windows management console (MMC) to disconnect users and close sessions in shared folders.

Prerequisites

You have logged in to MMC.

Context

If you close sessions without notifying users, user data may be lost. Before closing sessions, notify the users.

When you use MMC to enumerate sessions, Windows will use the IP address of each session to parse the session as the corresponding computer name on the DNS server due to Windows restrictions. You must configure the record for the IP address of each session in the reverse lookup zone of the DNS server. Otherwise, MMC refreshing will time out.

Procedure

- Check a session.

a. Choose **Shared Folders** > **Sessions**.

Details about all current sessions will be displayed in the window on the right.

- Close a session.

a. Choose **Shared Folders** > **Sessions**.

Details about all current sessions will be displayed in the window on the right.

b. Right-click the session you want to close and choose **Close Session** from the shortcut menu.

A confirmation dialog box is displayed.

c. Click **Yes**. The session is closed.

NOTE

If you want to close all sessions, right-click **Sessions** and choose **Disconnect All Sessions** from the shortcut menu.

----End

3.9.2.11.6 Managing Opened Files (Applicable to V300R006C10 and Later Versions)

You can use Windows management console (MMC) to close opened files in shared folders.

Prerequisites

You have logged in to MMC.

Context

When you close an opened file or folder, the users that connect to the file or folder will be disconnected and user data may be lost. Before closing opened files, notify the users.

Procedure

- Check an opened file.

a. Choose **Shared Folders** > **Open Files**.

All files that are opened currently will be displayed in the window on the right.

- Close an opened file.

a. Choose **Shared Folders** > **Open Files**.

All files that are opened currently will be displayed in the window on the right.

b. Right-click the file you want to close and choose **Close Open File** from the shortcut menu.

A confirmation dialog box is displayed.

c. Click **Yes**. The opened file is closed.

NOTE

If you want to close all opened files, right-click **Open Files** and choose **Disconnect All Open Files** from the shortcut menu.

----End

3.9.2.12 CIFS Share Configuration Example

The storage system provides a wide range of functions and solutions to meet customers' service requirements. This section explains some configuration processes that meet typical service requirements.

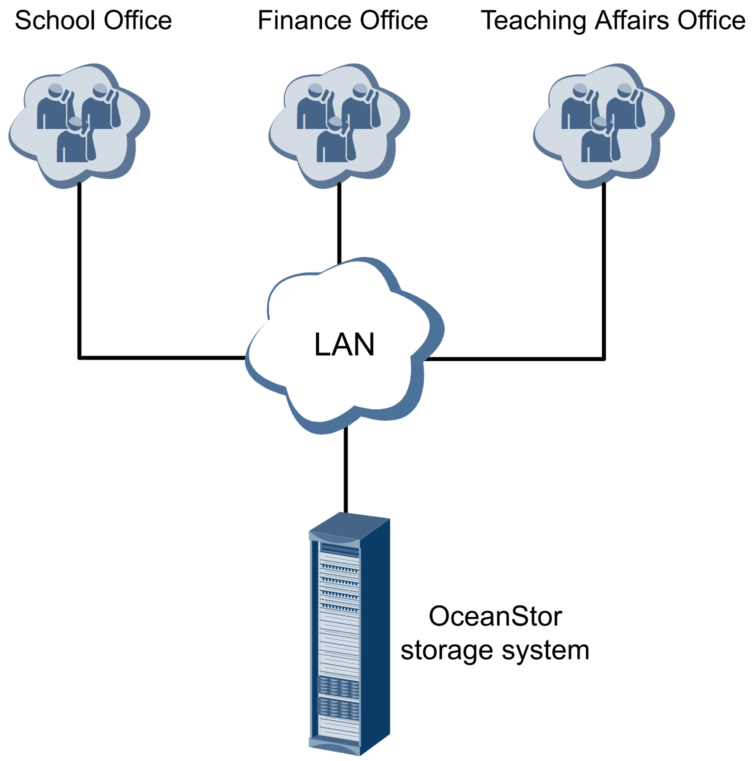
3.9.2.12.1 Scenario

A storage system is required to provide storage space for three departments of a school. Meantime, the three departments must have different permissions. This section describes the customer's existing environment and requirements.

Network Diagram

Figure 3-12 shows the customer's network.

Figure 3-12 Customer's network diagram



The status quo of the customer's live network can be concluded as follows:

- All clients use the Windows operating system.
- The clients of the three departments reside on the same LAN as the storage system.

Customer Requirements

A storage system is required to provide storage space for the School Office, Teaching Affairs Office, and Finance Office. The storage space must be allocated as follows:

- Each of the three departments has 1 TB dedicated storage space.

- The three departments can write and read data in their respective 1 TB storage space.
- The School Office can access but cannot write or modify the storage space of the Teaching Affairs Office and the Finance Office.
- The Teaching Affairs Office can access but cannot write or modify the storage space of the Finance Office.
- The Finance Office can access but cannot write or modify the storage space of the Teaching Affairs Office.
- The Teaching Affairs Office and Finance Office cannot access the storage space of the School Office.

3.9.2.12.2 Requirement Analysis

This section analyzes the customer's requirements and provides a solution.

The customer's requirements are analyzed as follows:

- All clients use the Windows operating system, so the OceanStor storage system can use the CIFS share to provide storage space for the three departments respectively.
- Storage system can manage CIFS share permission. Allocating different permissions to different shares controls the mutual data access of different departments.

Based on the previous analysis, a solution as follows is provided:

- **Table 3-43** describes the basic information of the three departments.

Table 3-43 Basic information of the three departments

Department	Share Name	Share Space	Local User	Local User Group
School Office	share01	1 TB	test_user01	group01
Teaching Affairs Office	share02	1 TB	test_user02	group02
Finance Office	share03	1 TB	test_user03	group03

- **Table 3-44** describes each local user group's permission to access the storage space of the School Office, Finance Office, and Teaching Affairs Office.

Table 3-44 Local user groups' permission to access the storage space of the three departments

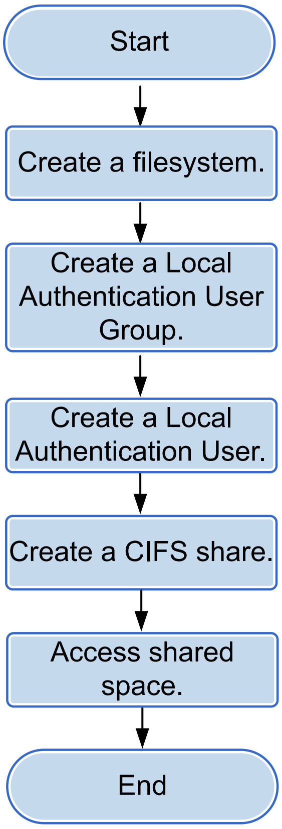
Local User Group	School Office	Finance Office	Teaching Affairs Office
group01	Read-write	Read-only	Read-only
group02	Forbidden	Read-write	Read-only
group03	Forbidden	Read-only	Read-write

3.9.2.12.3 Configuration Process

The preceding solutions and the following configuration flowchart help you understand the subsequent configuration.

Figure 3-13 shows the configuration process.

Figure 3-13 Configuration process


Start
Create a filesystem.
Create a Local Authentication User Group.
Create a Local Authentication User.
Create a CIFS share.
Access shared space.
End

NOTE

This configuration process is only applicable to this configuration example. For the complete configuration process of CIFS share, see **3.9.2.1 Configuration Process**.

3.9.2.12.4 Configuration Operations

After requirement analysis and service planning, you need to configure a CIFS share on DeviceManager.

Creating a File System

File systems provide storage space for CIFS shares. You can create different file systems to provide storage space for different CIFS shares.

Step 1 On the DeviceManager page, choose **Provisioning** > **File System**.

The **File System** page is displayed.

Step 2 Click **Create**.

The **Create File System** dialog box is displayed.

Step 3 In the **Create File System** dialog box, configure planned parameters. **Table 3-45** describes related parameters.

Table 3-45 Create File System parameters

Parameter	Planned Value
Name	FileSystem
Capacity	1 TB
File System Block Size	8 KB
Quantity	3
Owning Storage Pool	StoragePool000

NOTE

- When creating multiple file systems, the storage system automatically appends a number to each file system name based on the number of file systems to be created for identification. Therefore, the file systems that are created are named FileSystem0000, FileSystem0001, and FileSystem0002 respectively.
- Assume the size of most files in the file system is between 100 KB and 1 MB. the file system block size can be set to 8KB.

Step 4 Click **OK**.

----End

Creating a Local Authentication User Group

This section explains how to create a local authentication user group. Local authentication user groups help you control the share access permissions of local users.

Step 1 On the **DeviceManager** page, click **Provisioning** > **User Authentication**.

The **User Authentication** page is displayed.

Step 2 Click **Local Authentication User Group**.

Step 3 Click **Create**.

The **Local Authentication User Group** dialog box is displayed.

Step 4 In **User Group Name**, enter **group01**.

Step 5 Click **OK**.

The system starts adding the user group.

Step 6 In the **Success** dialog box that is displayed, click **OK**.

Step 7 Repeat **Step 3** to **Step 6** to create user groups **group02** and **group03**.

----End

Creating a Local Authentication User

This section describes how to create a local authentication user. For applications that use local authentication, local authentication user accounts are used to access a CIFS share.

Step 1 On the **DeviceManager** page, click **Provisioning** > **User Authentication**.

The **User Authentication** page is displayed.

Step 2 Click **Create**.

The **Local Authentication User** dialog box is displayed.

Step 3 In the **Local Authentication User** dialog box, enter required local user information. **Table 3-46** describes related parameters.

Table 3-46 Local Authentication User parameters

Parameter	Value
Username	test_user01
Password **NOTICE** The default validity period for password is 180 days. When the password expires, the user may not access the share and services may be interrupted. You can modify the validity period for password in **More** > **Set Security Policies**.	Password
Confirm Password	confirms password
Primary Group	group01

Step 4 Click **OK**.

The system starts adding the user.

Step 5 In the **Success** dialog box that is displayed, click **OK**.

Step 6 Repeat **Step 2** to **Step 5** to add users **test_user02** and **test_user03** respectively to user groups **group02** and **group03**.

----End

Creating a CIFS Share

After creating a local user group and local users, you need to create a CIFS share. You can assign different permissions to different users when creating a CIFS share.

Step 1 On the DeviceManager page, choose **Provisioning** > **Share**.

The **Share** page is displayed.

Step 2 Create a CIFS share.

1. Choose **CIFS (Windows/MAC)** > **Create**.

   The **Create CIFS Share Wizard** page is displayed.

2. In **File System**, select file system **FileSystem0000** which the CIFS share belongs. In **Share Name**, enter the planned CIFS share name **share01**.

3. Click **Next**.

   The **Set Permissions** page is displayed.

4. Click **Next**.

   The **Permissions are not configured for users or user groups to access the CIFS share. Are you sure to continue?** dialog box is displayed.

   NOTE

   Access permission configurations for the CIFS share are introduced in **Step 4**.

5. Click **OK**.

   The **Summary** page is displayed.

6. Click **Finish**.

   The **Execution Result** page is displayed.

7. Click **Close**.

Step 3 Repeat **Step 2** to add CIFS shares **share02** and **share03**.

Step 4 Configure access permissions for the CIFS share.

1. Select **share01**.

2. In **Users/User Groups**, click **Add**.

   The **Add User/User Group** dialog box is displayed.

3. In **User/User Group**, select **Local user group**. In **Name**, click **Find**.

   The **Select User Group** dialog box is displayed.

4. Select user group **group01** and click **OK**.

   The **Add User/User Group** dialog box is displayed.

5. In **Permission Level**, select **Read-write**. Click **OK**.

   The **Execution Result** page is displayed.

6. Click **Close**.

Step 5 Repeat **Step 4** to configure different access permissions for different user groups. **Table 3-47** lists planned access permissions.

Table 3-47 Access permission planning

User Group	share01	share02	share03
group01	Read-write	Read-only	Read-only
group02	Forbidden	Read-write	Read-only
group03	Forbidden	Read-only	Read-write

----End

Accessing Shared Space

After a CIFS share is configured, users need to map the shared space provided by the storage system to the network drive on the client. This section describes how to map the network drive on a client of the School Office. You can map the network drives on the other clients in the same way. Note that user names **test_user02** and **test_user03** must be used to map the network drives on the clients of the Teaching Affairs Office and Finance Office.

Step 1 Map a network drive to a client.

1. Right-click **Computer** on a Windows-based client.
2. Select **Map Network Drive**.
3. In **Folder**, enter \\172.16.150.40\share01, and select **Connect using different credentials**.

   172.16.150.40 is the logical IP address of the storage system.
4. Click **Finish**.

Step 2 Authenticate the user.

1. In the **Windows Security** dialog box, enter local user name **test_user01** in **User Name**.
2. In **Password**, enter the password of user **test_user01**.
3. Click **OK**.

Step 3 View the mapped network drive.

Double-click **Computer**. The **Computer** window is displayed, listing mapped network drives.

----End

3.9.2.13 CIFS GNS Share Configuration Example (Applicable to V300R006C10 and Later Versions)

The storage system provides a wide range of functions and solutions to meet customers' service requirements. This section explains some configuration processes that meet typical service requirements.

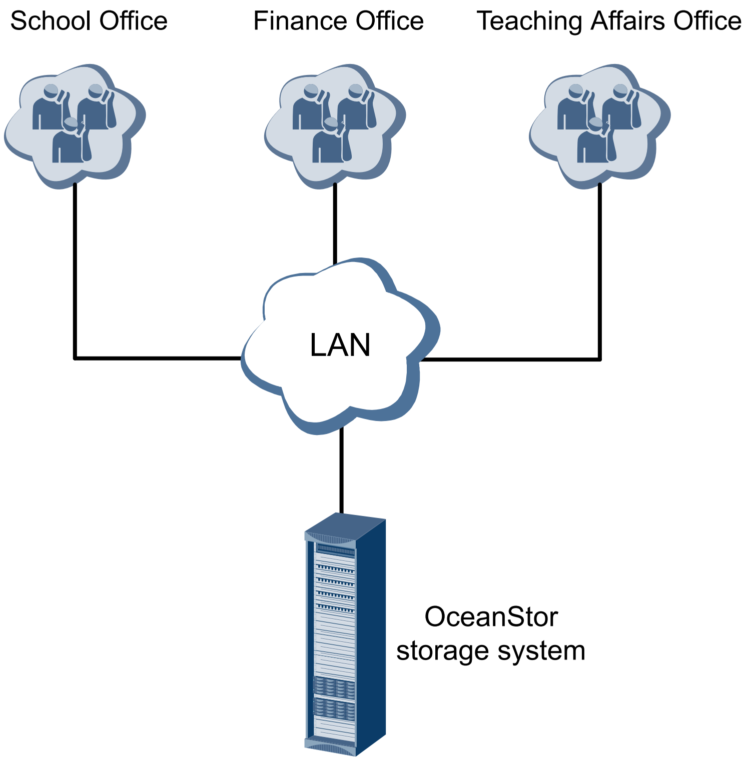
3.9.2.13.1 Scenario

The storage administrator of a school needs to manage the contents of all departments on a management interface. This section describes the customer's live network environment and detailed requirements.

Network Diagram

Figure 3-14 shows the customer's network.

Figure 3-14 Customer's network diagram



The status quo of the customer's live network can be concluded as follows:

- All clients use the Windows operating system.
- The clients of the three departments reside on the same LAN as the storage system.

Customer Requirements

A storage system is required to provide storage space for the School Office, Teaching Affairs Office, and Finance Office. The storage space must be allocated as follows:

- The Teaching Affairs Office and Finance Office have 1 TB dedicated storage space each.
- The Teaching Affairs Office and Finance Office can write and read data in their respective 1 TB storage space.
- The School Office can access, write, and modify the storage space of the Teaching Affairs Office and the Finance Office.

3.9.2.13.2 Requirement Analysis

This section analyzes the customer's requirements and provides a solution.

The customer's requirements are analyzed as follows:

- All clients use the Windows operating system, so the OceanStor storage system can use the CIFS share to provide storage space for the three departments respectively.
- Storage system can manage CIFS share permission. Allocating different permissions to different shares controls the mutual data access of different departments.

Based on the previous analysis, a solution as follows is provided:

- **Table 3-48** describes the basic information of the three departments.

Table 3-48 Basic information of the three departments

Department	Share Name	Share Space	Local User	Local User Group
School Office	share01	1 TB	office_user01	group01
Teaching Affairs Office	share02	1 TB	test_user02	group02
Finance Office	share03	1 TB	test_user03	group03

- **Table 3-49** describes each local user group's permission to access the storage space of the School Office, Finance Office, and Teaching Affairs Office.

Table 3-49 Local user groups' permission to access the storage space of the three departments

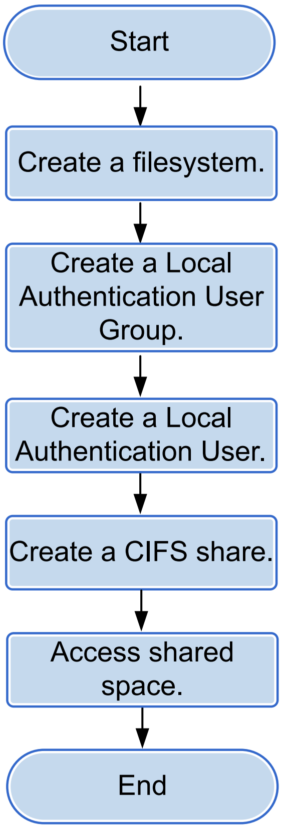
Local User Group	School Office	Finance Office	Teaching Affairs Office
group01	Read-write	Read-write	Read-write
group02	Forbidden	Read-write	Read-only
group03	Forbidden	Read-only	Read-write

3.9.2.13.3 Configuration Process

The preceding solutions and the following configuration flowchart help you understand the subsequent configuration.

Figure 3-15 shows the configuration process.

Figure 3-15 Configuration process


Start
Create a filesystem.
Create a Local Authentication User Group.
Create a Local Authentication User.
Create a CIFS share.
Access shared space.
End

NOTE

This configuration process is only applicable to this configuration example. For the complete configuration process of CIFS share, see **3.9.2.1 Configuration Process**.

3.9.2.13.4 Configuration Operations

After requirement analysis and service planning, you need to configure a CIFS share on DeviceManager.

Creating a File System

File systems provide storage space for CIFS shares. You can create different file systems to provide storage space for different CIFS shares.

Step 1 On the DeviceManager page, choose **Provisioning** > **File System**.

The **File System** page is displayed.

Step 2 Click **Create**.

The **Create File System** dialog box is displayed.

Step 3 In the **Create File System** dialog box, configure planned parameters. **Table 3-50** describes related parameters.

Table 3-50 Create File System parameters

Parameter	Planned Value
Name	FileSystem
Capacity	1 TB
File System Block Size	8 KB
Quantity	2
Owning Storage Pool	StoragePool000

NOTE

- When creating multiple file systems, the storage system automatically appends a number to each file system name based on the number of file systems to be created for identification. Therefore, the file systems that are created are named FileSystem0000 and FileSystem0001 respectively.
- Assume the size of most files in the file system is between 100 KB and 1 MB. the file system block size can be set to 8KB.

Step 4 Click **OK**.

----End

Creating a Local Authentication User Group

This section explains how to create a local authentication user group. Local authentication user groups help you control the share access permissions of local users.

Step 1 On the **DeviceManager** page, click **Provisioning** > **User Authentication**.

The **User Authentication** page is displayed.

Step 2 Click **Local Authentication User Group**.

Step 3 Click **Create**.

The **Local Authentication User Group** dialog box is displayed.

Step 4 In **User Group Name**, enter **group01**.

Step 5 Click **OK**.

The system starts adding the user group.

Step 6 In the **Success** dialog box that is displayed, click **OK**.

Step 7 Repeat **Step 3** to **Step 6** to create user groups **group02** and **group03**.

----End

Creating a Local Authentication User

This section describes how to create a local authentication user. For applications that use local authentication, local authentication user accounts are used to access a CIFS share.

Step 1 On the **DeviceManager** page, click **Provisioning** > **User Authentication**.

The **User Authentication** page is displayed.

Step 2 Click **Create**.

The **Local Authentication User** dialog box is displayed.

Step 3 In the **Local Authentication User** dialog box, enter required local user information. **Table 3-51** describes related parameters.

Table 3-51 Local Authentication User parameters

Parameter	Value
Username	office_user01
Password NOTICE The default validity period for password is 180 days. When the password expires, the user may not access the share and services may be interrupted. You can modify the validity period for password in **More** > **Set Security Policies**.	Password
Confirm Password	confirms password
Primary Group	group01

Step 4 Click **OK**.

The system starts adding the user.

Step 5 In the **Success** dialog box that is displayed, click **OK**.

Step 6 Repeat **Step 2** to **Step 5** to add users **test_user02** and **test_user03** respectively to user groups **group02** and **group03**.

----End

Creating a CIFS GNS Share

After creating a local user group and local users, you need to create a CIFS GNS share. You can assign different permissions to different users when creating a CIFS GNS share.

Step 1 On the DeviceManager page, choose **Provisioning** > **Share**.

The **Share** page is displayed.

Step 2 Create a CIFS share.

1. Choose **CIFS (Windows/MAC)** > **Create**.

   The **Create CIFS Share Wizard** page is displayed.

2. In **File System**, select /. In **Share Name**, enter the planned share name **share01**.
3. Click **Next**.

   The **Set Permissions** page is displayed.

4. Click **Next**.

   The **Permissions are not configured for users or user groups to access the CIFS share. Are you sure to continue?** dialog box is displayed.

   NOTE

   Access permission configurations for the CIFS share are introduced in **Step 4**.

5. Click **OK**.

   The **Summary** page is displayed.

6. Click **Finish**.

   The **Execution Result** page is displayed.

7. Click **Close**.

Step 3 Repeat **Step 2** to add CIFS shares **share02** and **share03** for **FileSystem0000** and **FileSystem0001** respectively.

Step 4 Configure access permissions for the CIFS share.

1. Select **share01**.
2. In **Users/User Groups**, click **Add**.

   The **Add User/User Group** dialog box is displayed.

3. In **User/User Group**, select **Local user group**. In **Name**, click **Find**.

   The **Select User Group** dialog box is displayed.

4. Select user group **group01** and click **OK**.

   The **Add User/User Group** dialog box is displayed.

5. In **Permission Level**, select **Read-write**. Click **OK**.

   The **Execution Result** page is displayed.

6. Click **Close**.

Step 5 Repeat **Step 4** to configure different access permissions for different user groups. **Table 3-52** lists planned access permissions.

Table 3-52 Access permission planning

User Group	share01	share02	share03
group01	Read-write	Read-write	Read-write
group02	Forbidden	Read-write	Read-only
group03	Forbidden	Read-only	Read-write

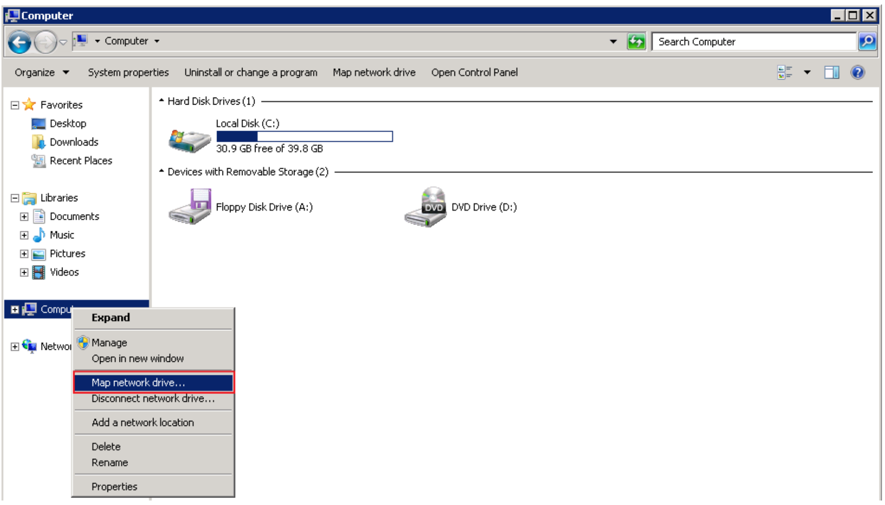
----End

Accessing Shared Space

After a CIFS GNS share is configured, users need to map the shared space provided by the storage system to the network drive on the client. This section describes how to map the network drive on a client of the School Office. You can map the network drives on the other clients in the same way. Note that user names **test_user02** and **test_user03** must be used to map the network drives on the clients of the Teaching Affairs Office and Finance Office.

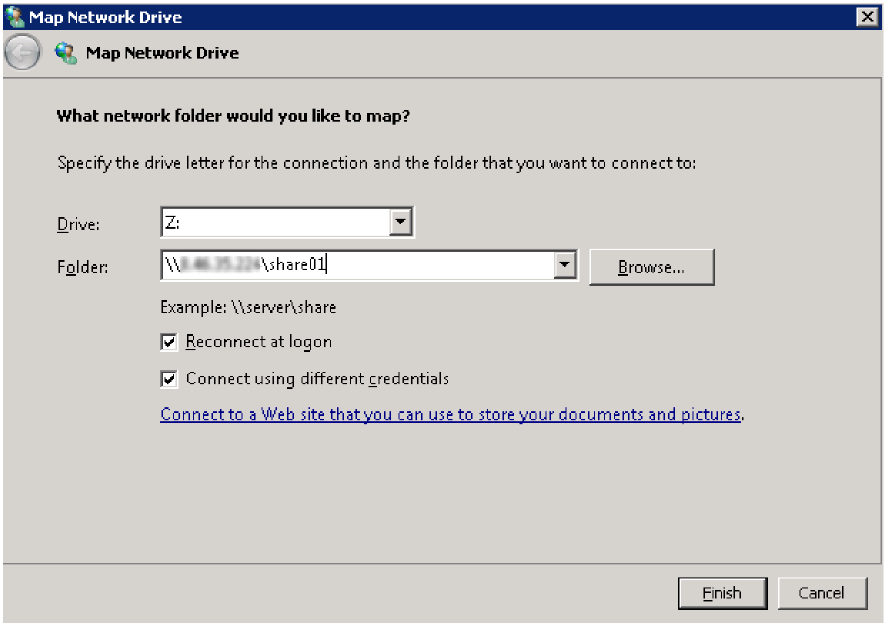
Step 1 Map a network drive to a client.

1. Right-click **Computer** on a Windows-based client, and select **Map Network Drive**.



2. In **Folder**, enter **\\172.16.150.40\share01**, and select **Connect using different credentials**.

   172.16.150.40 is the logical IP address of the storage system.



What network folder would you like to map?

Specify the drive letter for the connection and the folder that you want to connect to:

Drive: Z:

Folder: \\[redacted]\share01

Browse...

Example: \\server\share

☑ Reconnect at logon

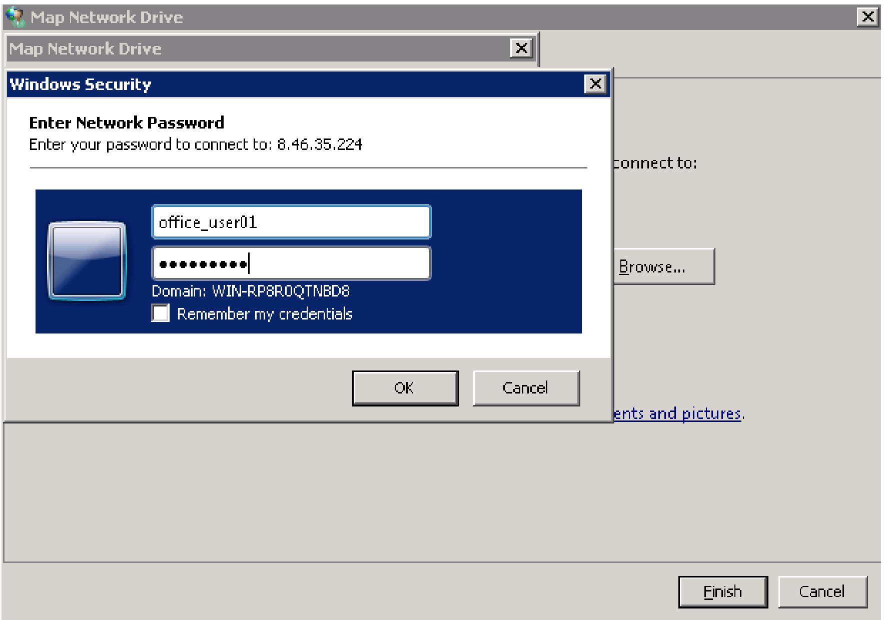
☑ Connect using different credentials

Connect to a Web site that you can use to store your documents and pictures.

3. Click **Finish**.

Step 2 Authenticate the user.

1. In the **Windows Security** dialog box, enter local user name **office_user01** in **User Name**.
2. In **Password**, enter the password of user **test_user01**.



Enter Network Password

Enter your password to connect to: 8.46.35.224

office_user01

•••••••••

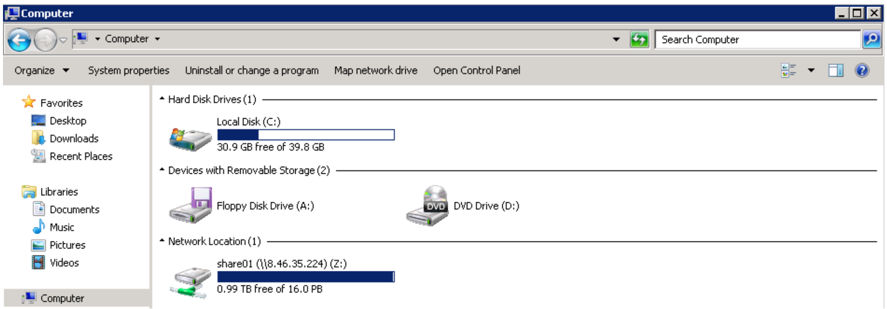
Domain: WIN-RP8R0QTNBD8

☐ Remember my credentials

3. Click **OK**.

Step 3 View the mapped network drive.

Double-click **Computer**. The **Computer** window is displayed, listing mapped network drives.



Hard Disk Drives (1)

Local Disk (C:)
30.9 GB free of 39.8 GB

Devices with Removable Storage (2)

Floppy Disk Drive (A:)

DVD Drive (D:)

Network Location (1)

share01 (\\8.46.35.224) (Z:)
0.99 TB free of 16.0 PB

----End

3.9.3 Configuring a CIFS Homedir Share

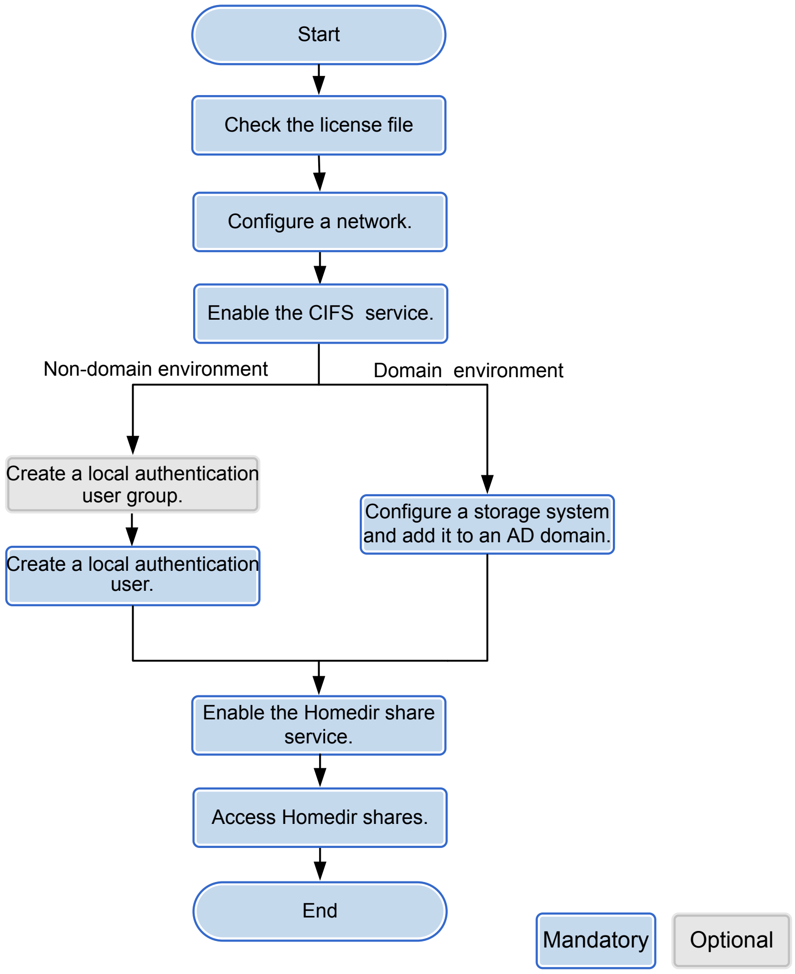
Home Directory (Homedir for short) is a private directory that can save private data of users. You can configure a CIFS Homedir share either in a non-domain environment or an AD domain. This section describes how to configure a CIFS Homedir share.

3.9.3.1 Configuration Process (Applicable to V300R006C00)

This section describes the process of configuring a CIFS Homedir share.

Figure 3-16 shows the flowchart for configuring a CIFS Homedir share.

Figure 3-16 Flowchart for configuring a CIFS Homedir share

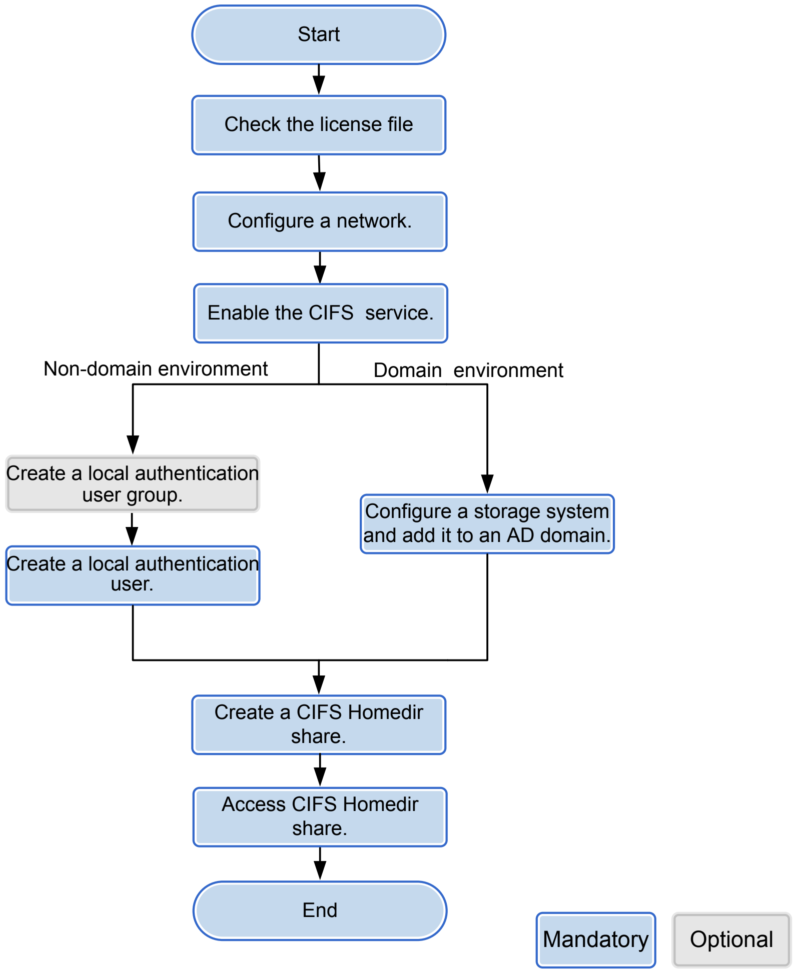

Start
Check the license file
Configure a network.
Enable the CIFS service.
Non-domain environment
Domain environment
Create a local authentication user group.
Create a local authentication user.
Configure a storage system and add it to an AD domain.
Enable the Homedir share service.
Access Homedir shares.
End
Mandatory
Optional

3.9.3.2 Configuration Process (Applicable to V300R006C10)

This section describes the process of configuring a CIFS Homedir share.

Figure 3-17 shows the flowchart for configuring a CIFS Homedir share.

Figure 3-17 Flowchart for configuring a CIFS Homedir share


Start
Check the license file
Configure a network.
Enable the CIFS service.
Non-domain environment
Domain environment
Create a local authentication user group.
Create a local authentication user.
Configure a storage system and add it to an AD domain.
Create a CIFS Homedir share.
Access CIFS Homedir share.
End
Mandatory
Optional

3.9.3.3 Checking the License File

Each value-added feature requires a license file for activation. Before configuring a value-added feature, ensure that its license file is valid for the feature.

Context

On the DeviceManager interface, CIFS Homedir feature is displayed in **Feature** of **CIFS Protocol**.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Settings** > **License Management**.

Step 3 Check the active license files.

1. In the navigation tree on the left, choose **Active License**.
2. In the middle information pane, verify the information about active license files.

----End

Follow-up Procedure

- If the information about the license of the feature is not displayed on the **Active License** page, apply for and import a license file as instructed in the *Installation Guide* of the corresponding product model.
- If the storage system generates an alarm indicating that the license expired, purchase and import another license file.

3.9.3.4 Configuring a Network

This section describes how to use DeviceManager to configure a logical IP address for a storage system. The logical IP address is used for accessing shares.

3.9.3.4.1 (Optional) Configuring DNS-based Load Balancing Parameters (Applicable to V300R006C10 and Later Versions)

Storage arrays' DNS-based load balancing feature can detect the IP address load on the arrays in real time and use a proper IP address as the DNS response to achieve load balancing among IP addresses. This section describes how to configure DNS-based load balancing and DNS zones.

Context

Working principle:

1. When a host accesses the NAS service of a storage array using the domain name, the host first sends a DNS request to the built-in DNS server of the storage array and the DNS server obtains the IP address according to the domain name.
2. When a domain name contains multiple IP addresses, the storage array selects the IP address with a light load as the DNS response based on the configured load balancing policy and returns the DNS response to the host.
3. After receiving the DNS response, the host sends a service request to the destination IP address.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Settings** > **Storage Settings** > **File Storage Service** > **DNS-based Load Balancing**.

Step 3 Table 3-53 lists parameters related to DNS-based load balancing.

Table 3-53 DNS-based load balancing parameters

Parameter	Description	Value
DNS-based Load Balancing	Enables or disables DNS-based load balancing. **NOTE** ● When enabling the DNS-based load balancing function, you are advised to disable the global namespace forwarding function. This function affects DNS-based load balancing. ● After the DNS-based load balancing function is disabled, the domain name resolution service is unavailable and file systems cannot use the function. ● This parameter can be set only in the system view, not in the vStore view. The setting takes effect for the entire storage system.	[Example] Enable

Parameter	Description	Value
Load Balancing Policy	This parameter enables you to configure DNS-based load balancing policies. A storage system supports the following load balancing policies: ● Weighted round robin: When a client uses a domain name to initiate an access request, the storage system calculates the weight based on the performance data. Under the same domain name, IP addresses that are required to process loads have the same probability to be selected to process client services. ● CPU usage: When a client uses a domain name to initiate an access request, the storage system calculates the weight based on the CPU usage of each node. Using the weight as the probability reference, the storage system selects a node to process the client's service request. ● Bandwidth usage: When a client uses a domain name to initiate an access request, the storage system calculates the weight based on the total bandwidth usage of each node. Using the weight as the probability reference, the storage system selects a node to process the client's service request. ● Open connections: When a client uses a domain name to initiate an access request, the storage system calculates the weight based on the NAS connections of each node. Using the weight as the probability reference, the storage system selects a node to process the client's service request. ● Overall load: When a client uses a domain name to initiate an access request, the storage system selects a node to process the client's service request based on the comprehensive load. The comprehensive node load is calculated based on the CPU usage, bandwidth usage, and number of NAS connections. Less	[Example] Weighted round robin

Parameter	Description	Value
	loaded nodes are more likely to be selected. NOTE This parameter can be set only in the system view, not in the vStore view. The setting takes effect for the entire storage system.	

Step 4 Configure a DNS zone.

A DNS zone contains IP addresses of a group of logical ports. A host can use the name of a DNS zone to access shared services provided by a storage system. Services can be evenly distributed to logical ports.

NOTE

Only the logical ports whose **Role** is **Service** or **Management+Service** can be added into a DNS zone. The logical ports whose **Role** is **Management** cannot be added in to a DNS zone.

1. Add a DNS zone.
   a. Click **Add**.
   b. The **Add DNS Zone** dialog box is displayed. In **Domain Name**, type the domain name of the DNS zone you want to add and click **OK**.

      NOTE

      The domain name complexity requirements are as follows:

      - A domain name contains 1 to 255 characters and consists of multiple labels separated by periods (**.**).
      - A label contains 1 to 63 characters including letters, digits, hyphens (-), and underscores (_), and must start and end with a letter or a digit.
      - The domain name must be unique.
2. Remove a DNS zone.
   a. In the DNS zones that are displayed, select a DNS zone you want to remove.
   b. Click **Remove**.
3. Modify a DNS zone.
   a. In the DNS zones that are displayed, select a DNS zone you want to modify.
   b. Click **Modify**.
   c. The <**Modify DNS Zone** dialog box is displayed. In **Domain Name**, type the domain name of the DNS zone you want to modify and click **OK**.
4. View a DNS zone.
   a. In **DNS Zone**, type a keyword and click **Search**.
   b. In **DNS Zone**, the DNS zone names relevant to the keyword will be displayed.

      NOTE

      You can select a DNS zone to modify or remove it.

Step 5 Click **Save**. The **Warning** dialog box is displayed.

Step 6 Confirm the information in the dialog box and select **I have read and understand the consequences associated with performing this operation**.

Step 7 Click **OK**. The **Execution Result** page is displayed.

Step 8 On the **Execution Result** page, confirm the modification and click **Close**. The DNS zone configuration is complete.

----End

Follow-up Procedure

Choose **Provisioning** > **Port** > **Logical Ports** to configure **Listen DNS Query Request** and **DNS Zone** information for logical ports.

3.9.3.4.2 Creating a Logical Port

This operation enables you to create a logical port for managing and accessing file based on Ethernet ports, bond ports, or VLANs.

Precautions

The number of logical ports created for each controller is recommended not more than 64. If the number exceeds 64 and a large number of ports do not work properly, logical ports drift towards the small number of ports available. As a result, service performance deteriorates.

Procedure

Step 1 Log in to DeviceManager.

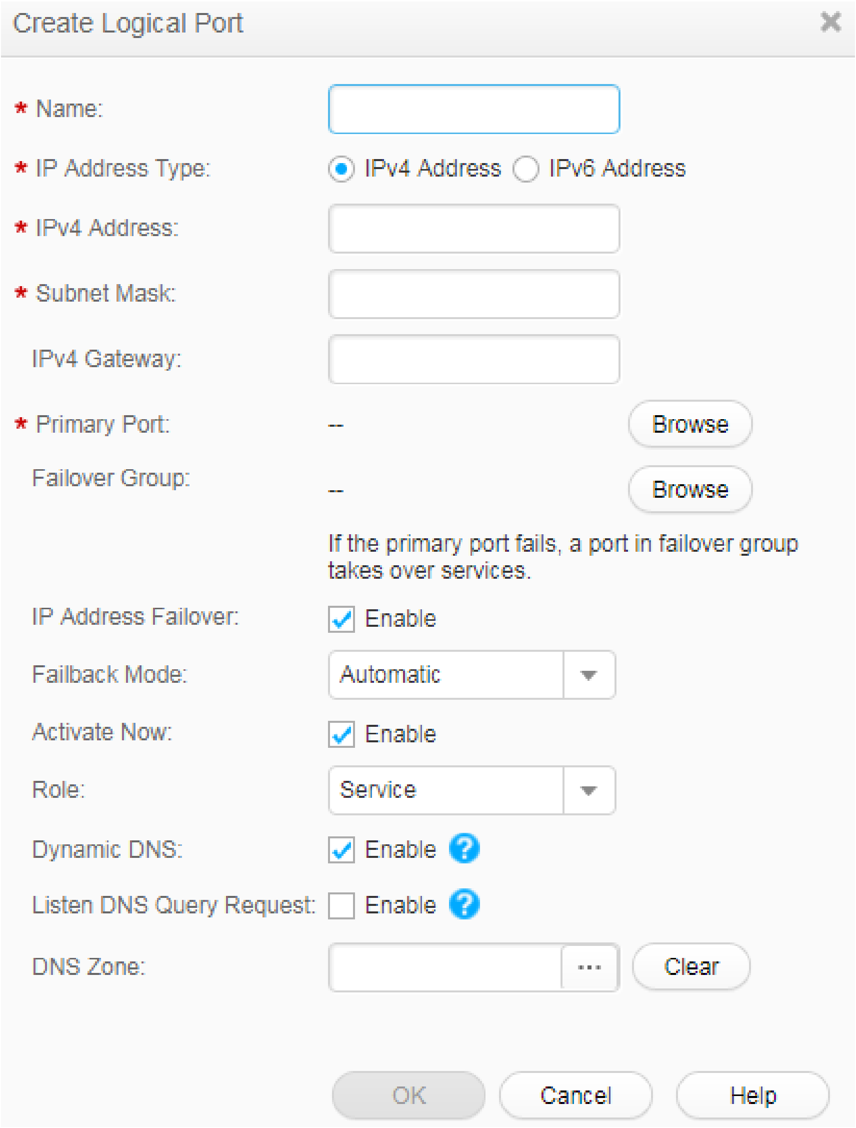
Step 2 Choose **Provisioning** > **Port** > **Logical Ports**.

Step 3 Click **Create**.

The **Create Logical Port** dialog box is displayed.

Step 4 In the **Create Logical Port** dialog box, configure related parameters.

Table 3-54 describes related parameters.



Create Logical Port

* Name:

* IP Address Type: ● IPv4 Address ○ IPv6 Address

* IPv4 Address:

* Subnet Mask:

IPv4 Gateway:

* Primary Port: --

Failover Group: --

If the primary port fails, a port in failover group takes over services.

IP Address Failover: ☑ Enable

Failback Mode: Automatic

Activate Now: ☑ Enable

Role: Service

Dynamic DNS: ☑ Enable

Listen DNS Query Request: □ Enable

DNS Zone:

Table 3-54 Logical port parameters

Parameter	Description	Value
Name	Name of the logical port. The name must meet the following requirements so that the logical port is available to compatible applications: ● The name must be unique. ● The name can contain only letters, digits, underscores (_), periods (.), and hyphens (-). ● The name contains 1 to 31 characters.	[Example] lif01
IP Address Type	IP address type of the logical port, including IPv4 or IPv6.	[Example] IPv4
IPv4 Address	IPv4 address of the logical port.	[Example] 192.168.100.11
Subnet Mask	IPv4 subnet mask of the logical port.	[Example] 255.255.0.0
IPv4 Gateway	IPv4 gateway of the logical port.	[Example] 192.168.100.1
IPv6 Address	IPv6 address of the logical port.	[Example] fc00::1234
Prefix	IPv6 prefix length of the logical port.	[Example] 64
IPv6 Gateway	IPv6 gateway of the logical port.	[Example] fc00::1
Primary Port	Port to which the logical port belongs, including the Ethernet port, Bond port, and VLAN.	[Example] None

Parameter	Description	Value
Failover Group	Failover group name. **NOTE** ● If a failover group is specified, services on the failed primary port will be taken over by a port in the specified failover group. ● If no failover group is specified, services on the failed primary port will be taken over by a port in the default failover group.	[Example] None
IP Address Failover	After IP address failover is enabled, services are failed over to other normal ports within the failover group if the primary port fails. However, the IP address used by services remains unchanged. **NOTE** Shares of file systems do not support the multipathing mode. IP address failover is used to improve reliability of links.	[Example] Enable
Failback Mode	Mode in which services fail back to the primary port after the primary port is recovered. The mode can be manual or automatic. **NOTE** ● If **Failback Mode** is **Manual**, ensure that the link to the primary port is normal before the failback. Services will manually fail back to the primary port only when the link to the primary port keeps normal for over five minutes. ● If **Failback Mode** is **Automatic**, ensure that the link to the primary port is normal before the failback. Services will auto fail back to the primary port only when the link to the primary port keeps normal for over five minutes.	[Example] Automatic

Parameter	Description	Value
Activate Now	To activate the logical port immediately.	[Example] Enable
Role	Roles of logical ports include the following: ● Management: The port is used by a super administrator to log in to the system for management. ● Service: The port is used by a super administrator to access services such as file system CIFS shares. ● Management+Service: The port is used by a super administrator to log in to the system to manage the system and access services.	[Example] Service
Dynamic DNS	When the dynamic DNS is enabled, the DNS server will automatically and periodically update the IP address configured for the logical port.	[Example] Enable
Listen DNS Query Request	After this function is enabled, external NEs can access the DNS service provided by the storage system by using the IP address of this logical port.	[Example] Enable

Parameter	Description	Value
DNS Zone	Name of a DNS zone. **NOTE** ● If the value is blank, the logical port is not used for DNS-based load balancing. ● Only the logical ports whose **Role** is **Service** or **Management+Service** can be added into a DNS zone. The logical ports whose **Role** is **Management** cannot be added in to a DNS zone. ● One logical port can be associated with only one DNS zone. One DNS zone can be associated with multiple logical ports. ● A DNS zone can be associated with both IPv4 and IPv6 logical ports. ● The load balancing effect varies with the distribution of logical ports associated with a DNS zone. To obtain a better load balancing effect, ensure that logical ports associated with a DNS zone are evenly distributed among controllers.	[Example] None

Step 5 Click **OK**.

The **Success** dialog box is displayed indicating that the logical port has been successfully created.

Step 6 Click **OK**.

----End

3.9.3.4.3 (Optional) Creating a Bond Port

This section describes how to bond Ethernet ports on a same controller.

Prerequisites

Ethernet ports that have IP addresses cannot be bound. The IP addresses of the bonded host ports need to be cleared before bonding.

Context

- Port bonding provides more bandwidth and redundancy for links. Although ports are bonded, each host still transmits data through a single port and the total bandwidth can

be increased only when there are multiple hosts. Determine whether to bond ports based on site requirements.

- The port bond mode of a storage system has the following restrictions:
  - On the same controller, a bond port is formed by a maximum of eight Ethernet ports.
  - Only the interface modules with the same port rate (GE or 10GE) can be bonded.
  - The port cannot be bonded across controllers. Non-Ethernet network ports cannot be bonded.
  - SmartIO interface modules cannot be bonded if they work in cluster or FC mode or run FCoE service in FCoE/iSCSI mode.
  - Read-only users are unable to bind Ethernet ports.
  - Each port only allows to be added to one bonded port. It cannot be added to multiple bonded ports.
  - Ports are bonded to create a bond port that cannot be added to the port group.
- After Ethernet ports are bonded, **MTU** changes to the default value and you must set the link aggregation mode for the ports. For example, on Huawei switches, you must set the ports to the static LACP mode.

  NOTE

  The detailed link aggregation mode varies with the switches' manufacturer.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Provisioning** > **Port** > **Bond Ports**.

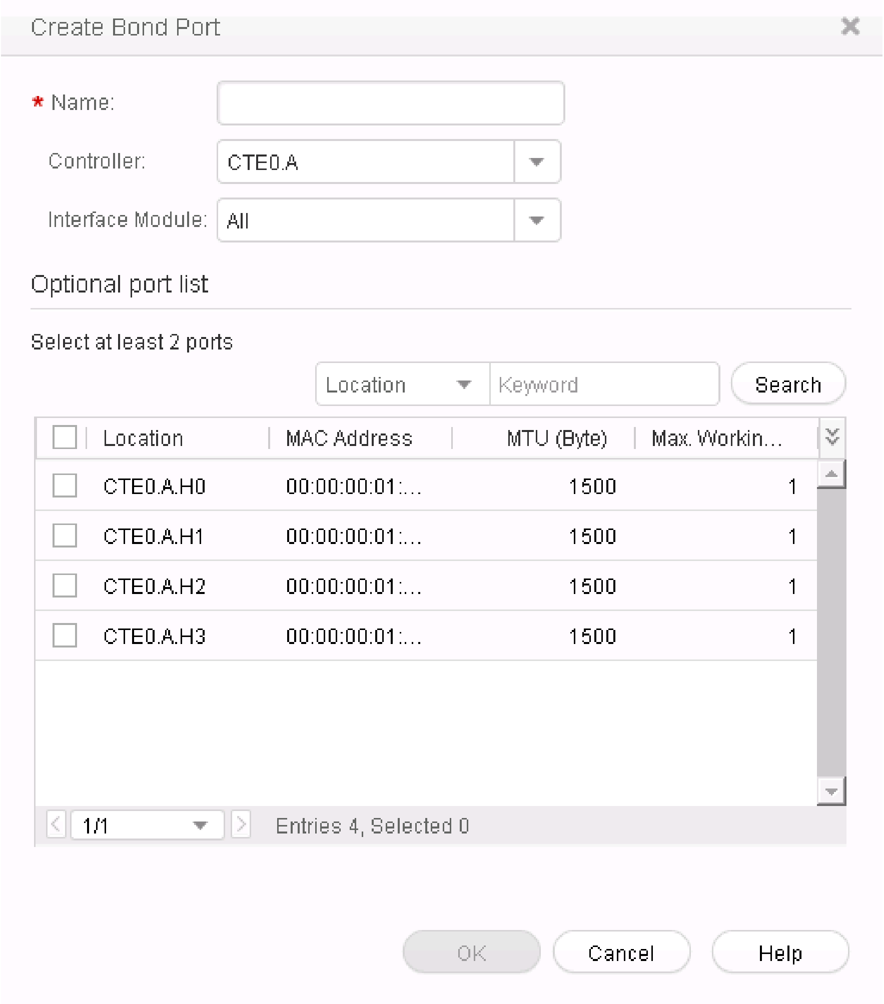
Step 3 Click **Create**.

The **Create Bond Port** dialog box is displayed.

NOTE

The port name format is **controller enclosure ID.interface module ID.port ID**.

Step 4 Set the name, interface module, and optional ports that can be bonded with the current Ethernet port.



Create Bond Port

* Name:

Controller: CTE0.A

Interface Module: All

Optional port list

Select at least 2 ports

Location ▾ | Keyword | Search

□	Location	MAC Address	MTU (Byte)	Max. Workin...
□	CTE0.A.H0	00:00:00:01:...	1500	1
□	CTE0.A.H1	00:00:00:01:...	1500	1
□	CTE0.A.H2	00:00:00:01:...	1500	1
□	CTE0.A.H3	00:00:00:01:...	1500	1

1/1 Entries 4, Selected 0

1. In **Name**, enter a name for the bond port.

   The name:

   - Contains only letters, digits, underscores (_), periods (.), and hyphens (-).
   - Contains 1 to 31 characters.

2. From the **Controller**, select the controller the Ethernet ports own to.
3. Select the **Interface Module**.
4. From the **Optional port list**, select the Ethernet ports you want to bond.

   NOTE

   Select at least two ports.

5. Click **OK**.

   The security alert dialog box is displayed.

Step 5 Confirm that you want to bond these Ethernet ports.

1. Confirm the information of the dialog box and select **I have read and understand the consequences associated with performing this operation.**.
2. Click **OK**.

   The **Success** dialog box is displayed indicating that the operation succeeded.

3. Click **OK**.

----End

3.9.3.4.4 (Optional) Managing a Route of Logical Port

When configuring share access, ensure that the logical IP addresses, domain controller, domain name server, and clients can ping each other. If they cannot ping each other, add the logical IP addresses to the network segment route among the domain controller, the domain name server, and clients.

Prerequisites

The logical port has been assigned an IP address.

Procedure

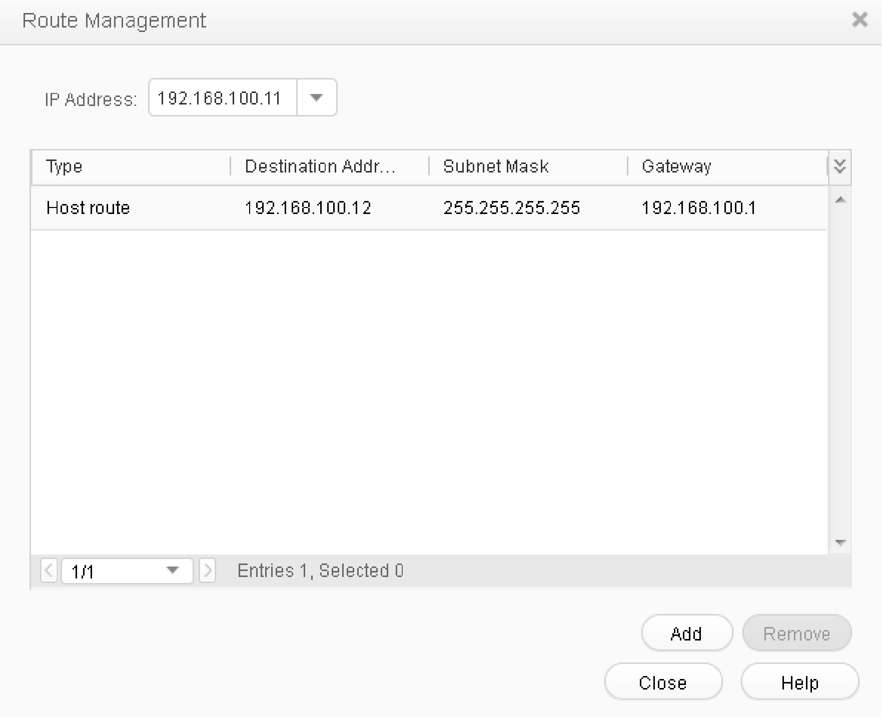
Step 1 Log in to DeviceManager.

Step 2 Go to the route management page.

You can go to the route management page by using either of the following methods:

- Choose **Provisioning** > **Port** > **Logical Ports**. Select a logical port for which you want to add a route and click **Route Management**. The **Route Management** dialog box is displayed.
- Choose **System** and click to switch to the rear view of the controller enclosure. Select the Ethernet port that you want to configure and click **Logical Port Management**. In the **Logical Port Management** dialog box that is displayed, select a logical port for which you want to add a route and click **Route Management**. The **Route Management** dialog box is displayed.

Step 3 Configure the route information for the logical port.



Route Management

IP Address: 192.168.100.11

Type	Destination Addr...	Subnet Mask	Gateway
Host route	192.168.100.12	255.255.255.255	192.168.100.1

1/1 Entries 1, Selected 0

1. In **IP Address**, select the IP address of the logical port.

2. Click **Add**.

   The **Add Route** dialog box is displayed.

   NOTICE

   The default IP addresses of the internal heartbeat on the dual-controller storage system are **127.127.127.10** and **127.127.127.11**, and the default IP addresses of the internal heartbeat on the four-controller storage system are **127.127.127.10**, **127.127.127.11**, **127.127.127.12**, and **127.127.127.13**. Therefore, the IP address of the router cannot fall within the 127.127.127.XXX segment. Besides, the IP address of the gateway cannot be **127.127.127.10**, **127.127.127.11**, **127.127.127.12**, or **127.127.127.13**. Otherwise, routing will fail. (Internal heartbeat links are established between controllers for these controllers to detect each other's working status. You do not need to separately connect cables. In addition, internal heartbeat IP addresses have been assigned before delivery, and you cannot change these IP addresses).

3. In **Type**, select the type of the route to be added.

   Possible values of **Type** are **Default route**, **Host route**, and **Network segment route**.

4. Set **Destination Address**.
   - If **IP Address** is an IPv4 address, set **Destination Address** to the IPv4 address or network segment of the application server's service network port or that of the other storage system's logical port.
   - If **IP Address** is an IPv6 address, set **Destination Address** to the IPv6 address or network segment of the application server's service network port or that of the other storage system's logical port.

5. Set **Destination Mask** (IPv4) or **Prefix** (IPv6).
   - If a **Destination Mask** is set for an IPv4 address, this parameter specifies the subnet mask of the IP address for the service network port on the application server or storage device.
   - If a **Prefix** is set for an IPv6 address, this parameter specifies the prefix of the IPv6 address for application server's service network port or that of the other storage system's logical port.

6. In **Gateway**, enter the gateway of the local storage system's logical port IP address.

Step 4 Click **OK**. The route information is added to the route list.

The security alert dialog box is displayed.

Step 5 Confirm the information of the dialog box and select **I have read and understand the consequences associated with performing this operation.**.

Step 6 Click **OK**.

The **Success** dialog box is displayed indicating that the operation succeeded.

NOTE

To remove a route, select it and click **Remove**.

Step 7 Click **Close**.

----End

3.9.3.5 Setting the CIFS Service (Applicable to V300R006C00)

Before creating a share, enable and configure the CIFS service.

Prerequisites

The license for CIFS protocol has been imported and activated.

Procedure

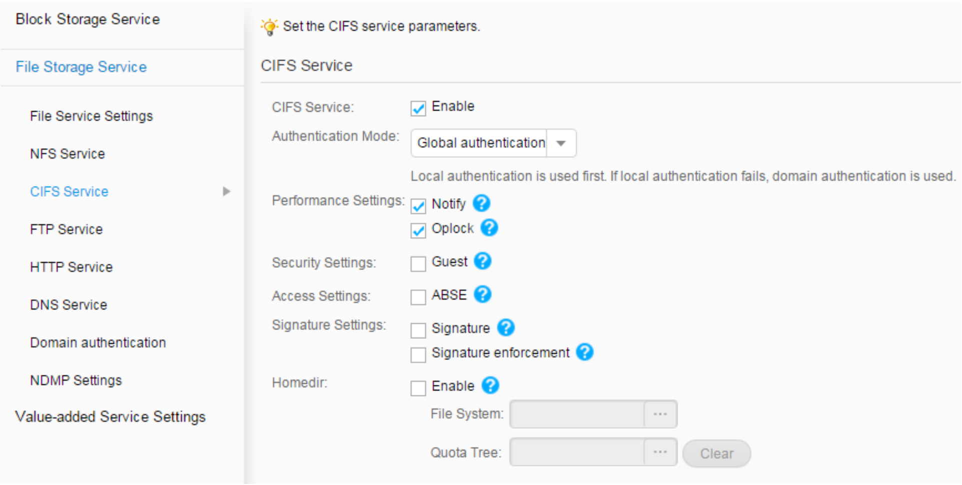
Step 1 Log in to DeviceManager.

Step 2 Choose **Settings** > **Storage Settings** > **File Storage Service** > **CIFS Service**.

Step 3 In **CIFS Service**, check whether **Enable** is selected. If not, select **Enable**.

Step 4 Configure CIFS service parameters.

1. Configure parameters described in **Table 3-55** based on site conditions.



Set the CIFS service parameters.

CIFS Service

CIFS Service: ☑ Enable

Authentication Mode: Global authentication

Local authentication is used first. If local authentication fails, domain authentication is used.

Performance Settings: ☑ Notify ☑ Oplock

Security Settings: □ Guest

Access Settings: □ ABSE

Signature Settings: □ Signature □ Signature enforcement

Homedir: □ Enable

File System:

Quota Tree:

Table 3-55 CIFS service parameters

Parameter	Description	Setting
Authentication Mode	Authentication mode for accessing a CIFS share. – **Local authentication**: Applies to scenarios where a local authentication user accesses a CIFS share in a non-domain environment. – **Domain authentication**: Applies to scenarios where a domain user accesses a CIFS share in an AD domain. – **Global authentication**: Local authentication is used first. If local authentication fails, domain authentication is used.	[Default value] Global authentication

Parameter	Description	Setting
Performance Settings	You can configure performance parameters to improve the CIFS share access efficiency. – Oplock: Opportunistic locking (Oplock) is a mechanism used to adjust cache policies of clients, improving performance and network utilization. This function is not recommended in the following scenarios: ■ Scenarios that have high requirements for data integrity: Local cache loss will occur if your network is interrupted or your client breaks down after Oplock is enabled. If the upper-layer service software does not have a mechanism to ensure data integrity, recovery, or retry, data loss may occur. ■ Scenarios where multiple clients access the same file: If Oplock is enabled, the system performance will be adversely affected. – Notify: After this parameter is enabled, a client's operations on a directory, such as adding a sub-directory, adding a new file, modifying the directory, and modifying a file, can be sensed by other clients that are accessing this	[Default value] Enabled

Parameter	Description	Setting
	directory or the parent directory of this directory.	
Security Settings	After the guest service is enabled, users can access shared directories without user names or passwords. Besides, users have the same permission as the **Everyone** local authentication group. **NOTE** After this function is enabled, unauthorized users can access shared directories as a guest user, which may cause information security issues. You are advised to disable this function.	[Default value] Disabled
Access Settings	After ABSE (Access based share enumeration) has been enabled, when user view the CIFS share information, only the CIFS shares that the user has permission to access displays. **NOTE** – It takes 10 to 20 minutes to load the CIFS share permission information after the storage system is powered on. During this period, the function does not take effect. – You are advised to enable this function. If this function is disabled, users can find all shares (including the shares for which the users do not have access permission), which may cause security threats to other shares.	[Default value] Disabled

Parameter	Description	Setting
Signature Settings	You can set signatures to enhance CIFS share access security. – Signature: This item is available for a client that employs Server Message Block (SMB) 1.0. After this item is selected, the client supports the signature function. For a client that employs an SMB later than SMB 1.0, the client supports the signature function by default. Whether the signature function is enabled also depends on the client registry settings. By default, the registry settings do not support the signature function. – Signature enforcement: After this option is selected, servers must adopt the signature function no matter the signature function is enabled by clients or not. **NOTE** If the signature function is disabled, the storage system may encounter man-in-the-middle (MITM) attacks, resulting in security risks.	[Default value] Disabled

Parameter	Description	Setting
Homedir	The Homedir share provides specific users with directories exclusively shared to them. An exclusive directory can only be accessed by its owner. - File system: file system that is shared in CIFS Homedir mode (mandatory) - Quota Tree: level-1 directory of a file system (optional) **NOTE** After Homedir is enabled, a user can directly access the directory (the directory is the same as the user name) under the specified the file system directory.	[Default value] Disabled

2. After the parameters are configured, click **Save**.

   The **Success** dialog box is displayed indicating that the operation succeeded.

3. Click **OK** to finish configuring CIFS service parameters.

----End

3.9.3.6 Setting the CIFS Service (Applicable to V300R006C10 and Later Versions)

Before creating a share, enable and configure the CIFS service.

Prerequisites

The license for CIFS protocol has been imported and activated.

Procedure

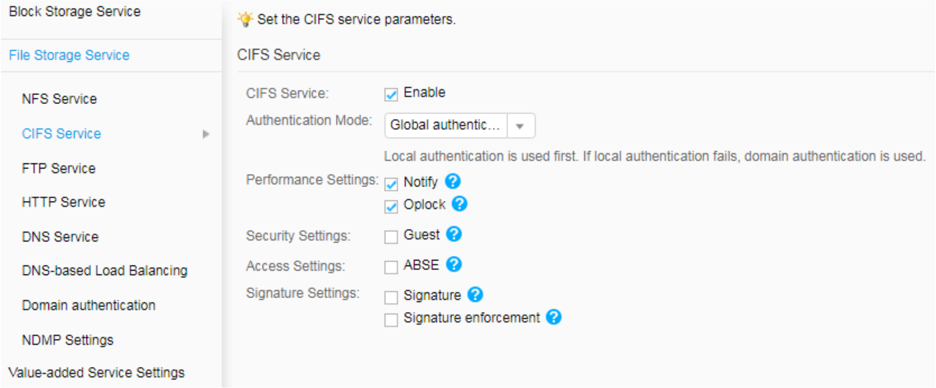
Step 1 Log in to DeviceManager.

Step 2 Choose **Settings** > **Storage Settings** > **File Storage Service** > **CIFS Service**.

Step 3 In **CIFS Service**, check whether **Enable** is selected. If not, select **Enable**.

Step 4 Configure CIFS service parameters.

1. Configure parameters described in **Table 3-56** based on site conditions.



Set the CIFS service parameters.

CIFS Service

CIFS Service: ☑ Enable

Authentication Mode: Global authentic...

Local authentication is used first. If local authentication fails, domain authentication is used.

Performance Settings: ☑ Notify ☑ Oplock

Security Settings: □ Guest

Access Settings: □ ABSE

Signature Settings: □ Signature □ Signature enforcement

Table 3-56 CIFS service parameters

Parameter	Description	Setting
Authentication Mode	Authentication mode for accessing a CIFS share. – **Local authentication**: Applies to scenarios where a local authentication user accesses a CIFS share in a non-domain environment. – **Domain authentication**: Applies to scenarios where a domain user accesses a CIFS share in an AD domain. – **Global authentication**: Local authentication is used first. If local authentication fails, domain authentication is used.	[Default value] Global authentication

Parameter	Description	Setting
Performance Settings	You can configure performance parameters to improve the CIFS share access efficiency. – Oplock: Opportunistic locking (Oplock) is a mechanism used to adjust cache policies of clients, improving performance and network utilization. This function is not recommended in the following scenarios: ■ Scenarios that have high requirements for data integrity: Local cache loss will occur if your network is interrupted or your client breaks down after Oplock is enabled. If the upper-layer service software does not have a mechanism to ensure data integrity, recovery, or retry, data loss may occur. ■ Scenarios where multiple clients access the same file: If Oplock is enabled, the system performance will be adversely affected. – Notify: After this parameter is enabled, a client's operations on a directory, such as adding a sub-directory, adding a new file, modifying the directory, and modifying a file, can be sensed by other clients that are accessing this directory or the parent directory of this directory.	[Default value] Enabled

Parameter	Description	Setting
Security Settings	After the guest service is enabled, users can access shared directories without user names or passwords. Besides, users have the same permission as the **Everyone** local authentication group. **NOTE** After this function is enabled, unauthorized users can access shared directories as a guest user, which may cause information security issues. You are advised to disable this function.	[Default value] Disabled
Access Settings	After ABSE (Access based share enumeration) has been enabled, when user view the CIFS share information, only the CIFS shares that the user has permission to access displays. **NOTE** – It takes 10 to 20 minutes to load the CIFS share permission information after the storage system is powered on. During this period, the function does not take effect. – You are advised to enable this function. If this function is disabled, users can find all shares (including the shares for which the users do not have access permission), which may cause security threats to other shares.	[Default value] Disabled

Parameter	Description	Setting
Signature Settings	You can set signatures to enhance CIFS share access security. – Signature: This item is available for a client that employs Server Message Block (SMB) 1.0. After this item is selected, the client supports the signature function. For a client that employs an SMB later than SMB 1.0, the client supports the signature function by default. Whether the signature function is enabled also depends on the client registry settings. By default, the registry settings do not support the signature function. – Signature enforcement: After this option is selected, servers must adopt the signature function no matter the signature function is enabled by clients or not. **NOTE** If the signature function is disabled, the storage system may encounter man-in-the-middle (MITM) attacks, resulting in security risks.	[Default value] Disabled

2. After the parameters are configured, click **Save**.

   The **Success** dialog box is displayed indicating that the operation succeeded.

3. Click **OK** to finish configuring CIFS service parameters.

----End

3.9.3.7 Configuring a Storage System to Add It to an AD Domain

After the storage system is added to an AD domain, domain users can access CIFS shares that are allocated to the domain. This section describes how to add a storage system to an AD domain.

3.9.3.7.1 Preparing AD Domain Configuration Data

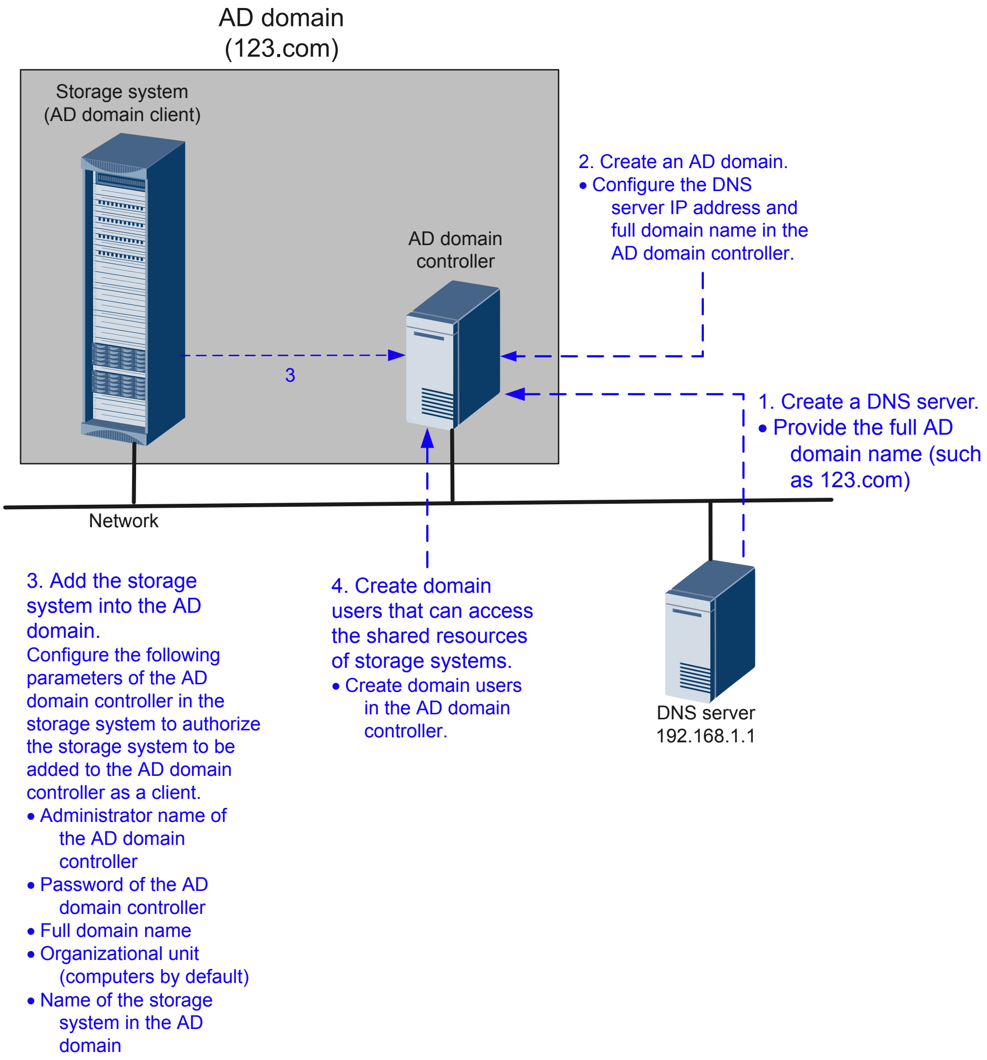
Why AD Domains?

In the Windows shared mode, every Windows host is an independent node. The account and permission information about users allowed to access the shares are stored on each node. As a result, the information maintenance is complex and uncontrollable. For example, to grant a user the access permission, you need to add the configuration information about this user to every node.

If an AD domain is used, however, the domain controller manages all the user configuration information and authenticates the access to the domain. The domain controller incorporates a database that stores information about the domain account, password, and nodes in the domain. A user can access all the shared content in the domain after passing the authentication by the domain controller.

Working Principles and Panorama

1. Create a DNS server and provide a full AD domain name (such as 123.com) using the server. Other servers only need to input the full domain name and pass the authentication to access the shares.
2. Set up an AD domain on the domain controller side.
3. Add the storage systems that need to provide sharing services to the AD domain.
4. Create a domain user on the domain controller side. Log in to the servers in the AD domain using the domain user account. The shares in the domain can be accessed.


AD domain
(123.com)
Storage system
(AD domain client)
AD domain
controller
2. Create an AD domain.
• Configure the DNS server IP address and full domain name in the AD domain controller.
3
1. Create a DNS server.
• Provide the full AD domain name (such as 123.com)
Network
3. Add the storage system into the AD domain.
Configure the following parameters of the AD domain controller in the storage system to authorize the storage system to be added to the AD domain controller as a client.
• Administrator name of the AD domain controller
• Password of the AD domain controller
• Full domain name
• Organizational unit (computers by default)
• Name of the storage system in the AD domain
4. Create domain users that can access the shared resources of storage systems.
• Create domain users in the AD domain controller.
DNS server
192.168.1.1

Data Preparation

The data to be prepared is as follows: **Domain Administrator Username**, **Password**, **Full Domain Name**, **Organization Unit** (optional), and **System Name**. For details about how to obtain the data, see the parameter description in section "Configuring AD Domain Authentication Parameters".

3.9.3.7.2 Configuring a Storage System to Add It to a DNS Server

After a storage system is connected to a DNS server, you can access the storage system through the IP address or domain name. This operation enables you to configure a system management IP address for the active or standby DNS.

Prerequisites

- The DNS has been configured and is running properly.
- Port 53 of the TCP/UDP protocol between the storage system and the DNS server is enabled.

Context

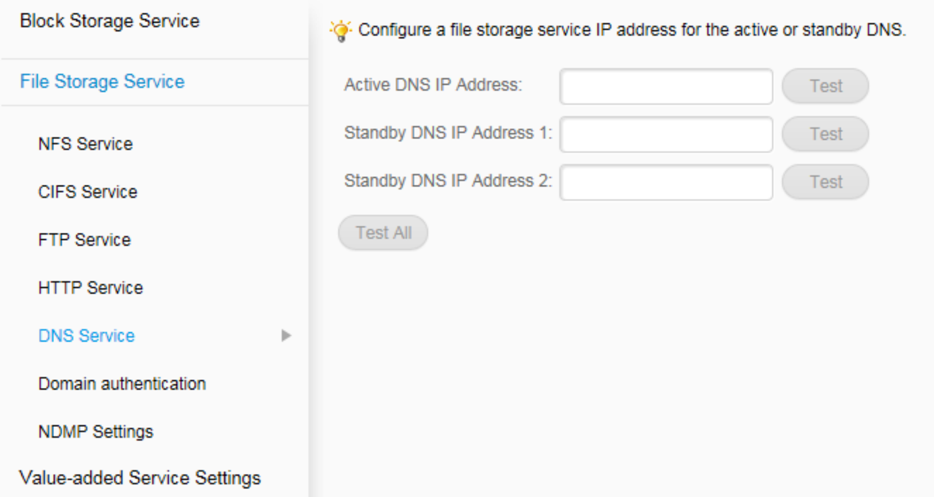
- A DNS server is used to resolve host names in a domain.
- If you want to configure a standby DNS server, keep the domain names of the active and standby servers consistent.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Settings** > **Storage Settings** > **File Storage Service** > **DNS Service**.

Step 3 Set the DNS information.



Configure a file storage service IP address for the active or standby DNS.

1. Set **Active DNS IP Address**.

   NOTE

   You can click **Test** of DNS IP address to test its availability.

2. **Optional:** Set **Standby DNS IP Address 1**.

   NOTE

   You can click **Test** of DNS IP address to test its availability.

3. **Optional:** Set **Standby DNS IP Address 2**.

   NOTE

   – Configure the standby DNS IP address 1 first and then the standby DNS IP address 2.

   – You can click **Test** of DNS IP address to test its availability.

NOTE

You can click **Test All** to test the connection between the DNS server and storage system.

Step 4 Click **Save**.

The **Success** dialog box is displayed, indicating that the operation succeeded.

Step 5 Click **OK**.

----End

3.9.3.7.3 Configuring AD Domain Authentication Parameters

In an AD domain, add a storage system to the AD domain. Then the AD server can authenticate CIFS clients when they try to access shared resources. The administrator can manage the share access permission and quotas of domain users. If the storage system is not added to the AD domain, domain users cannot use share services provided by the share server.

Prerequisites

- An AD domain has been set up.
- The storage system has been connected to the DNS server.
- AD domain server and DNS server have time synchronization with the storage system. The time difference must be no larger than 5 minutes.
- Ports 88, 389, 445, and 464 of the TCP/UDP protocol between the storage system and the AD domain environment are enabled.

NOTE

- The 2000, 5000, and 6000 series storage systems can be connected to the AD domain server and DNS server through the management network port or the service network port (logical port). If the storage system communicates with the AD domain server and DNS server through the management network port, the management network port of each controller must be connected properly to the AD domain server and DNS server. If the storage system communicates with the AD domain server and DNS server through the service network port, the service network port of each controller under each vStore must be connected properly to the AD domain server and DNS server, ensuring that the CIFS services related to the AD domain can be normally used. You are advised to use the service network port to connect to the AD domain server.
- For 6000 series storage systems, every two controllers share one management network port. When the management network port is used to connect to the AD domain server and DNS server, only one controller can be connected to the AD domain server and DNS server. Therefore, in 6000 series storage systems, you are not advised to use the management network port to connect to the AD domain server and DNS server.
- The 18000 series storage systems can be connected to the AD domain and DNS server through the service network port (logical port) only. And it requires all the controllers can communicate with the AD server.
- AD domain servers support the primary/secondary domain, parent/child domain, active/standby domain, or trust domain.

Precautions

- Before adding a storage system to an AD domain, ensure that the primary controller of the storage system has connected to a DNS server and an AD domain server. If it has not, enable the AD domain forwarding function and connect a service port of the storage system to a DNS server and an AD domain server.

  NOTE

  - Run **show controller general** to query information about all controllers.**Role** indicates the cluster role of a controller. When **Role** is **Master**, this controller is the primary controller of the storage system.
  - You can run the **change domain ad_config controller_forwarding_enable=yes** command to enable the AD domain forwarding function. For details, see the **Command Reference** of the corresponding product model.
- If **OverWrite System Name** is enabled and the entered system name is the same as that on the AD domain server, information of the existing system will be overwritten by that of the new system.

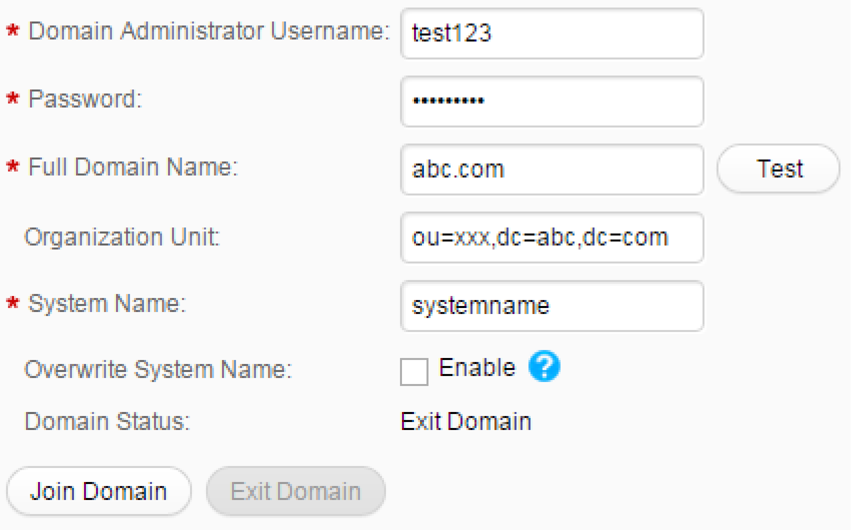
- Simple password may cause security risk. Complicated password is recommended, for example, password contains uppercases, lowercases, digits and special characters.
- You are advised to use physical isolation and end-to-end encryption to ensure security of data transfer between clients and AD domain servers.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Settings** > **Storage Settings** > **File Storage Service** > **Domain Authentication**.

Step 3 In the **AD Domain Settings** area, configure the AD domain authentication. The related parameters are as shown in **Table 3-57**.



* Domain Administrator Username:	test123
* Password:	•••••••••
* Full Domain Name:	abc.com
Organization Unit:	ou=xxx,dc=abc,dc=com
* System Name:	systemname
Overwrite System Name:	□ Enable
Domain Status:	Exit Domain

Table 3-57 Parameters of the AD domain

Parameter	Description	Value
Domain Administrator Username	User name of an administrator who logs in to the AD domain server.	[Rule] Contains 1 to 63 letters. [Example] test123 [How to Obtain] Contact the administrator of the AD domain controller.

Parameter	Description	Value
Password	Password of an administrator who logs in to the AD domain server.	[Rule] Contains 1 to 127 letters. [Example] !QAZ2wsx [How to Obtain] Contact the administrator of the AD domain controller.
Full Domain Name	Full domain name of the AD domain server	[Rule] Contains 1 to 127 characters. [Example] abc.com [How to Obtain] Contact the administrator of the AD domain controller.
Organization Unit	Organization unit of a type of directory objects in a domain. These objects include users, computers, and printers. After an object is added to a domain, it will be a member in the organization unit. If you do not enter anything, the storage system is added to organization unit as Computers by default.	If the **Type** of organization units of a domain controller is **Container**, enter **cn=xxx,dc=abc,dc=com**. Otherwise, enter **ou=xxx,dc=abc,dc=com**. [Example] ou=xxx,dc=abc,dc=com [How to Obtain] 1. On the Windows AD domain server, open **Active Directory Users and Computers** or **ADSI Edit**. 2. Select the folder directory on the left and right-click the directory. Choose **Properties**. 3. In the Properties dialog box that is displayed, click **Attribute Editor**. The value of **distinguishedName** is the organization unit.
System Name	Name of the storage system in the AD domain. After being added to the domain, the client can use the name to access storage systems.	[Rule] It can contain only letters, digits, and hyphens (-), and must not contain digits only, and contains 1 to 15 letters. [Example] systemname

Parameter	Description	Value
Overwrite System Name	If a same system name already exists on the domain control server, the existing system name is overwritten after this option is selected.	[Example] Enable
Domain Status	Whether storage system has been added to the domain.	[Example] Exited domain

Step 4 Click **Join Domain**. The AD domain authentication configuration is completed.

----End

Follow-up Procedure

If you want to exit domain, perform the following operations:

1. In **AD Domain Settings**, input **Domain Administrator Username** and **Password**.
2. Click **Exit domain**.

   The **Success** dialog box is displayed indicating that the operation succeeded.
3. Click **OK** to finish exiting the storage system to AD domain.

3.9.3.8 Configuring a Local Authentication User (Group)

In a non-domain environment, you must configure a local authentication user (group). After the Homedir share service is enabled, you can access Homedir shares as a local user.

3.9.3.8.1 (Optional) Creating a Local Authentication User Group

This section describes how to create a local authentication user group. Local authentication user groups help you control the share access permissions of local authentication users.

Context

A storage system has four local authentication user groups that are automatically created. The four local authentication user groups are reserved for the system and cannot be deleted.

- **default_group**: default user group. When the group members access the shared file system in the storage systems, they must be authenticated to obtain their permissions.
- **Administrators**: administrator group. When the group members access the shared file system in the storage system, they do not need to be authenticated by share level ACL and directory&file level NT ACL. They can operate any file in any share with administrator permissions.
- **AntivirusGroup**: antivirus user group. The group members can use third-party antivirus software to scan for shared file systems. They have administrator permissions.

- **Backup Operators**: backup user group. The group members can use third-party backup software to back up and recover shared file systems. They do not have administrator permissions.

NOTE

Access Control List (ACL): a collection of permissions that are authorized to users or user groups to operate shared files. ACL permissions are classified into ACL permission storage and ACL permission authentication. After a user logs in to a share, the user determines the share permissions, reads the ACL permissions, and determines whether files can be read and written. For storage, each ACL permission is called Access Control Entry (ACE). After CIFS shares are mounted to a Windows client, the client sends NT ACLs to a server (storage system that provides CIFS shares).

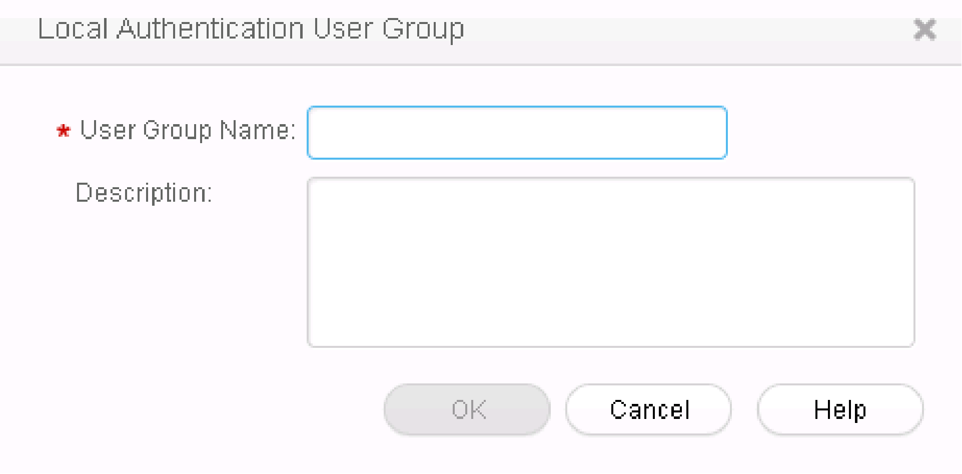
Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Provisioning** > **User Authentication** > **Local Authentication User Group**.

Step 3 Click **Create**.

The **Local Authentication User Group** dialog box is displayed.



Step 4 In **User Group Name**, enter a new user group name.

NOTE

- For V300R006C00:
  - Must contain 1 to 32 characters.
  - Cannot contain space, double quotation mark ("), slash (/), backslash (\), square brackets ([]), larger than (<), less than (>), plus (+), colon (:), semicolon (;), comma (,), question mark (?), asterisk (*), vertical bar (|), equal mark (=), (@), or end with a period (.).
  - The user group name can contain case-insensitive letters. Therefore, **aa** and **AA** cannot be created at the same time.
  - The user group name cannot be the same as the name of the local authentication user.
- For V300R006C10:
  - The user group name cannot contain the quotation mark ("), slash (/), backslash (\), square brackets ([]), less than sign (<), larger than sign (>), plus sign (+), colon (:), semicolon (;), comma (,), question mark (?), asterisk (*), vertical bar (|), equal sign (=), at sign (@) or end with a period (.). If the user group name start and end with spaces, the spaces are not displayed after the user group name is created.
  - The user group name can contain case-insensitive letters. Therefore, **aa** and **AA** cannot be created at the same time.
  - The user group name cannot be the same as the name of the local authentication user.
  - The user group name contains 1 to 63 characters.

Step 5 **Optional:** In **Description**, add the description of the user group.

Step 6 Click **OK**.

Step 7 In the **Success** dialog box that is displayed, click **OK**.

----End

3.9.3.8.2 Creating a Local Authentication User

This section describes how to create a local user. For applications that use local authentication, local user accounts are used to access a share. You can add a local user to a user group and access a share as the user group.

Procedure

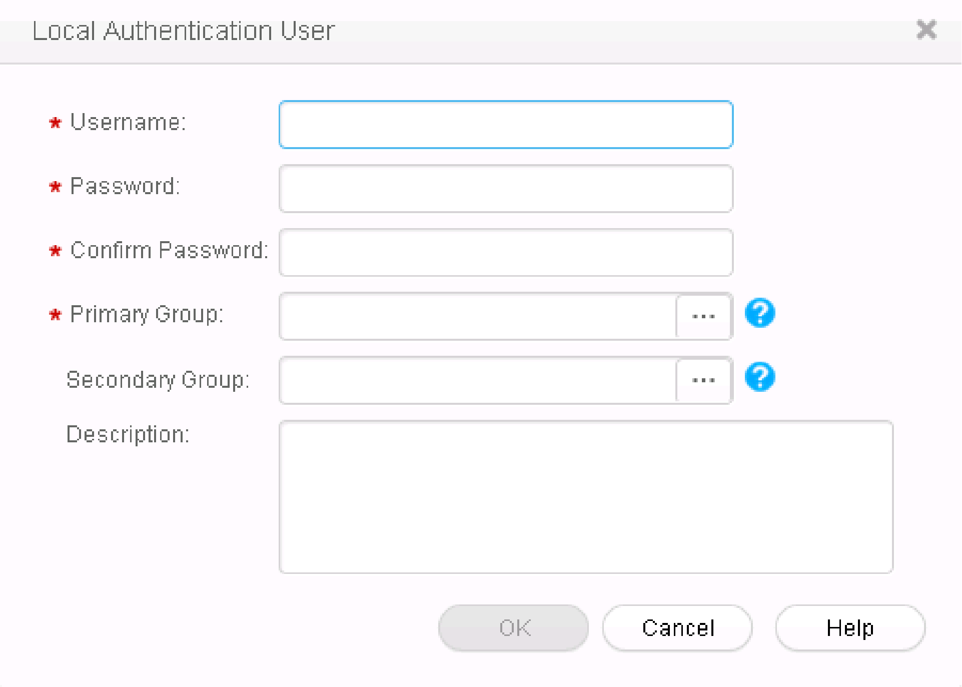
Step 1 Log in to DeviceManager.

Step 2 Choose **Provisioning** > **User Authentication**.

Step 3 Click **Local Authentication User** tab.

Step 4 Click **Create**.

The **Local Authentication User** dialog box is displayed.



Step 5 In **Username**, enter a new user name.

The user name:

- Cannot contain space, double quotation mark ("), slash (/), backslash (\), square brackets ([]), less than (<), larger than (>), plus (+), colon (:), semicolon (;), comma (,), question mark (?), asterisk (*), vertical bar (|), equal mark (=), (@), or end with a period (.).
- The user name can contain case-insensitive letters. Therefore, **aaaaaaaa** and **AAAAAAAA** cannot be created at the same time.
- The user name cannot be the same as the name of the local authentication user group.
- Contains 8 to 32 characters by default.

  NOTE

  You can modify the minimum length of user name in **More** > **Set Security Policies**.

Step 6 In **Password**, enter the password of the user.

The system default password requirements are:

- Contain 8 to 16 characters.
- Contain special characters. Special characters include: !"#$%&'()*+,-./:;<=>?@[\]^`{_|}~ and space.
- Contain any two types of the uppercase letters, lowercase letters, and digits.
- Cannot contain three consecutive same characters.
- Be different from the user name or the user name typed backwards.

NOTE

Click **More** and choose **Set Security Policies** to set a security policy for the password of the local authentication user in the file system. If **Password Validity Period (days)** is not selected, your password will never expire. For the security purpose, you are advised to select **Password Validity Period (days)** and set a validity period. The default validity period is 180 days. After the password expires, you cannot access shares, but you can set a password again and modify the password security policy.

Step 7 In **Confirm Password**, enter the new password again.

Step 8 Select **Primary Group**.

The **Select Primary Group** dialog box is displayed.

NOTE

The primary group to which users belong controls the users' permission for CIFS shares. A user must and can only belong to one primary group.

Step 9 Select the user group to which the user belongs to and click **OK**.

Step 10 (Optional) Select **Secondary Group**.

The **Select Secondary Group** dialog box is displayed.

NOTE

The concepts of primary group and secondary group are for local authentication users and have no relationship with each other. A local authentication user must belong to a primary group but not to a secondary group.

Step 11 Click **Add**.

The **Select User Group** dialog box is displayed.

Step 12 Select one or multiple groups which the user belongs to and click **OK**.

The system goes back to **Select Secondary Group** dialog box.

Step 13 Click **OK**.

The system goes back to **Local Authentication User** dialog box.

Step 14 **Optional:** In **Description** text box, enter the description for the local authentication user, for later management or search.

Step 15 Click **OK**.

Step 16 In the **Success** dialog box that is displayed, click **OK**.

----End

3.9.3.9 Enabling the Homedir Share Service (Applicable to V300R006C00)

After the Homedir share service is enabled, the storage system supports Homedir shares.

Prerequisites

A file system whose Homedir share service must be enabled has been created.

Procedure

Step 1 Log in to **DeviceManager**.

Step 2 Choose **Settings** > **Storage Settings** > **File Storage Service** > **CIFS Service**.

Step 3 In **CIFS Service**, check whether **Enable** is selected. If not, select **Enable**.

Step 4 In **Homedir**, select **Enable**.

Step 5 In **File System**, select the file system whose Homedir share service you want to enable.

NOTE

If you want to enable the Homedir share service for a quota tree in the file system, select the quota tree in **Quota Tree**.

Step 6 Click **Save**.

The **Success** dialog box is displayed.

Step 7 Click **OK**.

----End

3.9.3.10 Creating a CIFS Homedir share (Applicable to V300R006C10 and Later Versions)

You may share the file system through CIFS Homedir, and user can access the shared storage space.

Prerequisites

- The CIFS service is enabled.
- If it is a non-domain environment, the CIFS Homedir authentication mode is configured as local authentication or global authentication.
- If it is an AD domain environment, the CIFS Homedir authentication mode is configured as domain authentication or global authentication.

Procedure

Step 1 Log in to DeviceManager.

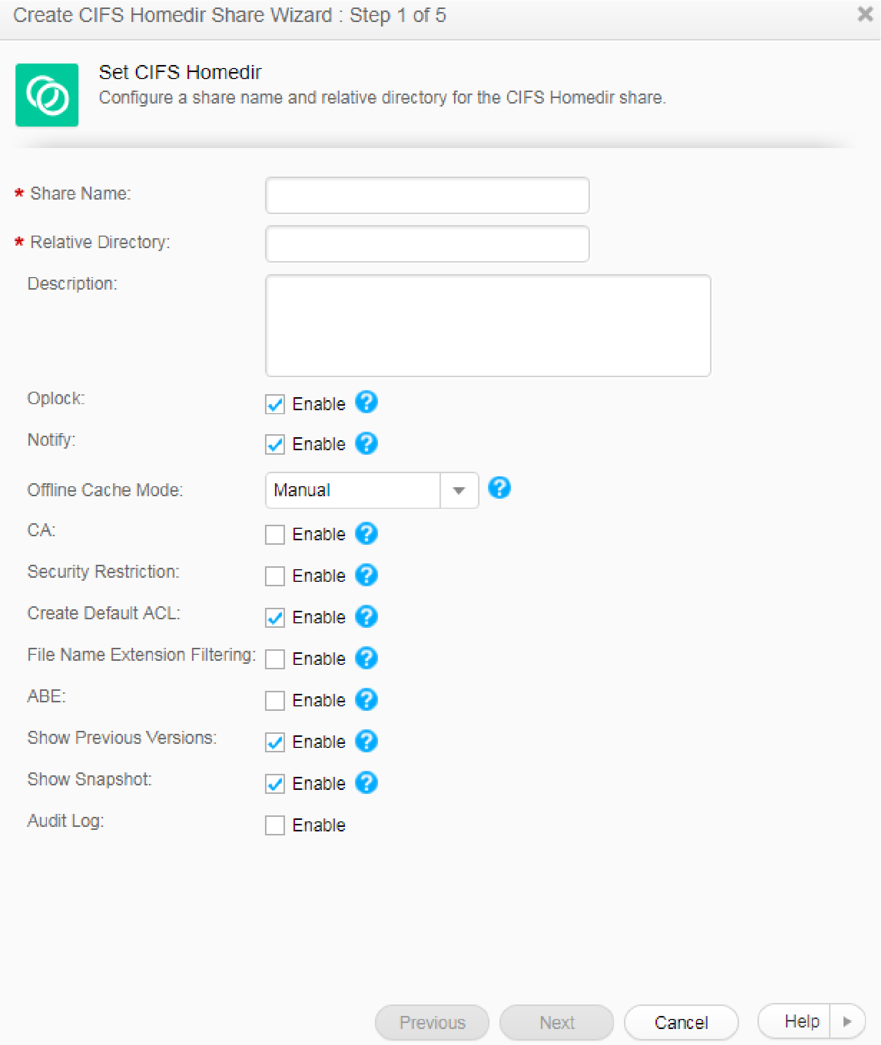
Step 2 Choose **Provisioning** > **Share** > **CIFS Homedir**.

Step 3 Click **Create**.

The **Create CIFS Homedir Share Wizard** dialog box is displayed.

Step 4 Set CIFS Homedir parameters.

1. On the CIFS Homedir setting page, configured required parameters.


Create CIFS Homedir Share Wizard : Step 1 of 5
Set CIFS Homedir
Configure a share name and relative directory for the CIFS Homedir share.

* Share Name:	
* Relative Directory:	
Description:	
Oplock:	☑ Enable
Notify:	☑ Enable
Offline Cache Mode:	Manual
CA:	□ Enable
Security Restriction:	□ Enable
Create Default ACL:	☑ Enable
File Name Extension Filtering:	□ Enable
ABE:	□ Enable
Show Previous Versions:	☑ Enable
Show Snapshot:	☑ Enable
Audit Log:	□ Enable

Previous
Next
Cancel
Help

Table 3-58 describes the related parameters.

Table 3-58 Parameters for creating a CIFS Homedir share

<table>
<tr><th>Parameter</th><th>Description</th><th>Value</th></tr>
<tr><td>Share Name</td><td>Name used by a user for accessing the shared resources.</td><td>[Value range]
– The share name can be letters of any language.
– Contain 1 to 80 characters.
– Cannot contain special characters "/\[]:|<>+;,?*=.
– Cannot be the name reserved by the system. The names reserved by the system are: **ipc$**, **autohome**, ~ and **print $**.
[Example]
share_for_user1</td></tr>
<tr><td>Relative Directory</td><td>Path of a user's relative directory</td><td>[Value range]
– Must contain 1 to 255 characters.
– Cannot contain special characters including \:*?"<>|
– Can contain **%d**, **%w**, and **%u**. **%d** indicates a domain name, **%w** indicates a user name, and **%u** indicates a Unix name after mapping. For example, if the relative path is **home_%d/%w**, the Homedir directory of user **usera** in domain **china** is **home_china/usera/**.
[Example]
home_%d/%w</td></tr>
<tr><td>Description</td><td>Description of the created CIFS Homedir share.</td><td>[Value range]
The name contains 0 to 255 characters.
[Example]
Share for user 1.</td></tr>
</table>

Parameter	Description	Value
Oplock	Opportunistic lock (Oplock) is a mechanism used to adjust cache policies of clients, improving performance and network utilization. This function is not recommended in the following scenarios: – Scenarios that have high requirements for data integrity: Local cache loss will occur if your network is interrupted or your client breaks down after Oplock is enabled. If the upper-layer service software does not have a mechanism to ensure data integrity, recovery, or retry, data loss may occur. – Scenarios where multiple clients access the same file: If Oplock is enabled, the system performance will be adversely affected.	[Default value] Enabled
Notify	After this parameter is enabled, a client's operations on a directory, such as adding a sub-directory, adding a new file, modifying the directory, and modifying a file, can be sensed by other clients that are accessing this directory or the parent directory of this directory.	[Default value] Enabled

Parameter	Description	Value
Offline Cache Mode	Cache files to be accessed in different offline cache modes to local clients so that files can be operated offline. The following offline cache modes are supported: - Manual Specified files and programs in the shared directory can be cached to local clients and operated offline. - Documents If a user accesses the shared directory and opens a file or program in the shared directory, the file or program is automatically cached to a local client so that the user can operate it offline. Files and programs that can be operated offline are saved in the cache of clients and they are synchronized with those in the shared directory until the cache is full or users delete them. Files and programs that have not been opened cannot be cached locally. - Programs Performance is optimized based on the Documents mode. If an executable file (EXE or DLL) in the shared directory is executed by a local client, the file is automatically cached to the client. If the client needs to run the executable file online or offline next time, it accesses the cached file instead of that in the shared directory. - None Files and programs in the shared directory cannot be cached to local clients. Therefore, these files and programs cannot be operated	[Default value] Manual

Parameter	Description	Value
	offline. This mode prevents the offline file function of clients from creating duplicates of files in the shared directory. **NOTE** The offline file function of clients must be enabled so that files and programs can be automatically cached.	
CA	This option is for SMB3.0 continuous availability, only applied to the share for Hyper-V. This feature depends on Oplock, ensure that Oplock is enabled.	[Default value] Disabled
Security Restriction	After security restriction is enabled, only the added IP addresses can be used to access devices. If security restriction is not enabled, all IP addresses can be used to access devices.	[Default value] Disabled
Create Default ACL	This function creates a default ACL (full control rights to everyone; applied to the current directory, its subdirectories, and files in them) for a shared CIFS Homedir root directory if the directory has no ACL. You can change the default ACL in follow-up operations. If you want to retain the UNIX MODE rights, disable this function.	[Default value] Enabled
File Name Extension Filtering	After file name extension filtering is enabled, the types of files that users access on a CIFS Homedir share are controlled. **NOTE** SMB2 and SMB3 support file name extension filtering while SMB1 does not support it.	[Default value] Disabled
ABE	After Access Based Enumeration (ABE) is enabled, files and folders that users have no access permission are not displayed. **NOTE** SMB2 and SMB3 support ABE while SMB1 does not support it.	[Default value] Disabled

Parameter	Description	Value
Show Previous Versions	If the function of showing historical versions is enabled, clients can show and roll back historical versions.	[Default value] Enabled
Show Snapshot	If the function of showing snapshots is enabled, clients can show and traverse snapshot directories.	[Default value] Enabled
Audit Log	After the audit function is enabled, the system can record audit logs of the shared directory. The audit log items include **Open**, **Create**, **Read**, **Write**, **Close**, **Delete**, **Rename**, **Obtain properties**, **Set properties**, **Obtain security properties**, **Set security properties**, **Obtain extension properties**, and **Set extension properties**. After the audit function is enabled, by default, the system records **Create**, **Write**, **Delete**, and **Rename** operations of the shared directory.	[Default value] Disabled

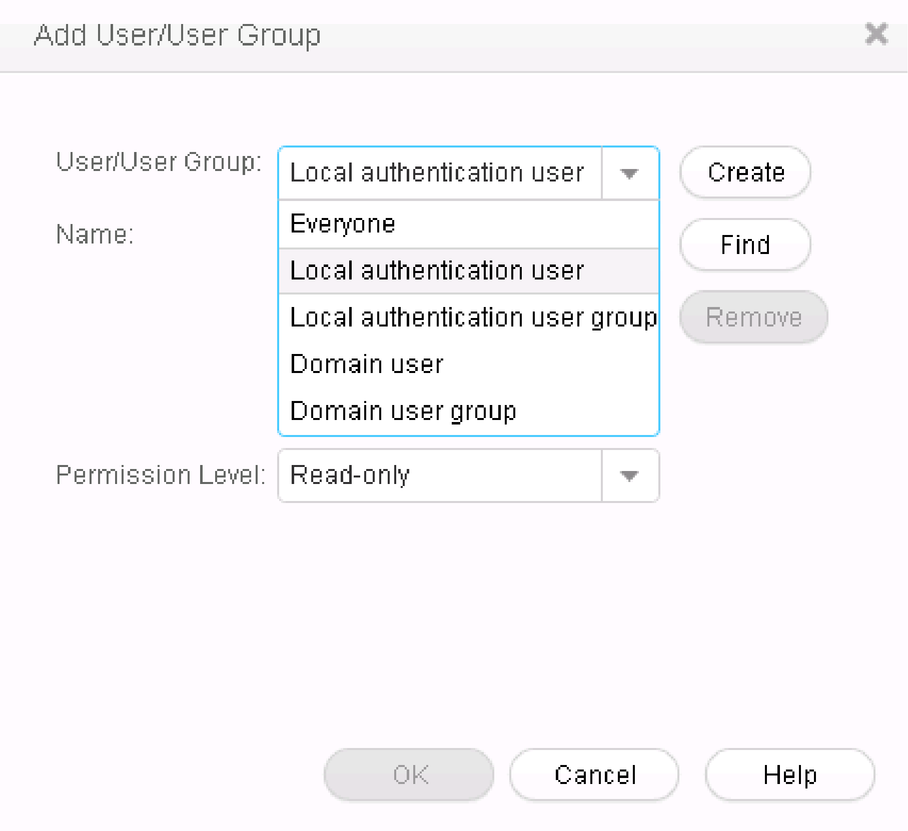
2. Click **Next**.

   The **Set Permissions** page is displayed.

Step 5 Set access permissions of the CIFS Homedir share for users or user groups.

1. In **Users/User Groups** area, click **Add**.

   The **Add User/User Group** dialog box is displayed.



2. In **User/User Group**, select user type or user group type.

   The values include: **Everyone**, **Local authentication user**, **Local authentication user group**, **Domain user** and **Domain user group**.

   – If you select **Everyone**, click **Add**.

     NOTE

     Everyone means every user has the access permission.

   – If you select **Local authentication user** or **Local authentication user group**, click **Find**, in the pop-up **Add User** or **Add User Group** dialog boxes to select the user or user group you want to add. Click **OK**.

   – If the desired local authentication user or user group does not exist, click **Create** to create and add a new authentication user or user group.

   – If you select **Domain user** or **Domain user group**, enter the corresponding name in **Name**, and click **Add**.

     NOTE

     The name format is **Domain name\Domain user name** or **Domain name\Domain user group name**.

3. In **Permission Level**, select the CIFS Homedir access permission for the user or user group added.

   Table 3-59 provides details about the permissions.

Table 3-59 Description of CIFS Homedir share permissions

Operation	Forbidden	Read-Only	Read and Write	Full Control
Viewing files and subdirectories	Not allowed	Allowed	Allowed	Allowed
Viewing the contents of files	Not allowed	Allowed	Allowed	Allowed
Running executable files	Not allowed	Allowed	Allowed	Allowed
Adding files or subdirectories	Not allowed	N/A	Allowed	Allowed
Modifying the contents of files	Not allowed	N/A	Allowed	Allowed
Deleting files and subdirectories	Not allowed	N/A	Allowed	Allowed
Renaming	Not allowed	N/A	Allowed	Allowed
Changing the ACL of files or directories	Not allowed	N/A	N/A	Allowed

NOTE

- Priorities in the descending order are **Forbidden**, **Full control**, **Read and write** , and **Read-only**. The permission with the highest priority prevails. When a user's access permission is extended, the new permission takes effect immediately. For example, if a user's original access permission is **Read-only** but the user is added to a user group with **Full control** permission later, the user's access permission changes to **Full control** and it does not need to be re-authenticated to access the CIFS Homedir share.
- When the primary group of a local authentication user is the local authentication user group of **Administrators**, the group members can access the shared file system in the storage system without being authenticated by share level ACL and directory and file level NT ACL. They can operate any file in any share with administrator permissions.

4. Click **OK**.

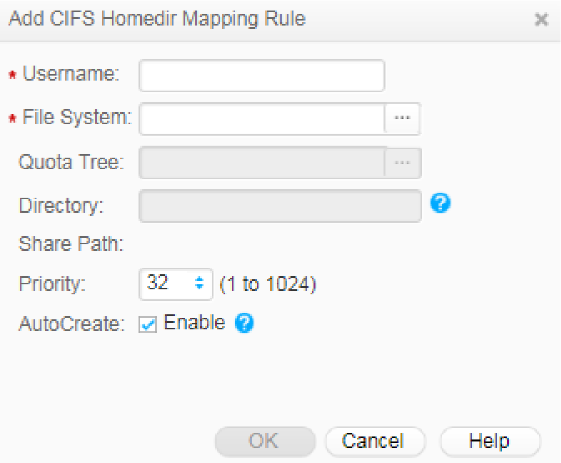
   The system adds the user or user group you select to the **Users/User Groups** list.

5. Click **Next**.

Step 6 Add a mapping rule of file system paths to the CIFS Homedir share. A mapping rule consists of user names, file systems, quota trees, priorities, and AutoCreate. Only users matching the mapping rule can access the Homedir directory.

1. In **Mapping Rule List**, click **Add**.

   The **Add CIFS Homedir Mapping Rule** dialog box is displayed.



2. In **Name**, enter user names.

NOTE

- The value contains 1 to 255 characters.
- The value can be names of common or domain users. Use a slash (\) to connect the domain name and user name. Only one slash (\) is allowed.
- Wildcard character * is allowed. The user name can contain only one wildcard character and the wildcard character must be at the end of the user name. For example, **china*** indicates all users in the **china** domain.
- The user name cannot contain spaces or special characters including **"/[]<>+:;,?=|**, and cannot end with a period (**.**).

3. In **File System**, select the file system for which you want to create a mapping rule.
   - In the file system list, select a file system and click **OK**.
   - If your desired file system does not exist, click **Create** to create one. After the file system is created, select the file system and click **OK**.
4. **Optional:** In **Quota Tree**, select a quota tree.
   - In the quota tree list of the file system, select quota trees and click **OK**.
   - If your desired quota trees do not exist, click **Create** to create ones. **Table 3-60** describes the related parameters.

Table 3-60 Quota tree parameters

<table>
<tr><th>Parameter</th><th>Description</th><th>Value</th></tr>
<tr><td>Name</td><td>Quota tree name</td><td>[Value range]
■ The name must be unique.
■ For V300R006C00, the name can only contain letters, digits, and underscores (_).
■ For V300R006C10, the name can only contain letters, digits and special characters. Special characters include !"#$%&'()*+-.;<=>?@[\]^`{_|}~ and spaces. On the CLI, some characters need to be entered as escape characters. For example, \| indicates |, || indicates \, \q indicates ?, and \s indicates spaces.
■ The name can be 1 to 127 characters in length.
[Example]
quotatree001</td></tr>
<tr><td>Quantity</td><td>Number of quota trees that you want to create in batch. Set this parameter based on site requirements.</td><td>[Value range]
1 to 500
[Example]
5</td></tr>
<tr><td>Owning file system</td><td>File system to which the newly created quota tree belongs</td><td>[Example]
filesystem_001</td></tr>
</table>

Parameter	Description	Value
Quota	This parameter specifies the number and size of files in the quota tree. **NOTE** ■ If the file system for which you want to create a quota tree has requirements for quotas, you are advised to enable the quota function. ■ After selecting the option to enable the quota function, a dialog box indicating danger will be displayed when you confirm the quota tree creation. Confirm the information of the dialog box and select **I have read and understand the consequences associated with performing this operation.** Then click **OK** to complete the creation.	[Example] Enable

5. **Optional:** In **Directory**, enter an accessible directory.
6. **Share Path** of a file system consists of the values of **File System**, **Quota Tree** and **Directory**.
7. In **Priority**, set the priority of the mapping rule.
   - The value of **Priority** ranges from 1 to 1024.
   - Mappings rules are sorted by priority in descending order. If two mapping rules have the same priority, the one that is created earlier is placed in the front. Users match mapping rules in sequence.
8. Determine whether to enable **AutoCreate**.
   - If **AutoCreate** is enabled but no relative directory exists under the CIFS Homedir share path. The system will automatically create a relative directory.
   - **AutoCreate** is enabled by default. You can disable it. If **AutoCreate** is disabled and the relative directory does not exist, users fail to match this rule and will match the next one.
9. Click **OK**.
   - Created mapping rules are displayed in the mapping rule list.
   - You can modify the priority of the mapping rule and determine whether to enable **AutoCreate**.
10. Click **Next**.

Step 7 (Optional) Set security restriction. This parameter is valid only after security restriction is enabled.

1. In the **Accessible IP Address/Address Segment** area, click **Add**.

   The **Add IP Address or IP Address Segment** dialog box is displayed.

2. In **IP Address/Address Segment**, specify the IP addresses or IP address segments.

   NOTE

   – The IP address segment is in the format of IP address/mask, for example, 192.168.1.100/16. The mask of IPv4 ranges from 1 to 32, and the mask of IPv6 ranges from 1 to 128. A mixed IP address segment (IPv4 and IPv6) is not supported.
   – The IP rule can be:
     ■ A single IPv4 or IPv6 address, for example, 192.168.1.100.
     ■ An IP address segment, for example, 192.168.1.100/16 or 192.168.1.10~192.168.1.11/30.
   – A maximum of 32 IP addresses or IP address segments can be added.

3. Click **OK**.

   The added IP addresses or IP address segments are displayed in the list.

4. Click **Next**.

Step 8 (Optional) Set the file name extension filter rule. The rule can be set only after the file name extension filtering function is enabled.

NOTE

File name extension filtering rules are valid only for the current share.

1. In **File Name Extension Filtering Rule**, click **Add**.

   The **Add File Name Extension Filtering Rule** dialog box is displayed.

2. In **File Name Extension**, specify the file name extension (file type) to be filtered.

   NOTE

   – The file name extension contains 1 to 127 visible ASCII characters, and contains only digits, letters, space, and special characters (!\"#$%&\'()*+\,-.\/\:;\<=\>?@[\\]^_`{\|}~). Wildcard character * can only be the last character. For example, the file name extension can be txt, TXT, T?X, or Tx*.
   – The maximum number of filtering items supported by a share is 128.
   – The maximum number of filtering items supported by a storage system is 120,000.
   – The following are recommended configurations: One share has a maximum of seven file name extension filtering rules, and one file name extension contains 1 to 32 characters (excluding wildcards). The recommended configurations minimize the adverse impact on CIFS Homedir service performance. If the recommended configurations are not used, CIFS Homedir performance may greatly deteriorate.
   – When configuring a file name extension filtering rule, ensure that the rule does not affect the storage of temporary files that may be generated when application software is running. For example, some application software may generate files with the .tmp file name extension. In this case, add the .tmp extension to the file name extension filtering rule. For details about specific temporary file name extension of application software, contact the corresponding software vendor.

3. Select the permission rule from the **Rule Type** drop-down list.

   NOTE

   – **Denied only**: Files with the specified extension do not have access permission.
   – **Allowed only**: Only files with the specified extension have access permission.

4. Click **OK**.

   The added file name extension filter rule is displayed in the list.

5. Click **Next**.

Step 9 The **Summary** page is displayed. On the **Summary** page, check whether the CIFS Homedir information is correct. Click **Finish**.

Step 10 On the **Execution Result** page, view the execution result. Click **Close** to finish creating a CIFS Hoemdir share.

You can view the created share in the CIFS Homedir share list.

----End

3.9.3.11 Accessing Homedir Shares (Applicable to V300R006C00)

This section describes how to access Homedir shares. By accessing a Homedir share, different users can access the shared directory.

Procedure

Step 1 Right-click **Computer** on a Windows-based client.

Step 2 Select **Map Network Drive**.

Step 3 In **Folder**, enter the path of the mapped folder, and select **Connect using different credentials**.

The path format is **\\*logical ip address*\*username***, *logical ip address* indicates the logical IP address of the storage system, and *sharename* indicates the name of the Homedir share.

NOTE

If you use a domain authentication user, enter the domain user name in the **~Domain name~Domain user name** format in *User Name*.

If you use a local authentication user, enter the user name of the local authentication user in *User Name*.

Step 4 Click **Finish**.

Step 5 In **Windows Security**, enter the user name and password of the local user and click **OK**.

- In a domain, enter the domain user name in the **Domain name/Domain user name** format in **User Name** and enter the password of the domain user in **Password**.

  NOTE

  After Homedir shares are allocated to domain users, do not modify the domain user information. Otherwise, the CIFS shares cannot be accessed.

- In a non-domain environment, enter the user name and password of the local authentication user in **User Name** and **Password** respectively.

Step 6 View the mapped network drive.

Double-click **Computer**. The **Computer** window is displayed, listing mapped network drives.

Step 7 Double-click the mapped network drive to access the Homedir share.

----End

Follow-up Procedure

To cancel the sharing, run the command **net use [DeviceName] /del** in the Windows CLI. *DeviceName* indicates the disk drive that needs to be disconnected, such as **z:**.

If the information about a local authentication user or domain user is changed (for example, the user is forbiddened, the password is changed or expires, the relationship is changed, or the user is deleted) when a client accesses the file system of CIFS and FTP shares, the changed information will take effect after authentication is passed in the next time (by mounting shares again).

The storage system supports offline sharing. When a client is mounted and shared, you can still read and write on a local duplicate on the client even when it is disconnected with the storage system. When the connection resumes, data modified offline is synchronized automatically to the storage system. (If the shared data in the storage system is changed, you need to manually start the synchronization.)

3.9.3.12 Accessing a CIFS Homedir Share (Applicable to V300R006C10 and Later Versions)

This section describes how to access CIFS Homedir shares. You can access the directory (the directory is the same as the user name) under the specified file system directory.

Prerequisites

- The CIFS service is running normally.
- The CIFS user client is connected to the storage server network.
- The CIFS user has been created.
- CIFS Homedir share has been created successfully.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Provisioning** > **Port** > **Logical Ports**.

Step 3 In the logical port list, find the logical IP address for accessing CIFS share.

The running status of logical port must be **Link up**.

Step 4 Map the network drive on a client.

NOTE

In this section, the client runs Windows 7.

1. Right-click **My Computer** on the Windows-based client.
2. Choose **Map Network Drive**.

   The **Map Network Drive** dialog box is displayed.
3. In **Folder**, enter the path of the mapped folder.

   The path of the mapped folder must be in the format of \\***logical ip address**sharename***, where *sharename* indicates the name of the CIFS Homedir share that you want to access.

   NOTE

   If autohome shares are created, the path of the mapped folder can be in the format of \\logical ip address\username, \\***logical ip address*\~*domain name~domain user name***, \\logical ip address \domain user name@domain name, \\***logical ip address*\~**, or \\logical ip address\autohome.
4. Click **Finish**.

Step 5 Authenticate the user.

1. In **User Name** of the **Connect As...** dialog box, enter the user name.

In an AD domain, the user name must be entered in the format of ***Domain name* *Domain user name***.

2. In **Password**, enter the password of the domain user.
3. Click **OK**.

Step 6 View the mapped network drive.

Double-click **Computer**. The **Computer** window is displayed listing mapped network drives.

Step 7 Double-click the mapped network drive to access the CIFS share.

The domain user can perform operations on the shared directory with configured permissions.

When a client accesses a shared directory, each name of the newly created files and directories can contain a maximum of 256 characters.

NOTE

If errors occur during the access, first check whether CIFS service is enabled or not, storage system is added into AD domain or not, the network between client and storage system is normal or not, and the domain user has the access permission or not. If the preceding check items are normal, log in to DeviceManager to restart the CIFS service in **CIFS Service**. It takes a period of time for the CIFS service to take effect after the restart.

NOTICE

Restarting the CIFS service interrupts all the ongoing CIFS share services. Before restarting the CIFS service, ensure that no CIFS share service is running.

----End

3.9.3.13 CIFS Homedir Share Configuration Example (Applicable to V300R006C10 and Later Versions)

The storage system provides a wide range of functions and solutions to meet customers' service requirements. This section explains some configuration processes that meet typical service requirements.

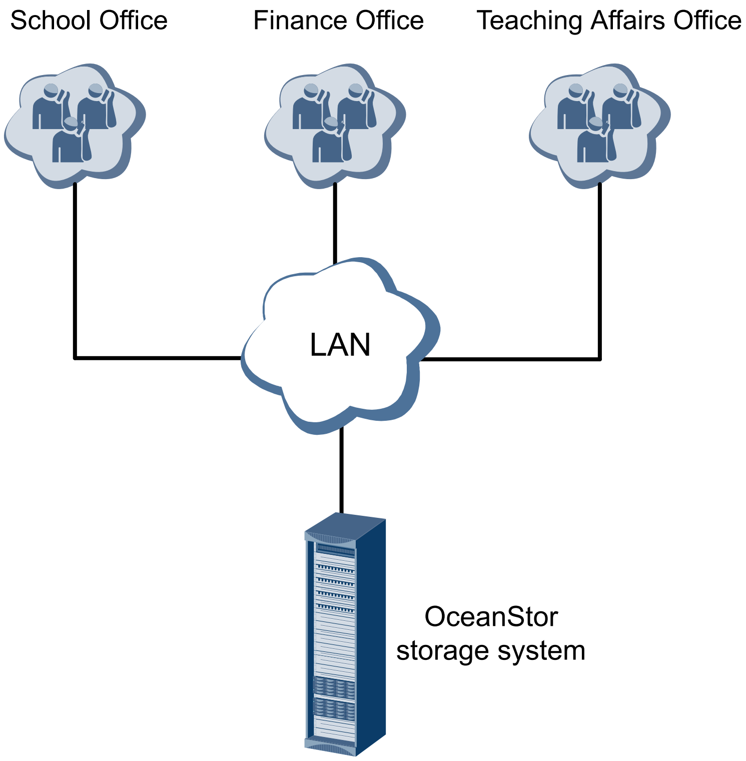
3.9.3.13.1 Scenario

A storage system is required to provide storage space for three departments of a school., and each member of the three departments has their own private directories and cannot be accessed by others. This section describes the customer's existing environment and requirements.

Network Diagram

Figure 3-18 shows the customer's network.

Figure 3-18 Customer's network diagram



The status quo of the customer's live network can be concluded as follows:

- All clients use the Windows operating system.
- The clients of the three departments reside on the same LAN as the storage system.

Customer Requirements

A storage system is required to provide storage space for the School Office, Teaching Affairs Office, and Finance Office. The storage space must be allocated as follows:

- Each of the three departments has 1 TB dedicated storage space.
- Each member of the three departments has read and write permissions to their own private directories.
- Private directories of a member in the three departments are invisible for other members.

3.9.3.13.2 Requirement Analysis

This section analyzes the customer's requirements and provides a solution.

The customer's requirements are analyzed as follows:

- All clients use the Windows operating system, so the OceanStor storage system can use the Homedir share to provide storage space for the three departments respectively.
- The Homedir multipath management function is supported, which allows employees to have their own private directories by setting rules for different Homedir shares.

Based on the previous analysis, a solution as follows is provided:

- **Table 3-61** describes the basic information of the three departments.

Table 3-61 Basic information of the three departments

Department	Share Name	User Name of the CIFS Homedir Mapping Rule.	Local User	Local User Group
School Office	share01	office*	office_user01	group01
Teaching Affairs Office	share02	education*	education_user01	group01
Finance Office	share03	finance*	finance_user01	group01

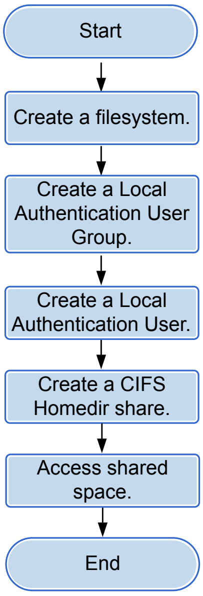
- **group01** has complete control over **share01**.

3.9.3.13.3 Configuration Process

The preceding solutions and the following configuration flowchart help you understand the subsequent configuration.

Figure 3-19 shows the configuration process.

Figure 3-19 Configuration process


Start
Create a filesystem.
Create a Local Authentication User Group.
Create a Local Authentication User.
Create a CIFS Homedir share.
Access shared space.
End

NOTE

This configuration process is only applicable to this configuration example. For the complete configuration process of CIFS Homedir share, see **3.9.3.2 Configuration Process (Applicable to V300R006C10)**.

3.9.3.13.4 Configuration Operations

After requirement analysis and service planning, you need to configure a Homedir share on DeviceManager.

Creating a File System

File systems provide storage space for shares. You can create different file systems to provide storage space for different shares.

Step 1 On the DeviceManager page, choose **Provisioning** > **File System**.

The **File System** page is displayed.

Step 2 Click **Create**.

The **Create File System** dialog box is displayed.

Step 3 In the **Create File System** dialog box, configure planned parameters. **Table 3-62** describes related parameters.

Table 3-62 Create File System parameters

Parameter	Planned Value
Name	FileSystem
Capacity	1 TB
File System Block Size	8 KB
Quantity	3
Owning Storage Pool	StoragePool000

NOTE

When creating multiple file systems, the storage system automatically appends a number to each file system name based on the number of file systems to be created for identification. Therefore, the file systems that are created are named FileSystem0000, FileSystem0001, and FileSystem0002 respectively.

Step 4 Click **OK**.

----End

Creating a Local Authentication User Group

This section explains how to create a local authentication user group. Local authentication user groups help you control the share access permissions of local users.

Step 1 On the **DeviceManager** page, click **Provisioning** > **User Authentication**.

The **User Authentication** page is displayed.

Step 2 Click **Local Authentication User Group**.

Step 3 Click **Create**.

The **Local Authentication User Group** dialog box is displayed.

Step 4 In **User Group Name**, enter **group01**.

Step 5 Click **OK**.

The system starts adding the user group.

Step 6 In the **Success** dialog box that is displayed, click **OK**.

----End

Creating a Local Authentication User

This section describes how to create a local authentication user. For applications that use local authentication, local authentication user accounts are used to access a CIFS share.

Step 1 On the **DeviceManager** page, click **Provisioning** > **User Authentication**.

The **User Authentication** page is displayed.

Step 2 Click **Create**.

The **Local Authentication User** dialog box is displayed.

Step 3 In the **Local Authentication User** dialog box, enter required local user information. **Table 3-63** describes related parameters.

Table 3-63 Local Authentication User parameters

Parameter	Value
Username	office_user01
Password NOTICE The default validity period for password is 180 days. When the password expires, the user may not access the share and services may be interrupted. You can modify the validity period for password in **More** > **Set Security Policies**.	Password
Confirm Password	confirms password
Primary Group	group01

Step 4 Click **OK**.

The system starts adding the user.

Step 5 In the **Success** dialog box that is displayed, click **OK**.

Step 6 Repeat **Step 2** to **Step 5** to add users **education_user01** and **finance_user01** to user groups **group01**.

----End

Creating a CIFS Homedir Share

After creating a local user group and local users, you need to create a CIFS Homedir share. You can assign different permissions to different users when creating a CIFS Homedir share.

Step 1 On the DeviceManager page, choose **Provisioning** > **Share**.

The **Share** page is displayed.

Step 2 Create a Homedir share.

1. Choose **CIFS Homedir** > **Create**.

   The **Create CIFS Homedir Share Wizard** page is displayed.
2. Enter **share01** for **Share Name** as the planned CIFS Homedir share name and enter **%d %w** for **Relative Directory**. **%d%w** is a wildcard character, which automatically matches the user's domain name and user name, thereby allowing each user to have their own space.
3. Click **Next**.

   The **Set Permissions** page is displayed.
4. Click **Next**.

   The **No permission for the user/user group to access the CIFS Homedir share. Are you sure you want to continue?** dialog box is displayed.

   NOTE

   Access permission configurations for the CIFS Homedir share are introduced in **Step 3**.
5. Click **OK**.

   The **Set Mapping Rule** page is displayed.
6. Click **Next**.

   The **No mapping rule for the CIFS Homedir share. Are you sure you want to continue?** dialog box is displayed.

   NOTE

   Mapping rule configurations for the CIFS Homedir share are introduced in **Step 4**.
7. Click **OK**.

   The **Set Mapping Rule** page is displayed.
8. Click **Next**.

   The **Summary** page is displayed.
9. Click **Finish**.

   The **Execution Result** page is displayed.
10. Click **Close**.

Step 3 Configure access permissions for the CIFS Homedir share.

1. Select **share01**.
2. In **Users/User Groups**, click **Add**.

   The **Add User/User Group** dialog box is displayed.
3. In **User/User Group**, select **Local user group**. In **Name**, click **Find**.

   The **Select User Group** dialog box is displayed.
4. Select user group **group01** and click **OK**.

   The **Add User/User Group** dialog box is displayed.

5. In **Permission Level**, select **Read-write**. Click **OK**.

   The **Execution Result** page is displayed.

6. Click **Close**.

Step 4 Add mapping rules for Homedir share.

1. Select **share01**.
2. Click **Add** on the **CIFS Homedir Mapping Rule** tab page.

   The **Add CIFS Homedir Mapping Rule** dialog box is displayed.

3. Enter **office*** for **Username**.
4. Click ... next to **File System**.

   The **Select File System** dialog box is displayed.

5. Select the file system whose **Name** is set to **FileSystem0000**, and click **OK**.

   The **Add CIFS Homedir Mapping Rule** dialog box is displayed.

6. Click **OK**.

   The **Warning** dialog box is displayed.

7. Confirm the information in the dialog box and select **I have read and understand the consequences associated with performing this operation**. Click **OK**.

   The **Success** page is displayed.

8. Click **OK**.

Step 5 Repeat **Step 4** to add mapping rules for the Homedir share. For mapping rules, see **Table 3-64**.

Table 3-64 Mapping Rule Planning

Department	Share Name of Homedir	Username of Mapping Rule	Name of File System	Local User	Local User Group
School Office	share01	office*	FileSystem000	office_user01	group01
Teaching Affairs Office	share01	education*	FileSystem001	education_user01	group01
Finance Office	share01	finance*	FileSystem002	finance_user01	group01

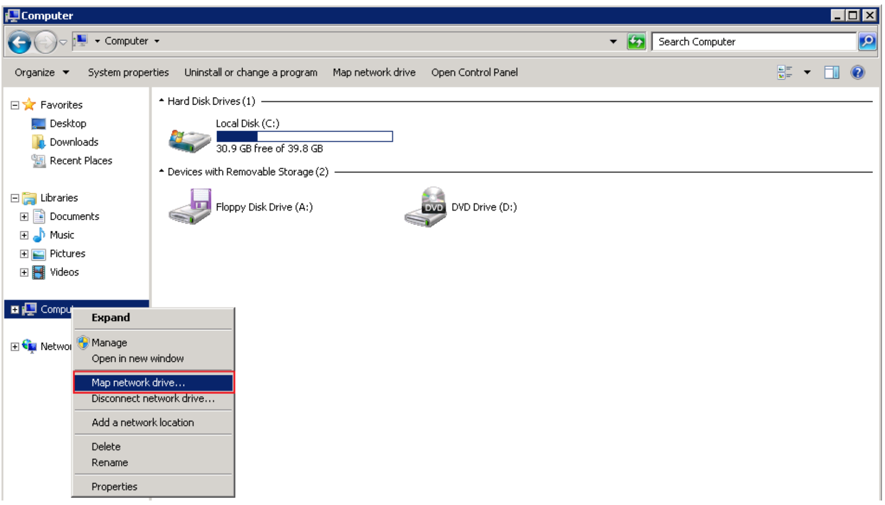
----End

Accessing Shared Space

After a Homedir share is configured, users need to map the shared space provided by the storage system to the network drive on the client. This section describes how to map the network drive on a client of the School Office. You can map the network drives on the other clients in the same way. Note that user names **education_user01** and **finance_user01** must be used to map the network drives on the clients of the Teaching Affairs Office and Finance Office.

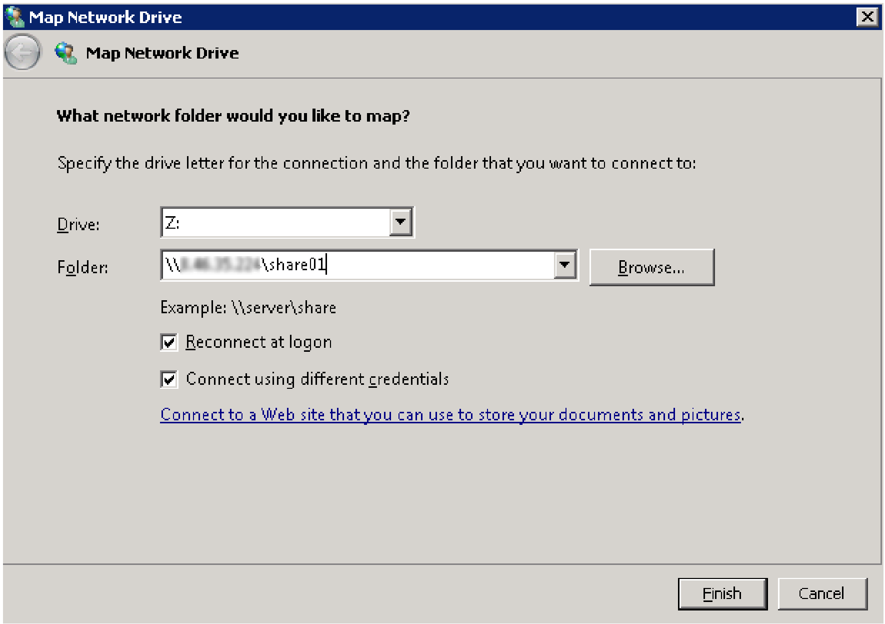
Step 1 Map a network drive to a client.

1. Right-click **Computer** on a Windows-based client, and select **Map Network Drive**.



2. In **Folder**, enter **\\172.16.150.40\share01**, and select **Connect using different credentials**.

   172.16.150.40 is the logical IP address of the storage system.



Map Network Drive

Map Network Drive

What network folder would you like to map?

Specify the drive letter for the connection and the folder that you want to connect to:

Drive: Z:

Folder: \\[redacted]\share01

Browse...

Example: \\server\share

☑ Reconnect at logon

☑ Connect using different credentials

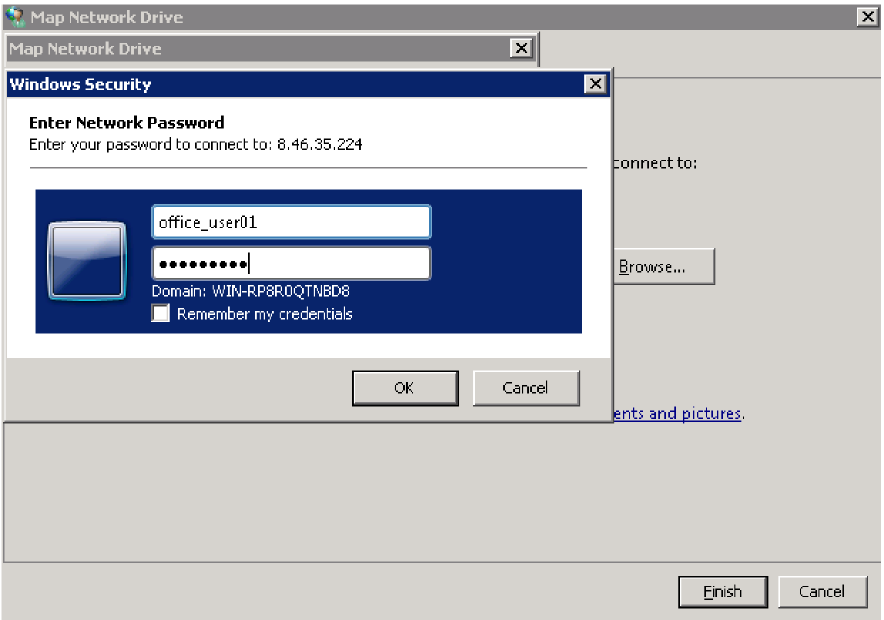
Connect to a Web site that you can use to store your documents and pictures.

Finish Cancel

3. Click **Finish**.

Step 2 Authenticate the user.

1. In the **Windows Security** dialog box, enter local user name **office_user01** in **User Name**.
2. In **Password**, enter the password of user **test_user01**.



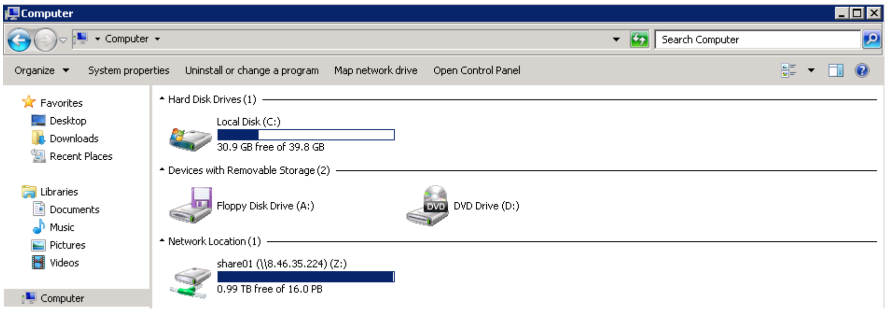
Enter Network Password
Enter your password to connect to: 8.46.35.224

office_user01
•••••••••
Domain: WIN-RP8R0QTNBD8
□ Remember my credentials

3. Click **OK**.

Step 3 View the mapped network drive.

Double-click **Computer**. The **Computer** window is displayed, listing mapped network drives.



----End

3.9.4 Cross-Protocol Share Access

Storage system allows NFS sharing and CIFS sharing to be configured for the same file system concurrently. This chapter describes how the storage system uses the user mapping function to allow users to access shared files across protocols (CIFS-NFS) used by clients on different platforms and obtain precise permission control.

3.9.4.1 Overview

This section introduces the user mapping mechanism used during cross-protocol (CIFS-NFS) share access.

CIFS-NFS Cross-Protocol Share Access

Storage system allows users to share a file system or quota tree using NFS and CIFS at the same time. Different clients, such as Windows clients (CIFS), Linux clients (NFS), and Mac OS X clients (CIFS or NFS) can access a file system or quota tree simultaneously. Since

Windows, Linux, and UNIX adopt different mechanisms to authenticate users and control access, the storage system manages user mapping and permission control of different operating systems in a unified manner, protecting the security of CIFS-NFS cross-protocol access.

- If a CIFS user attempts to access a file or directory on the storage system, the storage system authenticates local or AD domain users in the first place. If the UNIX permission (UNIX Mode bits, or NFSv4 ACL) has been configured for the file or directory to be accessed, the CIFS user is mapped as an NFS user based on preset user mapping rules during authentication. Then the storage system performs UNIX permission authentication for the user.
- If an NFS user attempts to access a file or directory that has NT ACL on the storage system, the NFS user is mapped as a CIFS user based on the preset mapping rules. Then the storage system performs NT ACL permission authentication for the user.

CIFS-NFS Cross-Protocol Access Permissions

If permission types of a file or directory and a client that attempts to access the file or directory mismatch, CIFS-NFS cross-protocol access is required. You need to map the permission of the file or directory so that it can be displayed by the client.

- NFS client accessing a file or directory with the NTFS permission

  When an NFS client checks the NTFS permission that a file or directory has, the client can obtain the UNIX permission mapped from an NT ACL. The NFS client displays as many permissions as possible but the actual permissions are determined by the NT ACL. For example, the NFS client shows that all users have read, write, and execute permissions, but one of the users may only have the write permission.
- CIFS client accessing a file or directory with the UNIX permission

  When a CIFS client checks the UNIX permission that a file or directory has, the UNIX permission is mapped into three ACEs for the CIFS client. The three ACEs are for the owner, owner primary group, and **everyone** of the file or directory respectively. The NT ACL is displayed only but not used to control actual operation permissions.

Table 3-65 shows how permissions convert among UNIX Mode bits, NFSv4 ACL, and NT ACL.

Table 3-65 Permission conversion among UNIX Mode bits, NFSv4 ACL, and NT ACL

File Permission	Permission Conversion
The file or directory only has valid UNIX Mode bits.	● One ACL is mapped based on UNIX Mode bits when an NFS or CIFS client sends a request to read an ACL. ● If an NFSv4 client sends a request to set an ACL, an NFSv4 ACL takes effect and UNIX Mode bits are mapped based on the NFSv4 ACL. ● If a CIFS client sends a request to set an ACL, an NT ACL takes effect and UNIX Mode bits with the maximum permissions are mapped based on the NT ACL.

File Permission	Permission Conversion
The file or directory has a valid NFSv4 ACL or NT ACL.	● NFS clients use the **chmod** command to change permissions. The NFSv4 ACL or NT ACL is abandoned and UNIX Mode bits take effect. ● NFS clients use the **chmod** command to add or remove SUID/SGID/STICKY. The NFSv4 ACL or NT ACL is abandoned and UNIX Mode bits take effect.
The file or directory has a valid NFSv4 ACL.	● If an NFS client sends a request to read UNIX Mode bits, UNIX Mode bits (mapped based on the NFSv4 ACL) of the storage system are returned directly. ● If a CIFS client sends a request to read an NT ACL, an NT ACL is mapped based on the NFSv4 ACL (an NT ACE corresponding to V4Domain\name is generated for each NFSv4 ACE). Due to the difference between ordering rules of the NFSv4 ACL and NT ACL, the CIFS client may display a message indicating that the order of the NT ACL mapped based on the NFSv4 ACL is incorrect. Before setting an ACL on a CIFS client, delete all mapped NFSv4 ACLs. Otherwise, the setting will not take effect. ● If a CIFS client sends a request to set an NT ACL, all ACEs that correspond to V4Domain and are mapped based on the NFSv4 ACL must be deleted on the CIFS client, and new NT ACEs must be added. Then, the NFSv4 ACL is abandoned and the NT ACL takes effect. UNIX Mode bits are mapped based on the NT ACL.
The file or directory has a valid NT ACL.	● If an NFS client sends a request to read UNIX Mode bits, UNIX Mode bits (mapped based on the NT ACL) of the storage system are returned directly. ● If an NFSv4 client sends a request to read an NFSv4 ACL, an NFSv4 ACL is mapped based on UNIX Mode bits of the storage system. ● If the NFSv4 client sends a request to set an NFSv4 ACL, an NT ACL is discarded, an NFSv4 ACL takes effect, and UNIX Mode bits are mapped from the NFSv4 ACL.

CIFS-NFS Cross-Protocol User Mapping

Windows systems (CIFS) and Linux systems (NFS) use different mechanisms to identify and authenticate users:

- Windows systems use security identifiers (SIDs) to identify users. SIDs apply to all users, user groups, services, and computers in the systems. Regarding authentication, CIFS supports NT ACLs.
- Linux systems use user identities (UIDs) and one or more group identities (GIDs) to identify users. One user belongs to one user group at least. Regarding authentication, NFS supports diversified security control mechanisms such as UNIX Mode bits and NFSv4 ACL.

During CIFS-NFS cross-protocol share access, users using different protocols must be mapped based on user mapping rules for user authentication and precise permission control.

The timing of user mapping is as follows:

- When a CIFS client accesses files or directories with the NFSv4 ACL or UNIX Mode bits permission, a user mapping occurs. The user will have both the permissions before and after the user is mapped.
- When an NFS client accesses files or directories with the NT ACL permission, a user mapping occurs. The user will have both the permissions before and after the user is mapped.
- Cross-protocol permission editing changes permission types. For example, users are mapped when an NFS client accesses a file or directory that has the NT ACL permission. If the NFS client runs the **chmod** command or sets the NFSv4 ACL to change the permission of the file or directory, users are not mapped when the NFS client accesses the file or directory after the change. That is, users' permissions remain unchanged.

  NOTE

  You are advised not to edit permissions across protocols, avoiding permission type changes.
- When the parent directory has the inheritable NT ACL permission, the files or directories created no matter on an NFS client or a CIFS client will have the NT ACL permission by default. In this case, if the NFS client accesses files or directories, a user mapping will always occur. That is, the user will have both the permissions before and after the user is mapped. When the parent directory does not have the inheritable NT ACL permission, the files or directories created no matter on an NFS client or a CIFS client will have the UNIX Mode bits permission. In this case, if the NFS client accesses files or directories, no user mapping occurs. That is, the user's permission remains unchanged.
- If mappings are changed on CIFS clients, the change takes effect after CIFS connections are disconnected and next re-authentication is performed.
- User mappings on NFS clients are cached and expire after four hours by default. New user mappings and user information changes take effect after the cached data expires.

User mapping rules specify the mappings among different user accounts. The user mapping rules can be saved in a local database or managed in the AD domain in a centralized manner. A user mapping rule includes the mapping type, original user, mapped user, and mapping priority. If a user matches multiple mapping rules, it is mapped based on the rule with a higher priority. If the rules have the same priority, the user is mapped based on the rule that is configured the earliest.

A user mapping process is as follows: (Local mapping of a storage system is used as an example.)

- NFS-CIFS user mapping: An NFS user is authenticated by UID on the service end. When a user mapping occurs, the user name to which the UID corresponds will be queried in the sequence of the local host, LDAP domain, and NIS domain. Based on the queried user name and the local mapping, the user name, SID, and the owning group of the mapped user will be queried.
- CIFS-NFS user mapping: A CIFS user is authenticated by SID on the service end. When a user mapping occurs, the mapped user will be queried based on the user name to which the SID corresponds and the local mapping. Then the UID to which the mapped user name corresponds and its owing group will be queried in the sequence of the local host, LDAP domain, and NIS domain.

NOTE

You are advised not to configure the same UIDs or user names in the local host, LDAP domain, or NIS domain. If the same UIDs or user names exist, the user mapping results will not be the expected results.

After a user is mapped, the owner information of the files or directories owned by CIFS users (the files or directories that are created by CIFS users or the owner information of the files or directories are changed to CIFS users) is the information of the NFS users mapped from CIFS users on the NFS client. If no mapping rules have been configured for CIFS users, the owner information of the files or directories is about the IDs (calculated using IDMAP, a hash algorithm) of the CIFS users on the NFS client. If the client is an NFSv4 client, the owner information is displayed as **nobody**.

After a user is mapped, the owner information of the files or directories owned by NFS users (the files or directories that are created by NFS users or the owner information of the files or directories are changed to NFS users) is about NFS user names on the CIFS client:

- When NFS users are NIS domain users, the owner information is displayed as **NIS_DOMAIN***user name*.
- When NFS users are LDAP domain users, the owner information is displayed as **LDAP_DOMAIN***user name*.

NOTE

When CIFS users are mapped to NFS users, quota statistics will be collected for the NFS users or owning user group.

3.9.4.2 Managing User Mappings Across Protocols (CIFS-NFS)

Managing user mappings across protocols (CIFS-NFS) including configuring the mapping parameters and creating a user mapping.

3.9.4.2.1 Configuring Mapping Parameters

You can create user mappings in the local storage system as well as use user mappings in the external IDMU domain to access shares across different systems. The following introduces how to set the mapping mode as well as timeout duration of the IDMU query, and search for the domain name.

Context

If you only use IDMU user mappings, you do not need to configure user mappings in the local storage system.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Provisioning** > **User Authentication** > **User Mapping**.

Step 3 Click **Set Mapping Parameters**.

Step 4 Set the mapping parameters by referring to**Table 3-66**.

Table 3-66 Parameter description

Parameter Name	Description	Value
Mapping Mode	A global parameter of user mappings, including: ● User mapping not supported: The system does not support user mappings. ● User mapping supported (Mapping rules set in local): The system only supports user mappings created locally. ● User mapping supported (Mapping rules set in IDMU): The system only supports user mappings in the IDMU domain. ● User mapping supported (Mapping rules set in IDMU and local, IDMU preferentially): When user mappings of a specific original user exist both in the system and the IDMU domain, the system preferentially uses the mapping in the IDMU domain. ● User mapping supported (Mapping rules set in local and IDMU, local preferentially): When user mappings of a specific original user exist both in the local system and the IDMU domain, the mappings in the local system are used preferentially.	[Example] User mapping supported (Mapping rules set in IDMU): The storage system only supports user mappings in the IDMU domain.
IDMU Search Timeout Duration (s)	Timeout duration for the system to search for specific user mappings in the IDMU domain.	[Value range] 5~120 [Default value] 15

Parameter Name	Description	Value
IDMU Search DN	Benchmark directory where the system searches for specific user mappings in the IDMU domain. The benchmark directory stores the information of user mappings.	[Value range] The directory contains 0 to 255 characters. [Default value] None [Example] **DC=auth2kh8,DC=com** when the domain name is auth2k8.com.

Step 5 Click **OK**.

The **Success** dialog box is displayed.

Step 6 Click **OK**.

----End

3.9.4.2.2 Creating a Local System User Mapping

This operation enables the system to map the original user to the target user based on a mapping relationship for accessing shares across protocol.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Provisioning** > **User Authentication** > **User Mapping**.

Step 3 Click **Create**.

The **Create User Mapping** dialog box is displayed.

Step 4 Set the related parameters of the user mapping. **Table 3-67** explains the related parameters.

Table 3-67 User mapping parameters

Parameter Name	Description	Value
Mapping Type	A user mapping type related to the operating system, including: ● Windows to Unix: When accessing Unix shares using Windows, a Windows user has all the permissions granted to the target user. ● Unix to Windows: When accessing Windows shares using Unix, a Unix user has all the permissions granted to the target user.	[Example] Windows to Unix
Source User	The original user in a mapping.	[Example] sourceuser
Target User	The target user in a mapping.	[Example] targetuser

Step 5 Click **Add**, and set the **Priority**.

NOTE

Priority: A smaller number indicates a higher priority. When multiple mappings share the same original user, the system uses the mapping with the highest priority.

Step 6 **Optional:** Click **Test** ▶ to check whether the target user exists.

NOTE

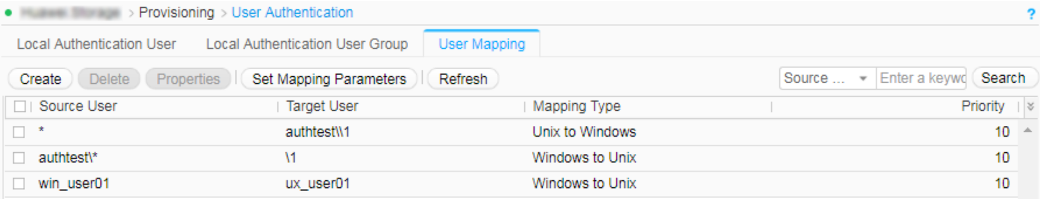
Click **Remove** 🗑 to delete the user mapping.

Step 7 Click **OK**.

Step 8 Click **Close**.

----End

Example



□ Source User	Target User	Mapping Type	Priority
□ *	authtest\\1	Unix to Windows	10
□ authtest*	\1	Windows to Unix	10
□ win_user01	ux_user01	Windows to Unix	10

- User mapping rule 1: A UNIX user is mapped to a user of the same name in the AD domain (domain name: **authtest**). For example, UNIX user **ABC** is mapped to user **ABC** in the AD domain.
  - Source user: *
  - Target user: authtest\\1
  - Mapping type: Unix to Windows
  - Priority: 10 (default)
- User mapping rule 2: A user in the AD domain (domain name: **authtest**) is mapped to a UNIX user of the same name.
  - Source user: authtest*
  - Target user: \1
  - Mapping type: Windows to Unix
  - Priority: 10 (default)
- User mapping rule 3: Windows user **win_user01** is mapped to UNIX user **ux_user01**.
  - Source user: win_user01
  - Target user: ux_user01
  - Mapping type: Windows to Unix
  - Priority: 10 (default)

3.9.4.3 Accessing a CIFS File Across Protocols

This section describes how an NFS client accesses CIFS files and directories for which the NT ACL permission has been configured.

Prerequisites

- The user of the Linux client has the same UID and GID as the local authentication user.

  You can query the local authentication user ID and ID of its owning primary group on the DeviceManager. On the Linux client, you can run the **groupadd -g** *GID user group name* command to create a user group, and then run the **useradd -u** *UID user name* command to create a user.
- If the NFS client uses NFSv4, enable the NFSv4 service in the storage system and enter the domain name based on the specific environment:
  - In non-domain or LDAP environment, enter the default domain name **localdomain**.
  - In an NIS environment, the entered information must be consistent with domain in the **/etc/idmapd.conf** file on the Linux client that accesses shares. It is recommended that both the two be the domain name of the NIS domain.
- Before you use an AD domain user to configure user mapping rules, the storage system (vStore) has been added to the AD domain.

Context

Before users can use an NFS client to access shared files and folders for which the NT ACL has been configured, the administrator needs to follow the process as shown in **Figure 3-20** to configure related parameters.

Figure 3-20 Flowchart of configuring cross-protocol access of a CIFS file

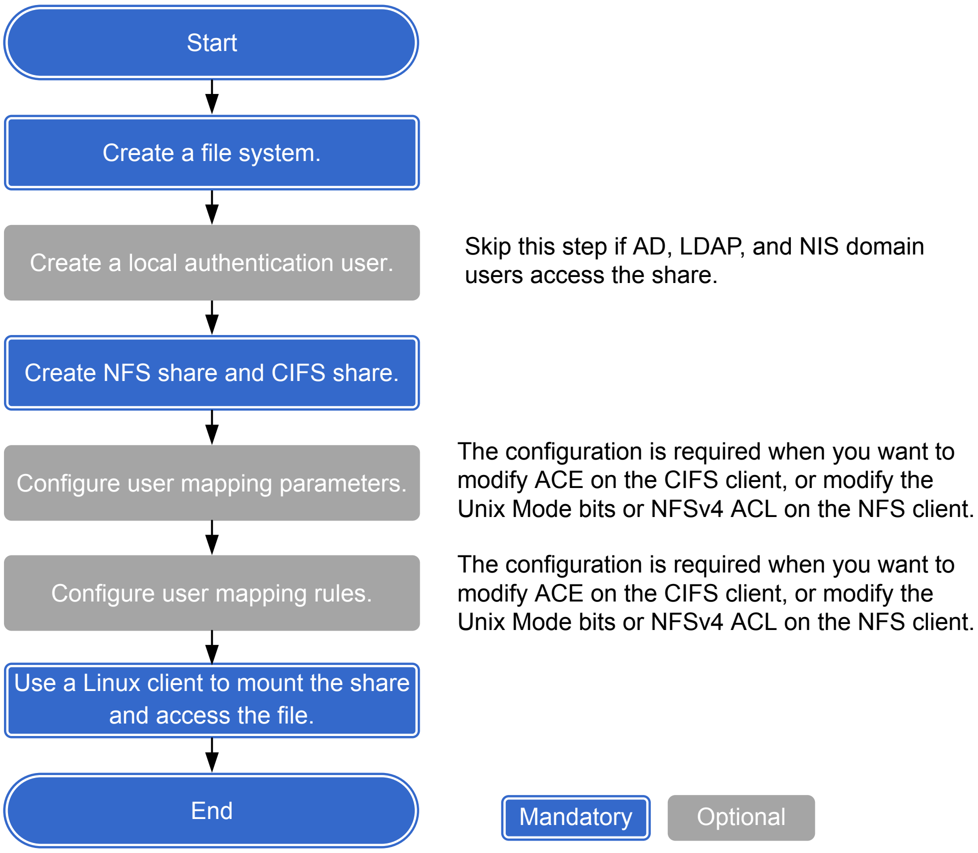

Start
Create a file system.
Create a local authentication user.
Skip this step if AD, LDAP, and NIS domain users access the share.
Create NFS share and CIFS share.
Configure user mapping parameters.
The configuration is required when you want to modify ACE on the CIFS client, or modify the Unix Mode bits or NFSv4 ACL on the NFS client.
Configure user mapping rules.
The configuration is required when you want to modify ACE on the CIFS client, or modify the Unix Mode bits or NFSv4 ACL on the NFS client.
Use a Linux client to mount the share and access the file.
End
Mandatory
Optional

Table 3-68 provides an example of data planning during the configuration.

Table 3-68 Example of data planning

Item	Planned Value	Description
File system	Name: share_dir	-
Local authentication user	local_user1	In this example, the default user group **default_group** is selected as the primary group.
NFS client user	linux_user1	The user must have the same UID and GID as the local authentication user.

Item	Planned Value	Description
NFS share	● Type of the client: host ● Name or IP address: 10.68.0.10 ● Permission: Read-write ● Advanced: The default settings are used.	In this example, the **Read-write** permission for the NFS share is added to the client. In **Advanced**, default settings are used.
CIFS share	● Share Name: share_dir_cifs ● Oplock: Enable ● Notify: Enable ● User/User Group: local authentication user **local_user1** ● Permission Level: Full control	In this example, the **Full control** permission for the CIFS share is added to local authentication user **local_user1**.
Mapping Mode	Local system user mappings are supported preferentially.	-
User mapping rule	● Mapping Type: Unix to Windows ● Source User: **linux_user1** ● Target User: **local_user1** ● Priority: 10	In this example, a Unix to Windows mapping rule is created. The source user is local authentication user **linux_user1**, whereas the target user is local authentication user **local_user1**. The priority of the mapping rule is set to **10**.

Procedure

Step 1 Log in to DeviceManager.

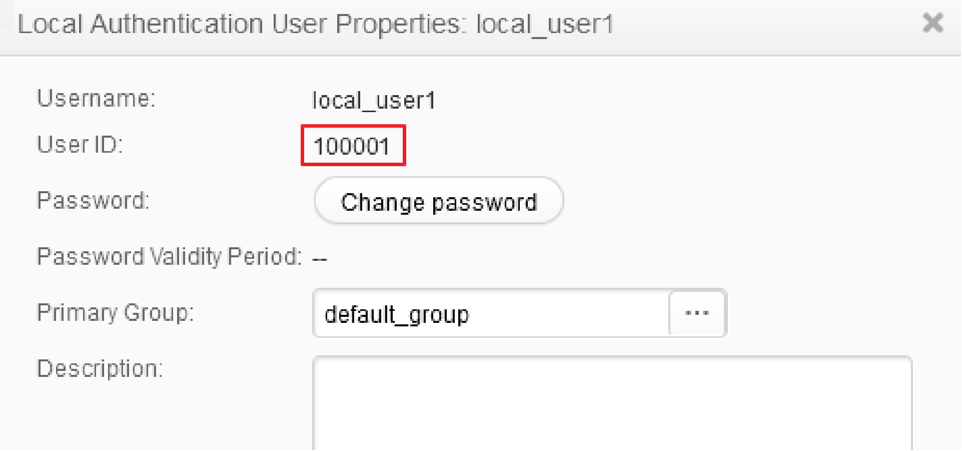
Step 2 Create a file system.

1. Select **Provisioning** > **File System**.
2. Create a file system named **share_dir** as planned.

Step 3 Create a local authentication user and record its ID and the ID of its owning primary group.

1. Select **Provisioning** > **User Authentication** > **Local Authentication User**.
2. Click **Create** and create local authentication user **local_user1** as planned.
3. Select **local_user1** and click **Properties**. Then record the user ID.

Figure 3-21 Recording the ID of the local authentication user


Local Authentication User Properties: local_user1

Username: local_user1

User ID: 100001

Password: Change password

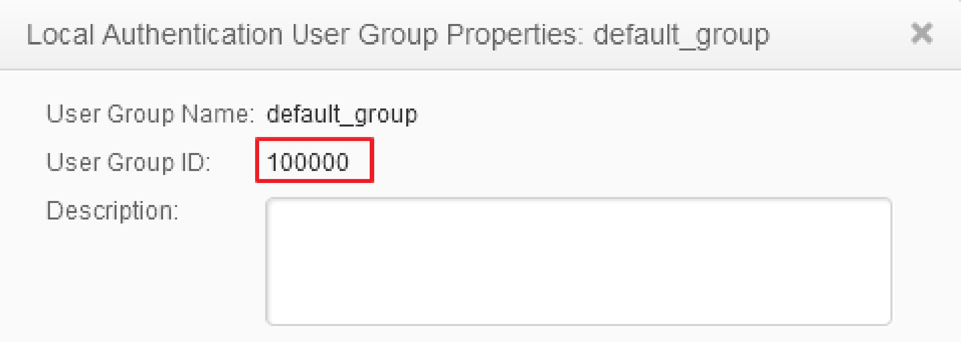
Password Validity Period: --

Primary Group: default_group

Description:

4. Click the **Local Authentication User Group** tab, select **default_group**, and click **Properties** to record the ID of the owning primary group of the local authentication user.

Figure 3-22 Recording the ID of the owning primary group of the local authentication user


Local Authentication User Group Properties: default_group

User Group Name: default_group

User Group ID: 100000

Description:

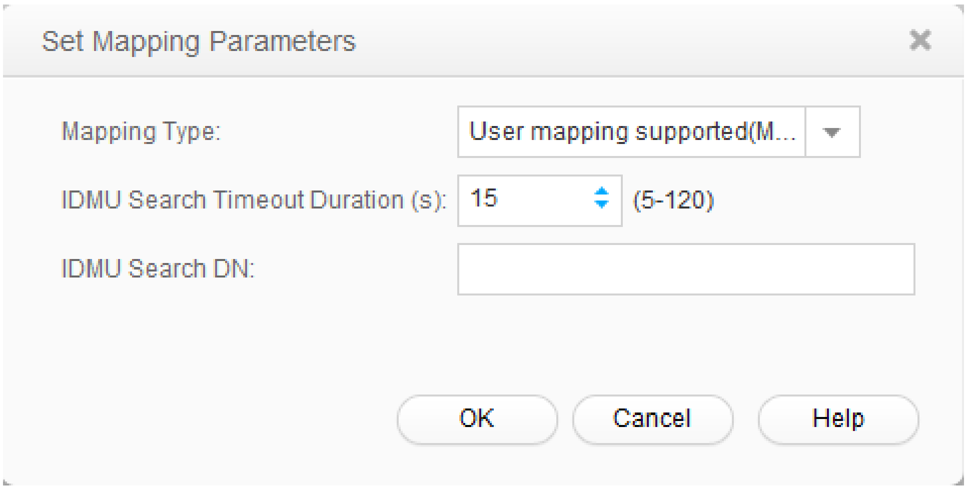
Step 4 Create an NFS share and a CIFS share for the same file system.

1. Select **Provisioning** > **Share**.
2. Create an NFS share and a CIFS share for the same file system based on parameters as planned.

Step 5 Configure user mapping parameters.

1. Select **Provisioning** > **User Authentication** > **User Mapping**.
2. Click **Set Mapping Parameters** and set **Mapping Mode** to **Local system user mappings are supported preferentially.**

Figure 3-23 Configuring user mapping parameters



Set Mapping Parameters

Mapping Type: User mapping supported(M...

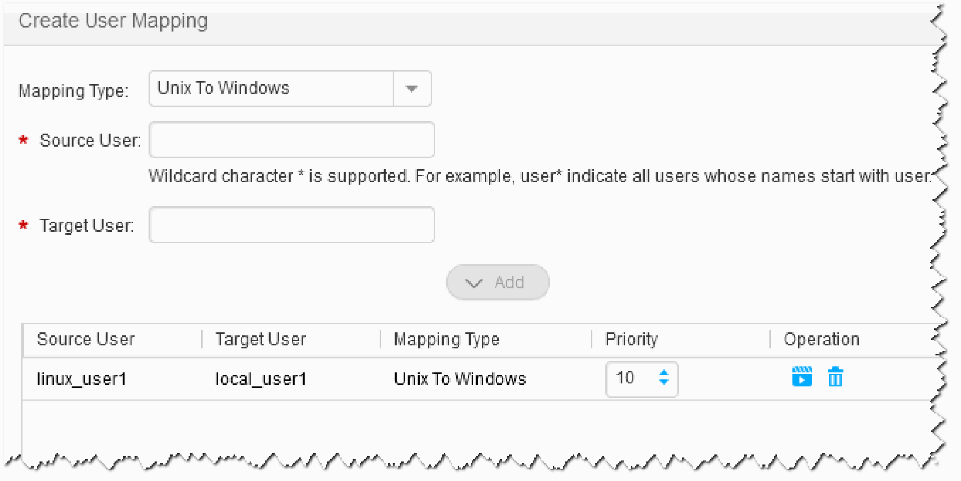
IDMU Search Timeout Duration (s): 15 (5-120)

IDMU Search DN:

Step 6 Configure user mapping rules.

1. Select **Provisioning** > **User Authentication** > **User Mapping**.
2. Click **Create** and configure user mapping rules as planned.

Figure 3-24 Configuring user mapping rules



Create User Mapping

Mapping Type: Unix To Windows

* Source User:

Wildcard character * is supported. For example, user* indicate all users whose names start with user.

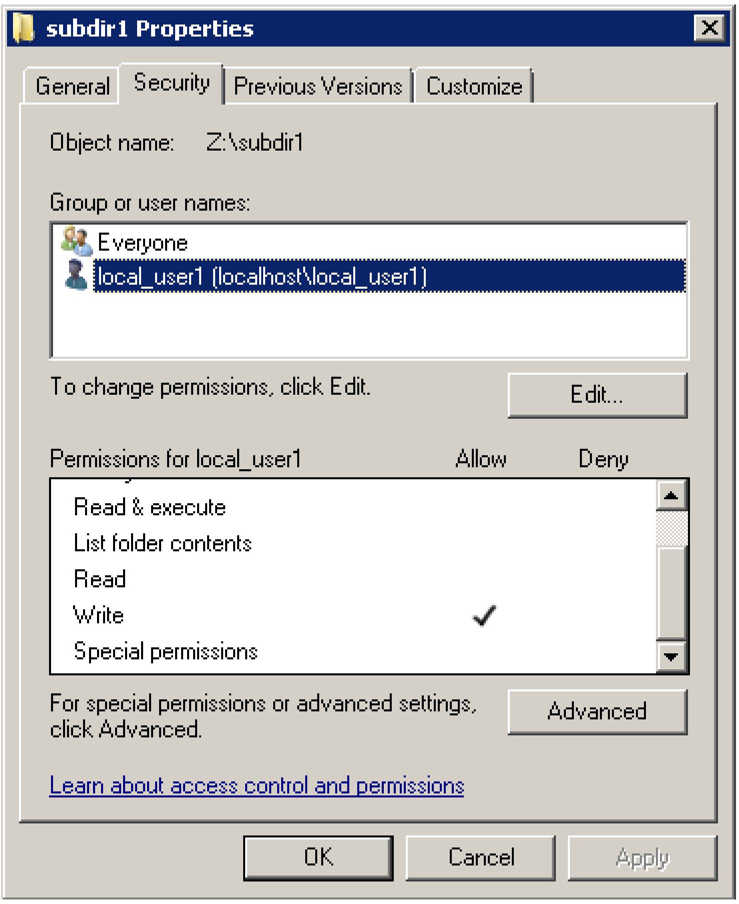
* Target User:

Source User	Target User	Mapping Type	Priority	Operation
linux_user1	local_user1	Unix To Windows	10	

Step 7 Use a Windows client to access shared directory **share_dir** and set permissions of files under the shared directory.

1. Use a Windows client to access a CIFS share.
2. Under the shared directory, create folder **subdir1** and file **file1**.
3. Add one ACE to **subdir1** and **file1**.

   Right-click the file or folder and choose properties from the shortcut menu that is displayed. In the properties dialog box that is displayed, click the **Security** tab and add the write permission ACE to user **local_user1**.



Object name: Z:\subdir1

Group or user names:

Everyone
local_user1 (localhost\local_user1)

To change permissions, click Edit.

Permissions for local_user1	Allow	Deny
Read & execute		
List folder contents		
Read		
Write	✓	
Special permissions		

For special permissions or advanced settings, click Advanced.

Step 8 Use an NFS client to mount the share and access the share as local user **linux_user1**.

1. Use an NFS client to mount the NFS share.
2. Run the **groupadd -g 100000 linux_group** command to create a user group that has the same d GID as the local authentication user group.
3. Run the **useradd -u 100001 -g 10000 linux_user1** command to create a user that has the same UID and GID as the local authentication user.

   NOTE

   The UID and GID in the command are used as an example only. They vary with site conditions.
4. Run the **su - linux_user1** command to switch users.
5. Write data to folder **subdir1**.

   If the data is written to the folder successfully, the Linux client has a write permission for the folder.

----End

3.9.4.4 Accessing an NFS File Across Protocols

This section describes how a CIFS client accesses an NFS share for which the UNIX permission has been configured.

Prerequisites

- The IDMU component has been installed on the AD domain server and the NIS has been enabled.

- Configuring a storage system to add it to a NIS domain has been completed and the NIS server is the NIS service of the AD domain controller.
- The user of the Linux client has the same UID and GID as the local authentication user.

  You can query the local authentication user ID and ID of its owning primary group on the DeviceManager. On the Linux client, you can run the **groupadd -g** *GID user group name* command to create a user group, and then run the **useradd -u** *UID user name* command to create a user.
- If the NFS client uses NFSv4, enable the NFSv4 service in the storage system and enter the domain name based on the specific environment:
  - In non-domain or LDAP environment, enter the default domain name **localdomain**.
  - In an NIS environment, the entered information must be consistent with domain in the **/etc/idmapd.conf** file on the Linux client that accesses shares. It is recommended that both the two be the domain name of the NIS domain.

Context

Before users can use a Windows client to access shared files and folders for which the UNIX permission has been configured, the administrator needs to follow the process as shown in **Figure 3-25** to configure related parameters.

Figure 3-25 Flowchart of configuring cross-protocol access of an NFS file

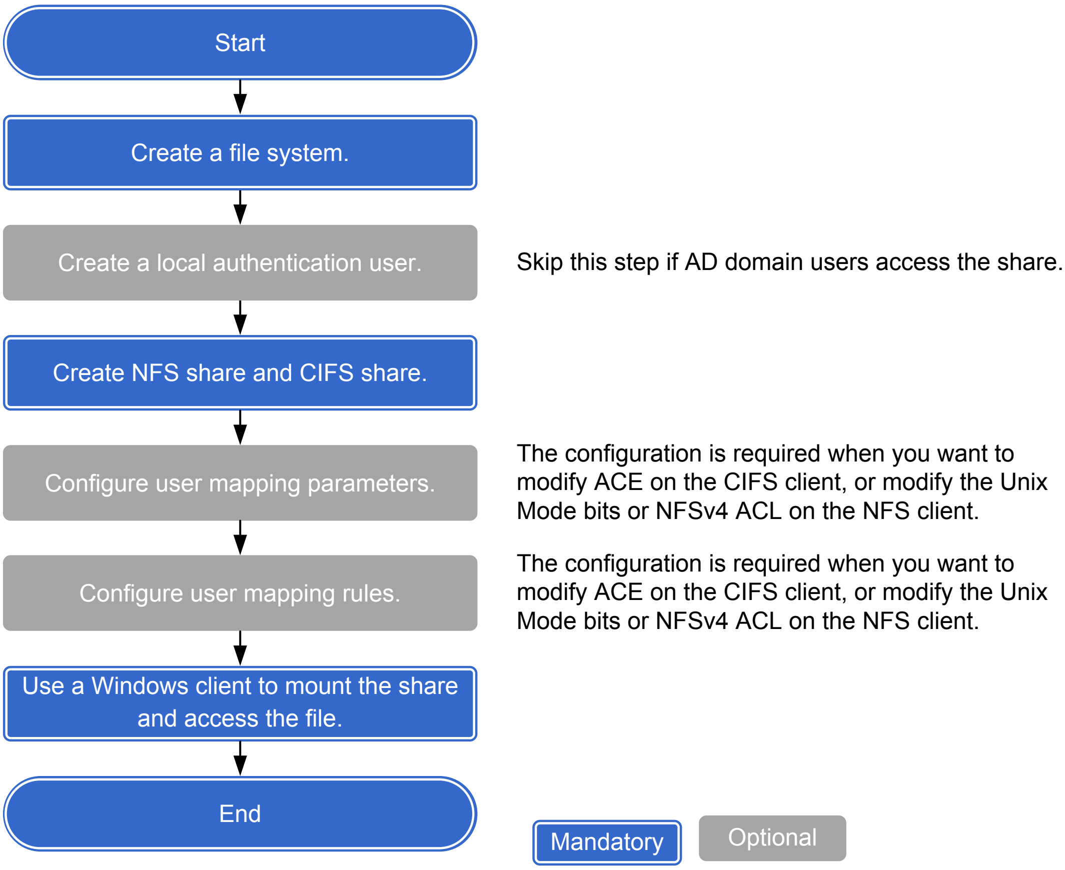

Start
Create a file system.
Create a local authentication user.
Skip this step if AD domain users access the share.
Create NFS share and CIFS share.
Configure user mapping parameters.
The configuration is required when you want to modify ACE on the CIFS client, or modify the Unix Mode bits or NFSv4 ACL on the NFS client.
Configure user mapping rules.
The configuration is required when you want to modify ACE on the CIFS client, or modify the Unix Mode bits or NFSv4 ACL on the NFS client.
Use a Windows client to mount the share and access the file.
End
Mandatory
Optional

Table 3-69 provides an example of data planning during the configuration.

Table 3-69 Example of data planning

Item	Planned Value	Description
File system	Name: share_dir2	-
Local authentication user	local_user2	In this example, the default user group **default_group** is selected as the primary group.
NFS client user	linux_user2	The user must have the same UID and GID as the local authentication user.
NFS share	● Type of the client: host ● Name or IP address: 10.68.0.10 ● Permission: Read-write ● Advanced: The default settings are used.	In this example, the Read-write permission for the NFS share is added to the client. In **Advanced**, default settings are used.
CIFS share	● Share Name: share_dir_cifs2 ● Oplock: Enabled ● Notify: Enabled ● User/User Group: local authentication user local_user2 ● Permission Level: Full control	In this example, the Full control permission for the CIFS share is added to local authentication user **local_user2**.
Mapping Mode	Local system user mappings are supported preferentially.	-
User mapping rule	● Mapping Type: Windows to Unix ● Source User: local_user2 ● Target User: linux_user2 ● Priority: 10	In this example, a **Windows to Unix** mapping rule is created. The source user is local authentication user **local_user2**, whereas the target user is local authentication user **linux_user2**. The priority of the mapping rule is set to **10**.

Windows operating systems do not allow a file name to contain special characters. Therefore, it is recommended that the file name and directory name of an NFS share do not contain special characters including \:*/?"<>|, and the file name and directory name do not end with a period (.) or a space. Otherwise, the storage system converts the file name and directory name to short names (for example, **~PY203**).

Procedure

Step 1 Log in to DeviceManager.

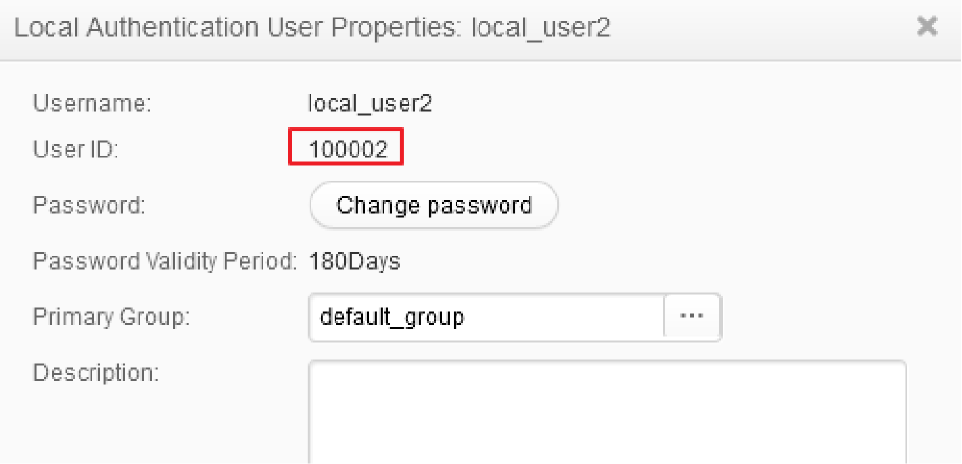
Step 2 Create a file system.

1. Select **Provisioning** > **File System**.
2. Create a file system named **share_dir2** as planned.

Step 3 Create a local authentication user and record its ID and the ID of its owning primary group.

1. Select **Provisioning** > **User Authentication** > **Local Authentication User**.
2. Click **Create** and create local authentication user **local_user2** as planned.
3. Select **local_user2** and click **Properties**. Then record the user ID.

Figure 3-26 Recording the ID of the local authentication user



Local Authentication User Properties: local_user2

Username: local_user2

User ID: 100002

Password: Change password

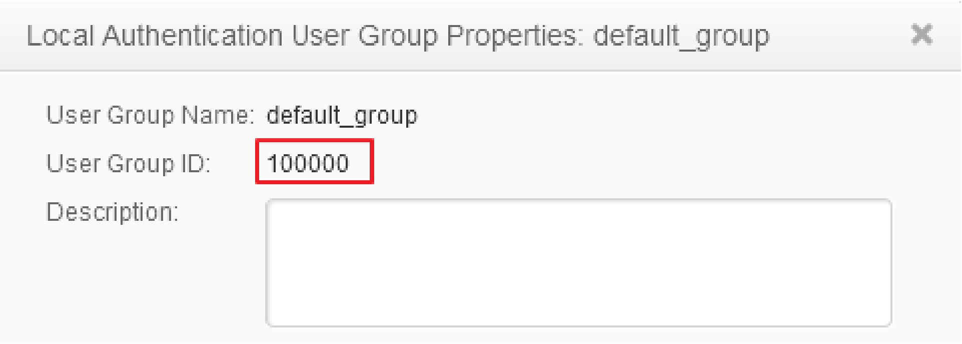
Password Validity Period: 180Days

Primary Group: default_group

Description:

4. Click the **Local Authentication User Group** tab, select **default_group**, and click **Properties** to record the ID of the owning primary group of the local authentication user.

Figure 3-27 Recording the ID of the owning primary group of the local authentication user



Local Authentication User Group Properties: default_group

User Group Name: default_group

User Group ID: 100000

Description:

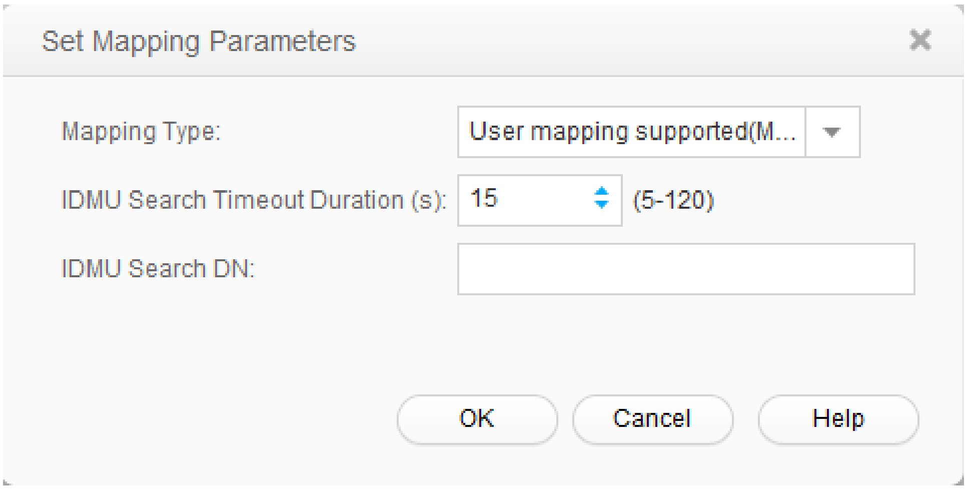
Step 4 Create an NFS share and a CIFS share for the same file system.

1. Select **Provisioning** > **Share**.
2. Create an NFS share and a CIFS share for the same file system based on parameters as planned.

Step 5 Configure user mapping parameters.

1. Select **Provisioning** > **User Authentication** > **User Mapping**.
2. Click **Set Mapping Parameters** and set **Mapping Mode** to **Local system user mappings are supported preferentially.**

Figure 3-28 Configuring user mapping parameters


Set Mapping Parameters

Mapping Type: User mapping supported(M...

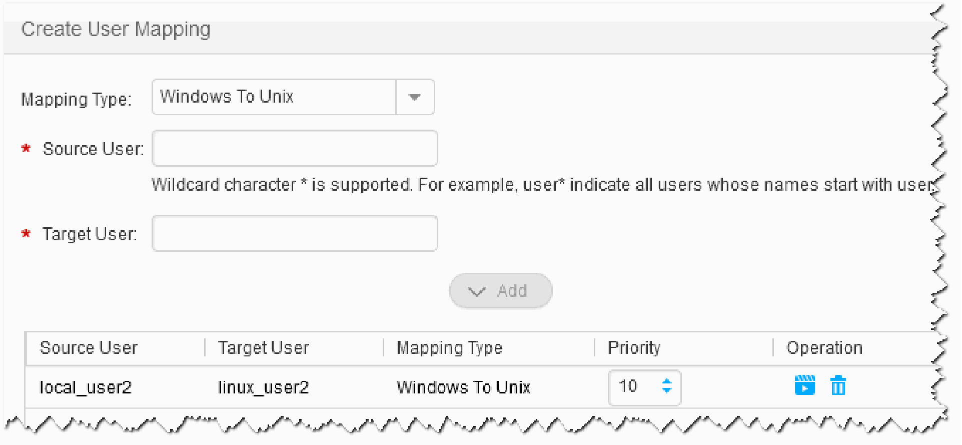
IDMU Search Timeout Duration (s): 15 (5-120)

IDMU Search DN:

Step 6 Configure user mapping rules.

1. Select **Provisioning** > **User Authentication** > **User Mapping**.
2. Click **Create** and configure user mapping rules as planned.

Figure 3-29 Configuring user mapping rules


Create User Mapping

Mapping Type: Windows To Unix

* Source User:

Wildcard character * is supported. For example, user* indicate all users whose names start with user

* Target User:

Source User	Target User	Mapping Type	Priority	Operation
local_user2	linux_user2	Windows To Unix	10	

Step 7 Use an NFS client to mount the share and set permissions of files under the shared directory.

1. Use an NFS client to mount the NFS share.
2. Run the **groupadd -g 100000 linux_group** command to create a user group that has the same d GID as the local authentication user group.
3. Run the **useradd -u 100002 -g 10000 linux_user2** command to create a user that has the same UID and GID as the local authentication user.

   NOTE

   The UID and GID in the command are used as an example only. They vary with site conditions.
4. Run the **su - linux_user2** command to switch users.
5. In the shared path, create a file **hard.txt** and run the **ln** command to point hard link **hard_file** to the file respectively.

Step 8 Use a Windows client to access the shared directory, and open, read data from, write data to, close, delete, and rename files under the shared directory.

1. On the Windows client, use **local_user2** to access shared directory **share_dir2**.
2. Open, read data from, write data to, close, delete, and rename files under the shared directory.

   All operations on the folder and files are successful.

----End

3.9.5 FTP-based File System Access

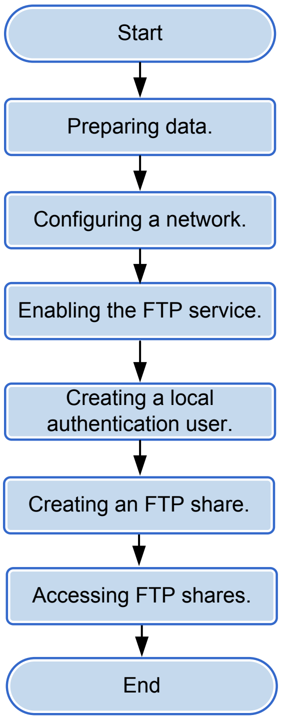
Storage system supports the FTP share file system and enables you to allocate different FTP share access permissions to different users.

3.9.5.1 Configuration Process

This section describes the FTP share configuration process.

Figure 3-30 shows the FTP share configuration process.

Figure 3-30 FTP share configuration process



3.9.5.2 Preparing Data

Before configuring an FTP share, obtain information about storage system IP addresses, shared file systems, local authentication users, and user permissions to assist in the follow-up configuration.

Table 3-70 describes preparations required for configuring an FTP share.

Table 3-70 Preparations required for configuring an FTP share

Item	Description	Example
IP address of the storage system *Indicates the service IP address used by a storage system.*	Storage system can provide FTP share for the client by using the Ethernet port or the Logical port.	Logical IP address 172.16.128.10
File system *Indicates a file system for which an FTP share is configured.*	Storage system enables you to configure a file system or its quota tree[a] as an FTP share.	FileSystem001

Item	Description	Example
User *Indicates a user employed to access an FTP share. Storage systems employ local authentication users to enable clients to access FTP shares.*	The user name: ● Must contain 8 to 32 characters by default. ● Cannot contain space, double quotation mark ("), slash (/), backslash (\\), square brackets ([]), larger than (<), less than (>), plus (+), colon (:), semicolon (;), comma (,), question mark (?), asterisk (*), vertical bar (|), equal mark (=), (@), or end with a period (.). I **NOTE** You cannot use the user accounts retained in the system, including: ● User accounts retained in Windows: **Everyone**, **Local**, **Creator Owner**, **Creator Group**, **Creator Owner Server**, **Creator Group Server**, **Owner Rights**, **Group Rights**, **NT Pseudo Domain**, **Dialup**, **Network**, **Batch**, **Interactive**, **Service**, **Anonymous Logon**, **Proxy**, **Enterprise Domain Controllers**, **Self**, **Authenticated Users**, **Restricted**, **Terminal Server User**, **Remote Interactive Logon**, **This Organization**, **System**, **Local Service**, **Network Service**, **Write Restricted**, **Other Organization**, **Builtin**, **Internet$**, **Members can fully administer the computer/domain**, **Users**, **Guests**, **Power Users**, **Members can share directories**, **Account Operators**, **Server Operators**, **Print Operators**, **Backup Operators**, **Members can bypass file security to back up files**, **Replicator**, **Current Owner**, **Current Group**. ● User accounts retained in Linux: **root**, **nogroup**, **nobody**, **ftp**, **anonymous**, **daemon**, **nobody**, **news**, **sshd**, **messagebus**. ● User accounts retained in a storage system: **ibc_os_hs**.	test_user01

Item	Description	Example
User group *User group that employs local authentication.*	The user group name: - Must contain 1 to 32 characters. - Cannot contain space, double quotation mark ("), slash (/), backslash (\), square brackets ([]), larger than (<), less than (>), plus (+), colon (:), semicolon (;), comma (,), question mark (?), asterisk (*), vertical bar (|), equal mark (=), (@), or end with a period (.). **NOTE** You cannot use the user accounts retained in the system, including: - User accounts retained in Windows: **Everyone**, **Local**, **Creator Owner**, **Creator Group**, **Creator Owner Server**, **Creator Group Server**, **Owner Rights**, **Group Rights**, **NT Pseudo Domain**, **Dialup**, **Network**, **Batch**, **Interactive**, **Service**, **Anonymous Logon**, **Proxy**, **Enterprise Domain Controllers**, **Self**, **Authenticated Users**, **Restricted**, **Terminal Server User**, **Remote Interactive Logon**, **This Organization**, **System**, **Local Service**, **Network Service**, **Write Restricted**, **Other Organization**, **Builtin**, **Internet$**, **Members can fully administer the computer/domain**, **Users**, **Guests**, **Power Users**, **Members can share directories**, **Account Operators**, **Server Operators**, **Print Operators**, **Backup Operators**, **Members can bypass file security to back up files**, **Replicator**, **Current Owner**, **Current Group**. - User accounts retained in Linux: **root**, **nogroup**, **nobody**, **ftp**, **anonymous**, **bin**, **daemon**, **sys**, **tty**, **disk**, **lp**, **www**, **kmem**, **wheel**, **mail**, **news**, **uucp**, **shadow**, **dialout**, **audio**, **floppy**, **cdrom**, **console**, **utmp**, **public**, **video**, , **games**, **xok**, **trusted**, **modem**, **man**, **users**, **nobody**, **nogroup**, **sshd**, **postfix**, **maildrop**. - User accounts retained in a storage system: **ibc_os_hs**.	default_group

Item	Description	Example
Permission *Permission of a user group to access a share.*	Permissions include: ● Viewing a file list: Users can view FTP share contents. ● Creating a file: Users can create files in the FTP share directory. ● Uploading a file: Users can upload files to an FTP share. ● Downloading a file: Users can download files from an FTP share. ● Deleting a file: Users can delete files from an FTP share.	Viewing a file list, creating a file, uploading a file, downloading a file, deleting a file.
a: Quota tree is a special directory of the file system. You can set a directory quota on the quota tree to manage the space used by all files under the directory.		

3.9.5.3 Configuring a Network

This section describes how to use DeviceManager to configure a logical IP address for a storage system. The logical IP address is used for accessing shares.

3.9.5.3.1 (Optional) Configuring DNS-based Load Balancing Parameters (Applicable to V300R006C10 and Later Versions)

Storage arrays' DNS-based load balancing feature can detect the IP address load on the arrays in real time and use a proper IP address as the DNS response to achieve load balancing among IP addresses. This section describes how to configure DNS-based load balancing and DNS zones.

Context

Working principle:

1. When a host accesses the NAS service of a storage array using the domain name, the host first sends a DNS request to the built-in DNS server of the storage array and the DNS server obtains the IP address according to the domain name.
2. When a domain name contains multiple IP addresses, the storage array selects the IP address with a light load as the DNS response based on the configured load balancing policy and returns the DNS response to the host.
3. After receiving the DNS response, the host sends a service request to the destination IP address.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Settings** > **Storage Settings** > **File Storage Service** > **DNS-based Load Balancing**.

Step 3 Table 3-71 lists parameters related to DNS-based load balancing.

Table 3-71 DNS-based load balancing parameters

Parameter	Description	Value
DNS-based Load Balancing	Enables or disables DNS-based load balancing. **NOTE** ● When enabling the DNS-based load balancing function, you are advised to disable the global namespace forwarding function. This function affects DNS-based load balancing. ● After the DNS-based load balancing function is disabled, the domain name resolution service is unavailable and file systems cannot use the function. ● This parameter can be set only in the system view, not in the vStore view. The setting takes effect for the entire storage system.	[Example] Enable

Parameter	Description	Value
Load Balancing Policy	This parameter enables you to configure DNS-based load balancing policies. A storage system supports the following load balancing policies: ● Weighted round robin: When a client uses a domain name to initiate an access request, the storage system calculates the weight based on the performance data. Under the same domain name, IP addresses that are required to process loads have the same probability to be selected to process client services. ● CPU usage: When a client uses a domain name to initiate an access request, the storage system calculates the weight based on the CPU usage of each node. Using the weight as the probability reference, the storage system selects a node to process the client's service request. ● Bandwidth usage: When a client uses a domain name to initiate an access request, the storage system calculates the weight based on the total bandwidth usage of each node. Using the weight as the probability reference, the storage system selects a node to process the client's service request. ● Open connections: When a client uses a domain name to initiate an access request, the storage system calculates the weight based on the NAS connections of each node. Using the weight as the probability reference, the storage system selects a node to process the client's service request. ● Overall load: When a client uses a domain name to initiate an access request, the storage system selects a node to process the client's service request based on the comprehensive load. The comprehensive node load is calculated based on the CPU usage, bandwidth usage, and number of NAS connections. Less	[Example] Weighted round robin

Parameter	Description	Value
	loaded nodes are more likely to be selected. NOTE This parameter can be set only in the system view, not in the vStore view. The setting takes effect for the entire storage system.	

Step 4 Configure a DNS zone.

A DNS zone contains IP addresses of a group of logical ports. A host can use the name of a DNS zone to access shared services provided by a storage system. Services can be evenly distributed to logical ports.

NOTE

Only the logical ports whose **Role** is **Service** or **Management+Service** can be added into a DNS zone. The logical ports whose **Role** is **Management** cannot be added in to a DNS zone.

1. Add a DNS zone.
   a. Click **Add**.
   b. The **Add DNS Zone** dialog box is displayed. In **Domain Name**, type the domain name of the DNS zone you want to add and click **OK**.

      NOTE

      The domain name complexity requirements are as follows:
      - A domain name contains 1 to 255 characters and consists of multiple labels separated by periods (**.**).
      - A label contains 1 to 63 characters including letters, digits, hyphens (-), and underscores (_), and must start and end with a letter or a digit.
      - The domain name must be unique.
2. Remove a DNS zone.
   a. In the DNS zones that are displayed, select a DNS zone you want to remove.
   b. Click **Remove**.
3. Modify a DNS zone.
   a. In the DNS zones that are displayed, select a DNS zone you want to modify.
   b. Click **Modify**.
   c. The <**Modify DNS Zone** dialog box is displayed. In **Domain Name**, type the domain name of the DNS zone you want to modify and click **OK**.
4. View a DNS zone.
   a. In **DNS Zone**, type a keyword and click **Search**.
   b. In **DNS Zone**, the DNS zone names relevant to the keyword will be displayed.

      NOTE

      You can select a DNS zone to modify or remove it.

Step 5 Click **Save**. The **Warning** dialog box is displayed.

Step 6 Confirm the information in the dialog box and select **I have read and understand the consequences associated with performing this operation**.

Step 7 Click **OK**. The **Execution Result** page is displayed.

Step 8 On the **Execution Result** page, confirm the modification and click **Close**. The DNS zone configuration is complete.

----End

Follow-up Procedure

Choose **Provisioning** > **Port** > **Logical Ports** to configure **Listen DNS Query Request** and **DNS Zone** information for logical ports.

3.9.5.3.2 Creating a Logical Port

This operation enables you to create a logical port for managing and accessing file based on Ethernet ports, bond ports, or VLANs.

Precautions

The number of logical ports created for each controller is recommended not more than 64. If the number exceeds 64 and a large number of ports do not work properly, logical ports drift towards the small number of ports available. As a result, service performance deteriorates.

Procedure

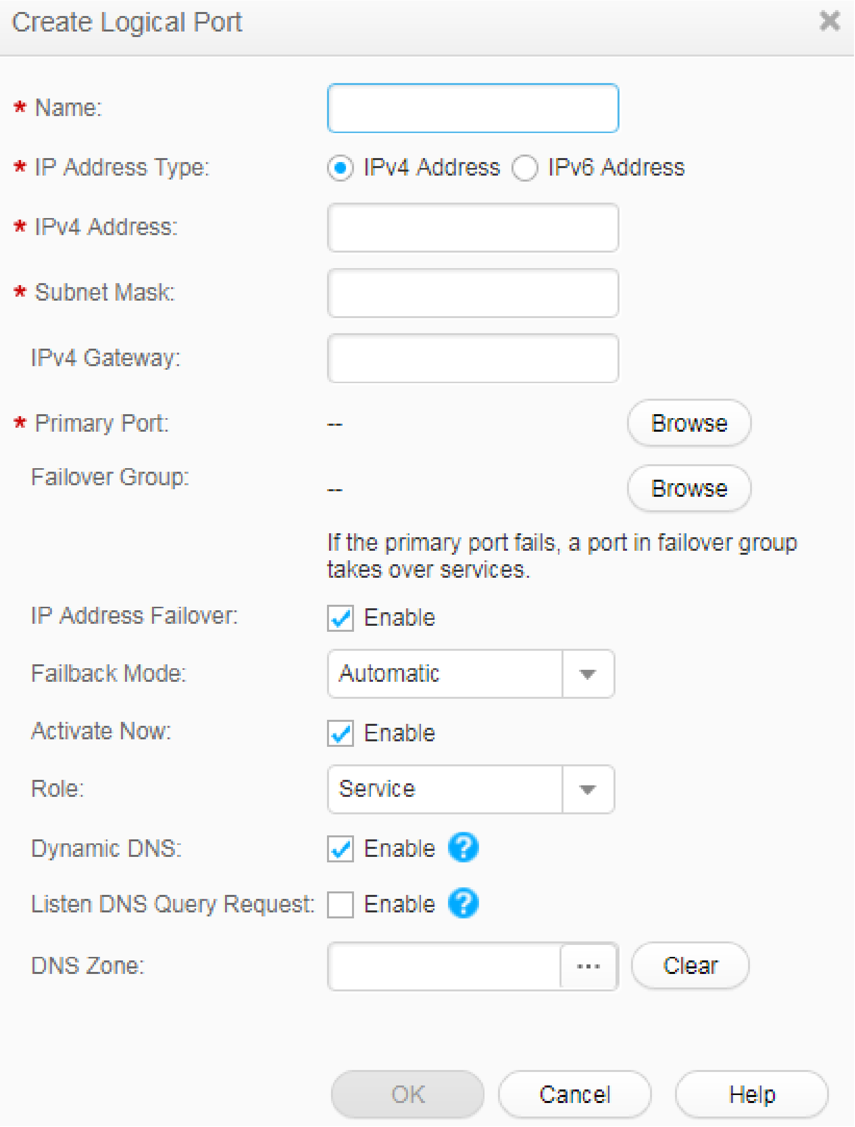
Step 1 Log in to DeviceManager.

Step 2 Choose **Provisioning** > **Port** > **Logical Ports**.

Step 3 Click **Create**.

The **Create Logical Port** dialog box is displayed.

Step 4 In the **Create Logical Port** dialog box, configure related parameters.
Table 3-72 describes related parameters.



Create Logical Port

* Name:	
* IP Address Type:	● IPv4 Address ○ IPv6 Address
* IPv4 Address:	
* Subnet Mask:	
IPv4 Gateway:	
* Primary Port:	-- Browse
Failover Group:	-- Browse If the primary port fails, a port in failover group takes over services.
IP Address Failover:	☑ Enable
Failback Mode:	Automatic
Activate Now:	☑ Enable
Role:	Service
Dynamic DNS:	☑ Enable
Listen DNS Query Request:	□ Enable
DNS Zone:	... Clear

Table 3-72 Logical port parameters

Parameter	Description	Value
Name	Name of the logical port. The name must meet the following requirements so that the logical port is available to compatible applications: ● The name must be unique. ● The name can contain only letters, digits, underscores (_), periods (.), and hyphens (-). ● The name contains 1 to 31 characters.	[Example] lif01
IP Address Type	IP address type of the logical port, including IPv4 or IPv6.	[Example] IPv4
IPv4 Address	IPv4 address of the logical port.	[Example] 192.168.100.11
Subnet Mask	IPv4 subnet mask of the logical port.	[Example] 255.255.0.0
IPv4 Gateway	IPv4 gateway of the logical port.	[Example] 192.168.100.1
IPv6 Address	IPv6 address of the logical port.	[Example] fc00::1234
Prefix	IPv6 prefix length of the logical port.	[Example] 64
IPv6 Gateway	IPv6 gateway of the logical port.	[Example] fc00::1
Primary Port	Port to which the logical port belongs, including the Ethernet port, Bond port, and VLAN.	[Example] None

Parameter	Description	Value
Failover Group	Failover group name. **NOTE** ● If a failover group is specified, services on the failed primary port will be taken over by a port in the specified failover group. ● If no failover group is specified, services on the failed primary port will be taken over by a port in the default failover group.	[Example] None
IP Address Failover	After IP address failover is enabled, services are failed over to other normal ports within the failover group if the primary port fails. However, the IP address used by services remains unchanged. **NOTE** Shares of file systems do not support the multipathing mode. IP address failover is used to improve reliability of links.	[Example] Enable
Failback Mode	Mode in which services fail back to the primary port after the primary port is recovered. The mode can be manual or automatic. **NOTE** ● If **Failback Mode** is **Manual**, ensure that the link to the primary port is normal before the failback. Services will manually fail back to the primary port only when the link to the primary port keeps normal for over five minutes. ● If **Failback Mode** is **Automatic**, ensure that the link to the primary port is normal before the failback. Services will auto fail back to the primary port only when the link to the primary port keeps normal for over five minutes.	[Example] Automatic

Parameter	Description	Value
Activate Now	To activate the logical port immediately.	[Example] Enable
Role	Roles of logical ports include the following: ● Management: The port is used by a super administrator to log in to the system for management. ● Service: The port is used by a super administrator to access services such as file system CIFS shares. ● Management+Service: The port is used by a super administrator to log in to the system to manage the system and access services.	[Example] Service
Dynamic DNS	When the dynamic DNS is enabled, the DNS server will automatically and periodically update the IP address configured for the logical port.	[Example] Enable
Listen DNS Query Request	After this function is enabled, external NEs can access the DNS service provided by the storage system by using the IP address of this logical port.	[Example] Enable

Parameter	Description	Value
DNS Zone	Name of a DNS zone. **NOTE** ● If the value is blank, the logical port is not used for DNS-based load balancing. ● Only the logical ports whose **Role** is **Service** or **Management+Service** can be added into a DNS zone. The logical ports whose **Role** is **Management** cannot be added in to a DNS zone. ● One logical port can be associated with only one DNS zone. One DNS zone can be associated with multiple logical ports. ● A DNS zone can be associated with both IPv4 and IPv6 logical ports. ● The load balancing effect varies with the distribution of logical ports associated with a DNS zone. To obtain a better load balancing effect, ensure that logical ports associated with a DNS zone are evenly distributed among controllers.	[Example] None

Step 5 Click **OK**.

The **Success** dialog box is displayed indicating that the logical port has been successfully created.

Step 6 Click **OK**.

----End

3.9.5.3.3 (Optional) Creating a Bond Port

This section describes how to bond Ethernet ports on a same controller.

Prerequisites

Ethernet ports that have IP addresses cannot be bound. The IP addresses of the bonded host ports need to be cleared before bonding.

Context

- Port bonding provides more bandwidth and redundancy for links. Although ports are bonded, each host still transmits data through a single port and the total bandwidth can

be increased only when there are multiple hosts. Determine whether to bond ports based on site requirements.

- The port bond mode of a storage system has the following restrictions:
  - On the same controller, a bond port is formed by a maximum of eight Ethernet ports.
  - Only the interface modules with the same port rate (GE or 10GE) can be bonded.
  - The port cannot be bonded across controllers. Non-Ethernet network ports cannot be bonded.
  - SmartIO interface modules cannot be bonded if they work in cluster or FC mode or run FCoE service in FCoE/iSCSI mode.
  - Read-only users are unable to bind Ethernet ports.
  - Each port only allows to be added to one bonded port. It cannot be added to multiple bonded ports.
  - Ports are bonded to create a bond port that cannot be added to the port group.
- After Ethernet ports are bonded, **MTU** changes to the default value and you must set the link aggregation mode for the ports. For example, on Huawei switches, you must set the ports to the static LACP mode.

  NOTE

  The detailed link aggregation mode varies with the switches' manufacturer.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Provisioning** > **Port** > **Bond Ports**.

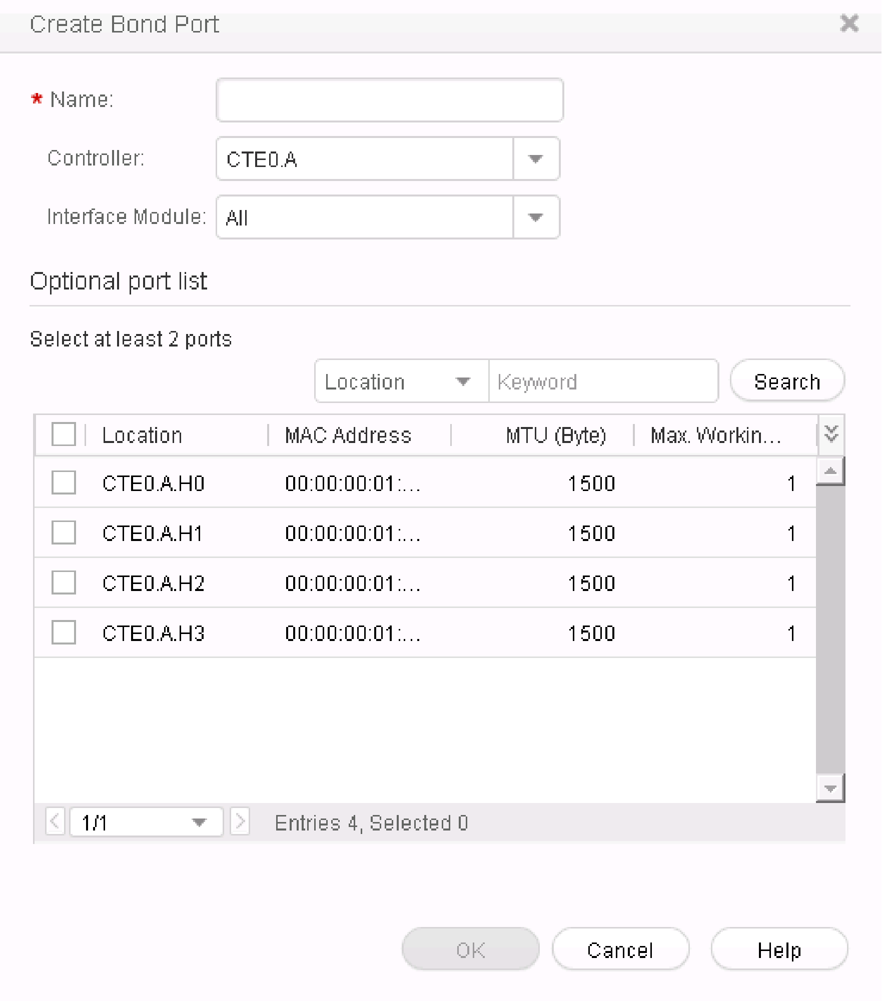
Step 3 Click **Create**.

The **Create Bond Port** dialog box is displayed.

NOTE

The port name format is **controller enclosure ID.interface module ID.port ID**.

Step 4 Set the name, interface module, and optional ports that can be bonded with the current Ethernet port.



□ Location	MAC Address	MTU (Byte)	Max. Workin...
□ CTE0.A.H0	00:00:00:01:...	1500	1
□ CTE0.A.H1	00:00:00:01:...	1500	1
□ CTE0.A.H2	00:00:00:01:...	1500	1
□ CTE0.A.H3	00:00:00:01:...	1500	1

1. In **Name**, enter a name for the bond port.

   The name:

   - Contains only letters, digits, underscores (_), periods (.), and hyphens (-).
   - Contains 1 to 31 characters.
2. From the **Controller**, select the controller the Ethernet ports own to.
3. Select the **Interface Module**.
4. From the **Optional port list**, select the Ethernet ports you want to bond.

   NOTE

   Select at least two ports.
5. Click **OK**.

   The security alert dialog box is displayed.

Step 5 Confirm that you want to bond these Ethernet ports.

1. Confirm the information of the dialog box and select **I have read and understand the consequences associated with performing this operation.**.
2. Click **OK**.

   The **Success** dialog box is displayed indicating that the operation succeeded.
3. Click **OK**.

----End

3.9.5.3.4 (Optional) Managing a Route of Logical Port

You need to configure a route when the FTP server and the storage system are not on the same network. If the FTP server and logical IP addresses cannot ping each other, add a route from the logical IP addresses to the network segment of the FTP server.

Prerequisites

The logical port has been assigned an IP address.

Procedure

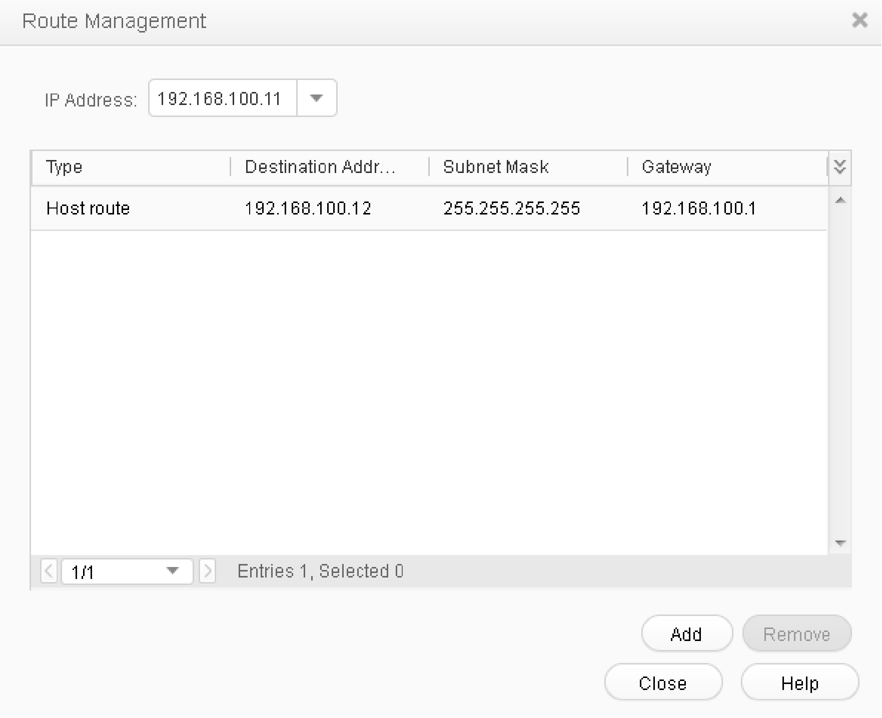
Step 1 Log in to DeviceManager.

Step 2 Go to the route management page.

You can go to the route management page by using either of the following methods:

- Choose **Provisioning** > **Port** > **Logical Ports**. Select a logical port for which you want to add a route and click **Route Management**. The **Route Management** dialog box is displayed.
- Choose **System** and click to switch to the rear view of the controller enclosure. Select the Ethernet port that you want to configure and click **Logical Port Management**. In the **Logical Port Management** dialog box that is displayed, select a logical port for which you want to add a route and click **Route Management**. The **Route Management** dialog box is displayed.

Step 3 Configure the route information for the logical port.



Route Management

IP Address: 192.168.100.11

Type	Destination Addr...	Subnet Mask	Gateway
Host route	192.168.100.12	255.255.255.255	192.168.100.1

1. In **IP Address**, select the IP address of the logical port.

2. Click **Add**.

   The **Add Route** dialog box is displayed.

   ⚠ **NOTICE**

   The default IP addresses of the internal heartbeat on the dual-controller storage system are **127.127.127.10** and **127.127.127.11**, and the default IP addresses of the internal heartbeat on the four-controller storage system are **127.127.127.10**, **127.127.127.11**, **127.127.127.12**, and **127.127.127.13**. Therefore, the IP address of the router cannot fall within the 127.127.127.XXX segment. Besides, the IP address of the gateway cannot be **127.127.127.10**, **127.127.127.11**, **127.127.127.12**, or **127.127.127.13**. Otherwise, routing will fail. (Internal heartbeat links are established between controllers for these controllers to detect each other's working status. You do not need to separately connect cables. In addition, internal heartbeat IP addresses have been assigned before delivery, and you cannot change these IP addresses).

3. In **Type**, select the type of the route to be added.

   Possible values of **Type** are **Default route**, **Host route**, and **Network segment route**.

4. Set **Destination Address**.

   - If **IP Address** is an IPv4 address, set **Destination Address** to the IPv4 address or network segment of the application server's service network port or that of the other storage system's logical port.
   - If **IP Address** is an IPv6 address, set **Destination Address** to the IPv6 address or network segment of the application server's service network port or that of the other storage system's logical port.

5. Set **Destination Mask** (IPv4) or **Prefix** (IPv6).

   - If a **Destination Mask** is set for an IPv4 address, this parameter specifies the subnet mask of the IP address for the service network port on the application server or storage device.
   - If a **Prefix** is set for an IPv6 address, this parameter specifies the prefix of the IPv6 address for application server's service network port or that of the other storage system's logical port.

6. In **Gateway**, enter the gateway of the local storage system's logical port IP address.

Step 4 Click **OK**. The route information is added to the route list.

The security alert dialog box is displayed.

Step 5 Confirm the information of the dialog box and select **I have read and understand the consequences associated with performing this operation.**.

Step 6 Click **OK**.

The **Success** dialog box is displayed indicating that the operation succeeded.

NOTE

To remove a route, select it and click **Remove**.

Step 7 Click **Close**.

----End

3.9.5.4 Enabling the FTP Service

Before creating an FTP share, check whether the FTP service has been enabled and whether parameters are correct.

Prerequisites

You have logged in to the DeviceManager as an administrator that has the permission to view the file system structure. The following administrators have the permission:

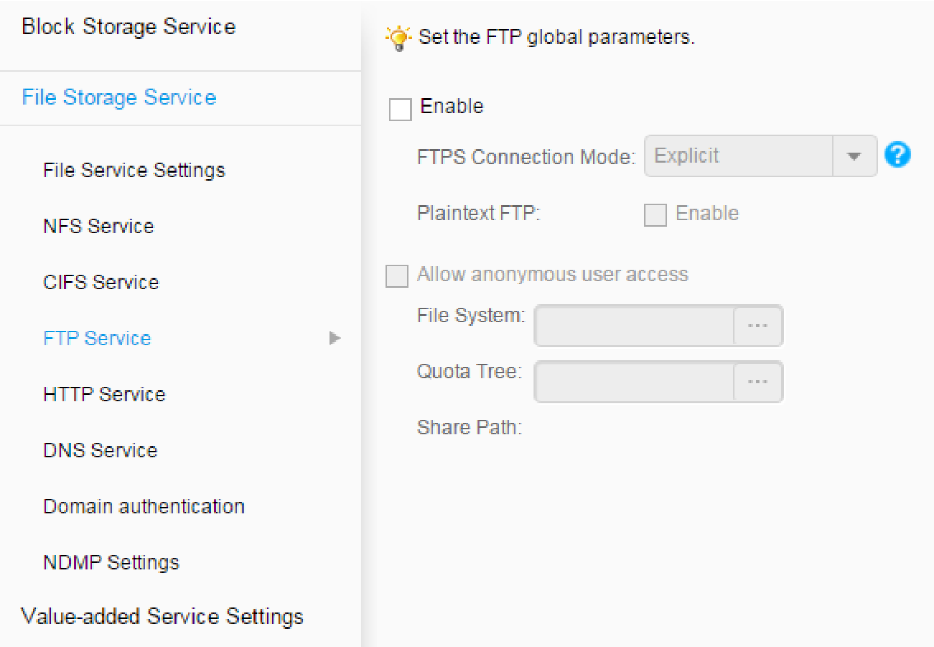
- Super administrator
- Administrator

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Settings** > **Storage Settings** > **File Storage Service** > **FTP Service**.

Step 3 Configure FTP service parameters. The related parameters are shown in **Table 3-73**.



Set the FTP global parameters.

□ Enable

FTPS Connection Mode: Explicit

Plaintext FTP: □ Enable

□ Allow anonymous user access

File System:

Quota Tree:

Share Path:

Table 3-73 FTP Parameters

Parameter	Description	Value
Enable	Whether to enable FTP sharing. After this function is enabled, you need to set **FTPS Connection Mode** and **Plaintext FTP**.	[Default value] Disabled [Example] Enable

Parameter	Description	Value
FTPS Connection Mode	File Transfer Protocol over SSL (FTPS) is an encrypted FTP protocol. It supports two transfer modes: ● Explicit: Port 21 is used for transferring by default. ● Implicit: Port 990 is used for transferring by default.	[Default value] Explicit [Example] Implicit
Plaintext FTP	Whether to enable the plaintext FTP that is not encrypted. After the plaintext FTP is enabled, there may be security risks.	[Default value] Disabled [Example] Enable
Allow anonymous user access	Whether anonymous users are allowed to access an FTP shared directory. After enabled, you must specify the shared directory, including file system and quota tree. **NOTE** The anonymous user has the permission restrictions below: ● Cannot upload file starting with **.**. ● No deleting or renaming file permission.	[Default value] Disabled [Example] Enable
File System	File system that is shared in FTP (mandatory).	[Example] FileSystem001
Quota Tree	Level-1 directory of a file system (optional).	[Example] Share
Share Path	The directory that the anonymous user can access. The path of such a directory consists of the **File System** and **Quota Tree**.	[Example] /FileSystem001/Share

Step 4 Click **Save**.

The **Warning** dialog box is displayed.

Step 5 Confirm the information in the dialog box and select **I have read and understand the consequences associated with performing this operation**, then click **OK**.

The **Success** dialog box is displayed.

Step 6 Click **OK** to finish configuring FTP service global parameters.

----End

3.9.5.5 Creating a Local Authentication User

This section describes how to create a local user. For applications that use local authentication, local user accounts are used to access a share. You can add a local user to a user group and access a share as the user group.

Procedure

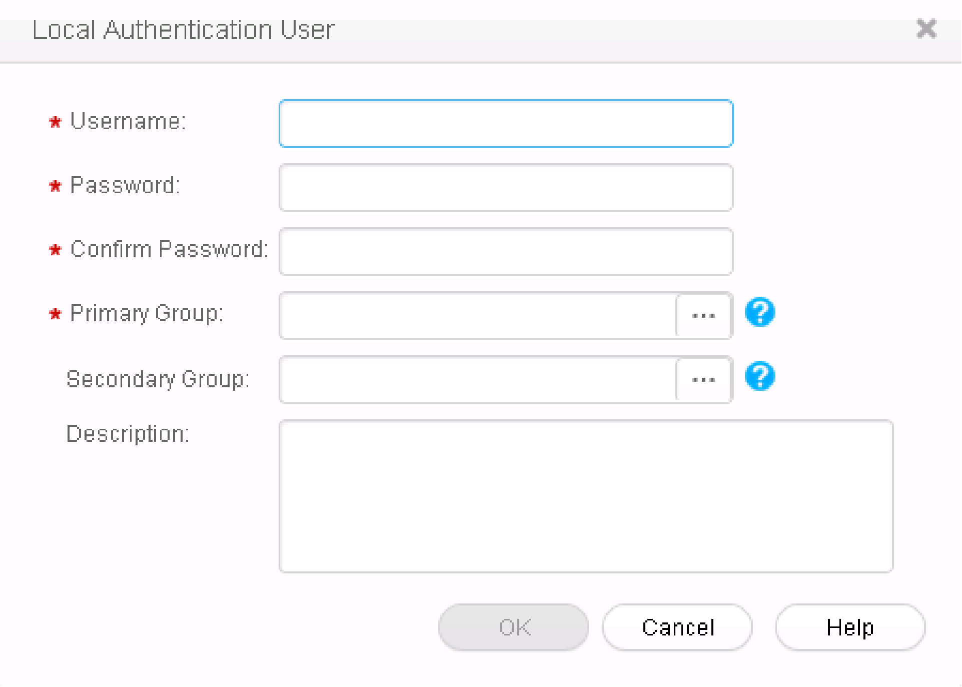
Step 1 Log in to DeviceManager.

Step 2 Choose **Provisioning** > **User Authentication**.

Step 3 Click **Local Authentication User** tab.

Step 4 Click **Create**.

The **Local Authentication User** dialog box is displayed.



Step 5 In **Username**, enter a new user name.

The user name:

- Cannot contain space, double quotation mark ("), slash (/), backslash (\), square brackets ([]), less than (<), larger than (>), plus (+), colon (:), semicolon (;), comma (,), question mark (?), asterisk (*), vertical bar (|), equal mark (=), (@), or end with a period (.).
- The user name can contain case-insensitive letters. Therefore, **aaaaaaaa** and **AAAAAAAA** cannot be created at the same time.
- The user name cannot be the same as the name of the local authentication user group.
- Contains 8 to 32 characters by default.

NOTE

You can modify the minimum length of user name in **More** > **Set Security Policies**.

Step 6 In **Password**, enter the password of the user.

The system default password requirements are:

- Contain 8 to 16 characters.
- Contain special characters. Special characters include: !"#$%&'()*+,-./:;<=>?@[\]^`{_|}~ and space.
- Contain any two types of the uppercase letters, lowercase letters, and digits.
- Cannot contain three consecutive same characters.
- Be different from the user name or the user name typed backwards.

NOTE

Click **More** and choose **Set Security Policies** to set a security policy for the password of the local authentication user in the file system. If **Password Validity Period (days)** is not selected, your password will never expire. For the security purpose, you are advised to select **Password Validity Period (days)** and set a validity period. The default validity period is 180 days. After the password expires, you cannot access shares, but you can set a password again and modify the password security policy.

Step 7 In **Confirm Password**, enter the new password again.

Step 8 Select **Primary Group**.

The **Select Primary Group** dialog box is displayed.

NOTE

The primary group to which users belong controls the users' permission for CIFS shares. A user must and can only belong to one primary group.

Step 9 Select the user group to which the user belongs to and click **OK**.

Step 10 (Optional) Select **Secondary Group**.

The **Select Secondary Group** dialog box is displayed.

NOTE

The concepts of primary group and secondary group are for local authentication users and have no relationship with each other. A local authentication user must belong to a primary group but not to a secondary group.

Step 11 Click **Add**.

The **Select User Group** dialog box is displayed.

Step 12 Select one or multiple groups which the user belongs to and click **OK**.

The system goes back to **Select Secondary Group** dialog box.

Step 13 Click **OK**.

The system goes back to **Local Authentication User** dialog box.

Step 14 **Optional:** In **Description** text box, enter the description for the local authentication user, for later management or search.

Step 15 Click **OK**.

Step 16 In the **Success** dialog box that is displayed, click **OK**.

----End

3.9.5.6 Creating an FTP Share

FTP enables file transfer between two hosts that run different operating systems and employ different file structures and character sets. After a directory is shared in FTP mode, FTP clients can access the directory.

Prerequisites

- You have logged in to the DeviceManager as an administrator that has the permission to view the file system structure. The following administrators have the permission:
  - Super administrator
  - Administrator
- A file system to be shared has been created.
- At least one local authentication user has been created.

Cautions

For the local authentication user whom the FTP share has been created for, you cannot create a new FTP share for this user. You can only modify the properties of FTP share of this user.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Provisioning** > **Share** > **FTP**.

Step 3 Click **Create**.

The **Create FTP Share Wizard** dialog box is displayed.

Step 4 In **File System**, select the file system you want to create FTP share.

NOTICE

If the selected file system is the secondary end of the remote replication or HyperVault, data in the file system is probably being modified when it is accessed. Before performing this operation, confirm that the application allows possible data inconsistency.

Step 5 **Optional:** In **Quota Tree**, select a quota tree you want to share.

NOTE

Quota tree is Level-1 directory under the root directory of the file system.

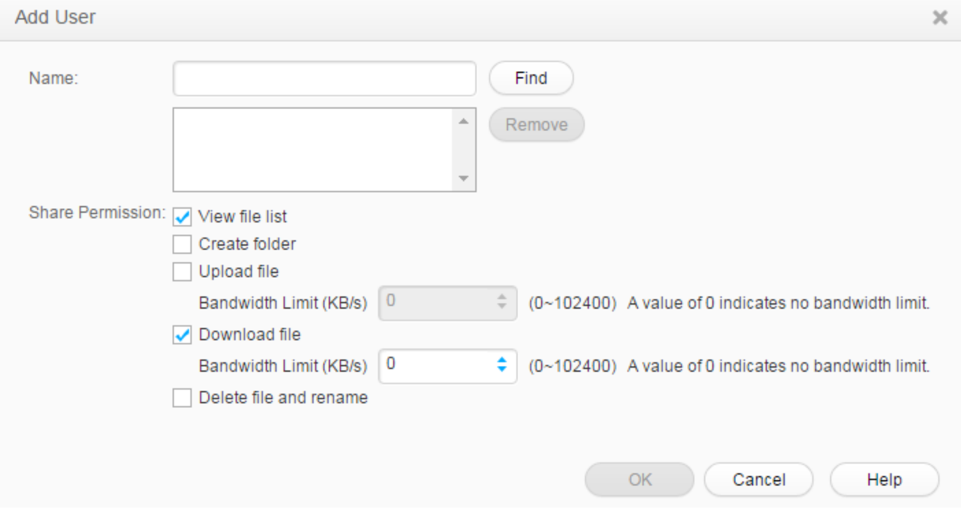
Step 6 **Optional:** In **Directory**, set the directory or subdirectory under the file system root directory.

NOTE

The share path consists of file system, quota tree and directory. The directory path cannot contain space, double quotation mark ("), backslash (\), square brackets ([]), less than (<), larger than (>), plus (+), colon (:), semicolon (;), comma (,), question mark (?), asterisk (*), vertical bar (|), equal mark (=), (@), and ('), or FTP share cannot be created.

Step 7 Click **Next**.

Step 8 On the **Set Permissions** page, set access permissions to the shared directory.



Name:

Share Permission:
☑ View file list
□ Create folder
□ Upload file
Bandwidth Limit (KB/s) 0 (0~102400) A value of 0 indicates no bandwidth limit.
☑ Download file
Bandwidth Limit (KB/s) 0 (0~102400) A value of 0 indicates no bandwidth limit.
□ Delete file and rename

1. Click **Add**.
2. In the **Name** text box, enter the criteria for searching for the users and click **Find**.
3. In the **Add User** dialog box that is displayed, select the users that you want to add and click **OK**.

   NOTE

   You can add multiple users at a time.
4. Go back to the **Add Users** dialog box. The newly added users are displayed on the page.
5. In **Share Permission**, set permissions for the users and click **OK**.

Table 3-74 Share Permissions

Parameter	Description	Value
Share permission	Permission of a new user. Possible values are: – View file list – Create folder – Upload file After this item is selected, the maximum upload speed (bandwidth) needs to be set for a single file. By default, the bandwidth is 0 KB/s. That is, the bandwidth is not limited. – Download file After this item is selected, the maximum download speed (bandwidth) needs to be set for a single file. By default, the bandwidth is 0 KB/s. That is, the bandwidth is not limited. – Delete file and rename	[Value range] – The upload speed (bandwidth) ranges from 0 to 102,400 (unit: KB/s). – The download speed (bandwidth) ranges from 0 to 102,400 (unit: KB/s). [Default value] – View file list – Download file

6. Go back to the **Set Permissions** page. The newly added users are included in the user list.

NOTE

– To modify user permissions, select the user whose permissions you want to modify from the user list and click **Modify**.

– To remove a user, select the user that you want to remove from the user list and click **Remove**.

Step 9 Click **Next**.

Step 10 On the **Summary** page, confirm the preceding information and click **Finish**.

Step 11 In the security alert dialog box, select **I have read and understand the consequences associated with performing this operation.** and click **OK**.

Step 12 On **Execution Result** page, click **Close**. Creating the FTP share is complete.

----End

3.9.5.7 Accessing FTP Shares

This section describes how to access FTP shares.

Accessing FTP Shares on a Windows-based Client

Step 1 Open the **Internet Explorer**.

Step 2 In the address box, enter **ftp://logical ip address**, where **logical ip address** indicates the logical port IP address of the storage system.

The system asks you to enter the user name and password.

NOTE

If the storage system allows access by anonymous users, anonymous users can directly log in to directories of anonymous users without entering their user names and passwords by default.

Step 3 Enter the user name and password that can be used to access the FTP shares.

----End

Accessing FTP Shares on a Linux/UNIX-based Client

Step 1 Enter **ftp logical ip address**, where **logical ip address** indicates the logical port IP address of the storage system.

The system asks you to enter the user name and password.

Step 2 Enter the user name and password that can be used to access the FTP shares.

NOTE

- When accessing the directory of an anonymous user, you need only to enter user name **anonymous** without entering the password.
- If many files or directories exist under a shared directory, ensure that the timeout parameter is correctly configured (set the parameter value to a large one or disable the parameter) on the client so that the ls command can be successfully executed.

For example, run an FTP command to access the FTP shares on the server whose IP address is **172.16.128.10**.

```
ldap-server:~ # ftp 172.16.128.10
Connected to 172.16.128.10.
220---------- Welcome to FTPd [privsep] ----------
220-You are user number 2 of 100 allowed.
220-Local time is now 16:16. Server port: 21.
220-IPv6 connections are also welcome on this server.
220 You will be disconnected after 10 minutes of inactivity.
Name (172.16.128.10:root): hlwuser1
331 User hlwuser1 OK. Password required
Password:
230-Your bandwidth usage is restricted
230-This server supports FXP transfers
230 OK. Current directory is /
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Extended Passive mode OK (|||30267|)
150 Accepted data connection
drwxrwxrwx    3 0          0                   5 Jan  7 16:36 .
drwxrwxrwx    3 0          0                   5 Jan  7 16:36 ..
-rw-rw----    1 100002     100000        4160064 Jan  7 16:36
FileZilla_3.3.2_win32-setup.exe
-rw-rw----    1 100002     100000             70 Jan  7 16:35 sdfdf.txt
drwxrwx---    3 100002     100000              3 Jan  7 16:34 testdir
226-Options: -a -l
226 5 matches total
```

----End

Accessing FTP Shares on an LFTP Client

LFTP is a file transmission client that supports multiple file transmission protocols including FTP, FTPS, SFTP,HTTP, and HTTPS.

NOTE

When the FTPS is accessed, you need to modify the configuration file **/etc/lftp.conf** of LTFP. Add **set ssl:verify-certificate no** at the end of the configuration file to close certificate verification.

Step 1 Run **lftp** *-u username,password ip_address*. **username** and **password** is the actual user name and password used to log in to **ip_address** of the FTP server.

Step 2 Run the **ls** command to check the remote file list.

For example, access the FTP shares on the server whose IP address is **192.168.1.11**.

```
linux-11215:~ # lftp -u user_ftp01,Admin@123 192.168.1.11
lftp user_ftp01@192.168.1.11:~> ls
drwxrwxrwx   2 root root           3 May 19 10:29 .
drwxrwxrwx   2 root root           3 May 19 10:29 ..
-rw-rw----   1 lyr_ftp01 default_group          0 Apr 18 16:20 ftp_01.txt
```

----End

Accessing FTP Shares over FTPS

Currently, you can only access FTP shares over FTPS using related tool software. The following describes how to access FTP shares over FTPS using **FileZilla** software as an example.

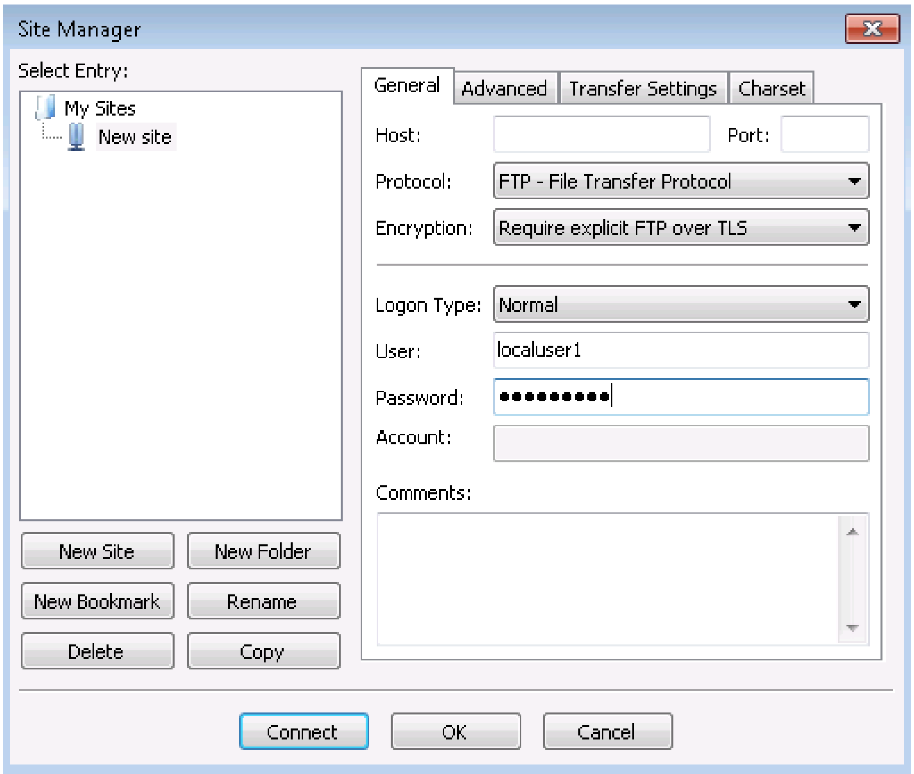
Step 1 Open the **FileZilla** client software.

Step 2 Choose **File** > **Site Manager**.

Site Manager is displayed.

Step 3 Click **New Site** to create a site.

Step 4 On the **General** tab page, type configuration information of storage system's FTP shares.



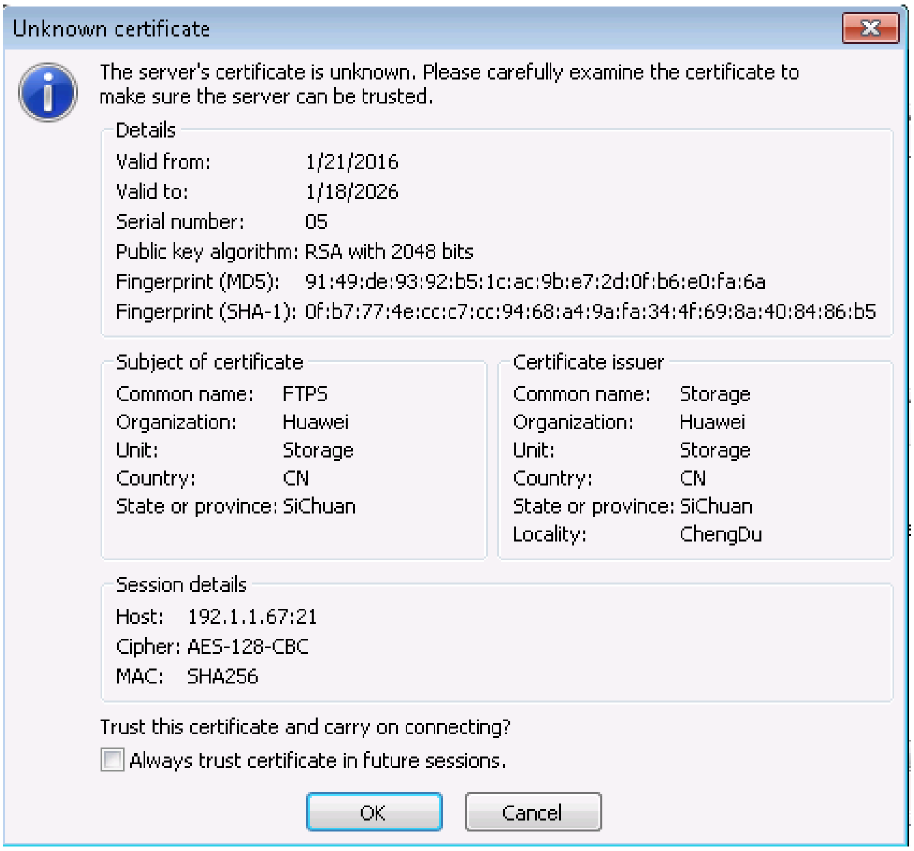
Host:
Port:
Protocol: FTP - File Transfer Protocol
Encryption: Require explicit FTP over TLS
Logon Type: Normal
User: localuser1
Password: ●●●●●●●●●
Account:
Comments:

Where:

- **Host** indicates the IP address of a logical port for FTP sharing.
- **Port** indicates the default port.
- **Protocol** indicates the used protocol type. Select **FTP - File Transfer Protocol** if you use FTPS.
- **Encryption** indicates the encryption mode. The value that you select must be consistent with that set in **FTPS Connection Mode**. If **FTPS Connection Mode** is **Show**, select **Require explicit FTP over TLS**. If **FTPS Connection Mode** is **Hide**, select **Require implicit FTP over TLS**.
- **Logon Type** indicates the login mode. Select **Normal** here.
- **User** indicates the name of a user account used to access FTP shares.
- **Password** indicates the password used to access FTP shares.

Step 5 Click **Connect** to connect to the FTP server.

If you use the default certificate, a certificate warning message is displayed.



The server's certificate is unknown. Please carefully examine the certificate to make sure the server can be trusted.

Details

Valid from: 1/21/2016
Valid to: 1/18/2026
Serial number: 05
Public key algorithm: RSA with 2048 bits
Fingerprint (MD5): 91:49:de:93:92:b5:1c:ac:9b:e7:2d:0f:b6:e0:fa:6a
Fingerprint (SHA-1): 0f:b7:77:4e:cc:c7:cc:94:68:a4:9a:fa:34:4f:69:8a:40:84:86:b5

Subject of certificate

Common name: FTPS
Organization: Huawei
Unit: Storage
Country: CN
State or province: SiChuan

Certificate issuer

Common name: Storage
Organization: Huawei
Unit: Storage
Country: CN
State or province: SiChuan
Locality: ChengDu

Session details

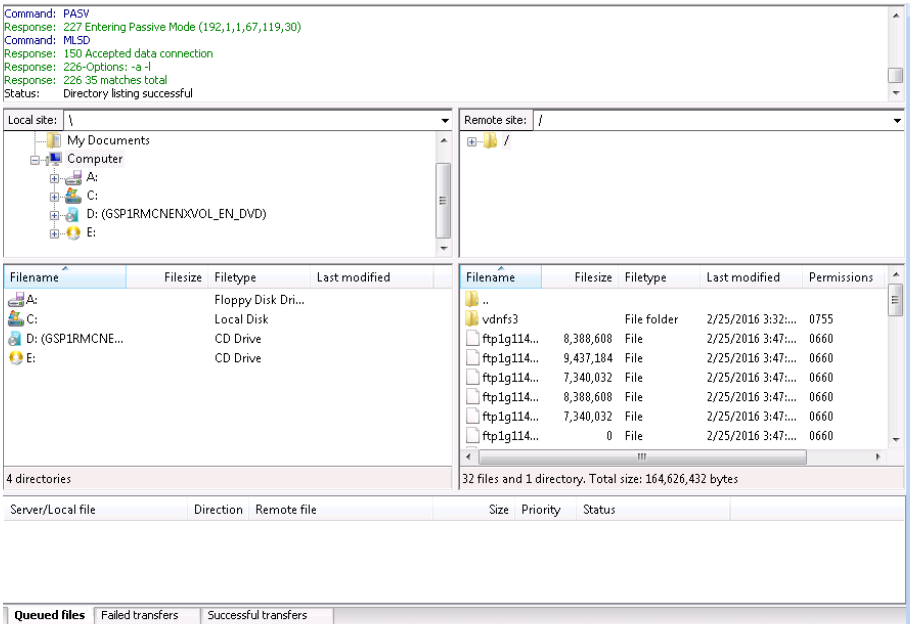
Host: 192.1.1.67:21
Cipher: AES-128-CBC
MAC: SHA256

Trust this certificate and carry on connecting?

☐ Always trust certificate in future sessions.

Step 6 **Optional:** Click **OK** to ensure the certificate information.

Step 7 Go to the page of FTP shares.



```
Command:  PASV
Response: 227 Entering Passive Mode (192,1,1,67,119,30)
Command:  MLSD
Response: 150 Accepted data connection
Response: 226-Options: -a -l
Response: 226 35 matches total
Status:   Directory listing successful
```

Local site: \

- My Documents
- Computer
  - A:
  - C:
  - D: (GSP1RMCNENXVOL_EN_DVD)
  - E:

Remote site: /

- /

Filename	Filesize	Filetype	Last modified
A:		Floppy Disk Dri...	
C:		Local Disk	
D: (GSP1RMCNE...		CD Drive	
E:		CD Drive	

4 directories

Filename	Filesize	Filetype	Last modified	Permissions
..				
vdnfs3		File folder	2/25/2016 3:32:...	0755
ftp1g114...	8,388,608	File	2/25/2016 3:47:...	0660
ftp1g114...	9,437,184	File	2/25/2016 3:47:...	0660
ftp1g114...	7,340,032	File	2/25/2016 3:47:...	0660
ftp1g114...	8,388,608	File	2/25/2016 3:47:...	0660
ftp1g114...	7,340,032	File	2/25/2016 3:47:...	0660
ftp1g114...	0	File	2/25/2016 3:47:...	0660

32 files and 1 directory. Total size: 164,626,432 bytes

Server/Local file	Direction	Remote file	Size	Priority	Status

----End

Follow-up Procedure

- If the information about a local authentication user or domain user is changed (for example, the user is forbiddened, the password is changed or expires, the relationship is changed, or the user is deleted) when a client accesses the file system of FTP shares, the changed information will take effect after authentication is passed in the next time (by mounting shares again).
- Newly modified FTP configuration parameters need several seconds to take effect in all controllers. During that period, your client may not be able to access other controllers. In such a case, wait a few seconds and use your client to retry connections.

3.9.6 Configuring an HTTP Share

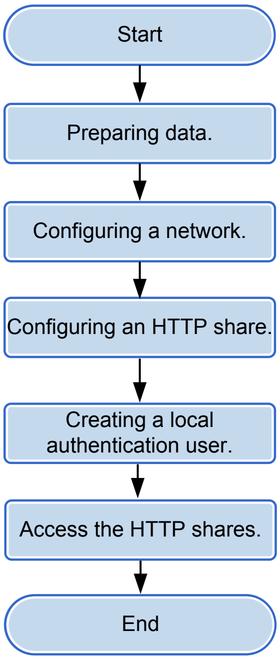
Storage system supports the HTTP share file system. After enabling the HTTP service, you can share a file system in HTTP share mode. After enabling the **DAV** function, you can manage contents in a shared file system.

3.9.6.1 Configuration Process

This section describes the HTTP share configuration process.

Figure 3-31 shows the HTTP share configuration process.

Figure 3-31 HTTP share configuration process



3.9.6.2 Preparing Data

Before configuring an HTTP share, obtain information about storage system IP addresses, shared file systems, and local authentication users to assist in the follow-up configuration.

Table 3-75 describes preparations required for configuring an HTTP share.

Table 3-75 Preparations required for configuring an HTTP share

Item	Description	Example
IP address of the storage system *Indicates the service IP address used by a storage system.*	Storage system can provide HTTP share for the client by using the Ethernet port or the Logical port.	Logical IP address 172.16.128.10
File system *Indicates a file system for which an HTTP share is configured.*	Storage system enables you to configure a file system as an HTTP share.	FileSystem001

Item	Description	Example
User *Indicates a user that accesses an HTTP share. Storage systems employ local authentication users to enable clients to access HTTP shares.*	The user name: ● Must contain 8 to 32 characters by default. ● Cannot contain space, double quotation mark ("), slash (/), backslash (\), square brackets ([]), larger than (<), less than (>), plus (+), colon (:), semicolon (;), comma (,), question mark (?), asterisk (*), vertical bar (|), equal mark (=), (@), or end with a period (.). **NOTE** You cannot use the user accounts retained in the system, including: ● User accounts retained in Windows: **Everyone**, **Local**, **Creator Owner**, **Creator Group**, **Creator Owner Server**, **Creator Group Server**, **Owner Rights**, **Group Rights**, **NT Pseudo Domain**, **Dialup**, **Network**, **Batch**, **Interactive**, **Service**, **Anonymous Logon**, **Proxy**, **Enterprise Domain Controllers**, **Self**, **Authenticated Users**, **Restricted**, **Terminal Server User**, **Remote Interactive Logon**, **This Organization**, **System**, **Local Service**, **Network Service**, **Write Restricted**, **Other Organization**, **Builtin**, **Internet$**, **Members can fully administer the computer/domain**, **Users**, **Guests**, **Power Users**, **Members can share directories**, **Account Operators**, **Server Operators**, **Print Operators**, **Backup Operators**, **Members can bypass file security to back up files**, **Replicator**, **Current Owner**, **Current Group**. ● User accounts retained in Linux: **root**, **nogroup**, **nobody**, **ftp**, **anonymous**, **daemon**, **nobody**, **news**, **sshd**, **messagebus**. ● User accounts retained in a storage system: **ibc_os_hs**.	user1

Item	Description	Example
User group *User group that employs local authentication.*	The user group name: ● Must contain 1 to 32 characters. ● Cannot contain space, double quotation mark ("), slash (/), backslash (\), square brackets ([]), larger than (<), less than (>), plus (+), colon (:), semicolon (;), comma (,), question mark (?), asterisk (*), vertical bar (|), equal mark (=), (@), or end with a period (.). **NOTE** You cannot use the user accounts retained in the system, including: ● User accounts retained in Windows: **Everyone**, **Local**, **Creator Owner**, **Creator Group**, **Creator Owner Server**, **Creator Group Server**, **Owner Rights**, **Group Rights**, **NT Pseudo Domain**, **Dialup**, **Network**, **Batch**, **Interactive**, **Service**, **Anonymous Logon**, **Proxy**, **Enterprise Domain Controllers**, **Self**, **Authenticated Users**, **Restricted**, **Terminal Server User**, **Remote Interactive Logon**, **This Organization**, **System**, **Local Service**, **Network Service**, **Write Restricted**, **Other Organization**, **Builtin**, **Internet$**, **Members can fully administer the computer/domain**, **Users**, **Guests**, **Power Users**, **Members can share directories**, **Account Operators**, **Server Operators**, **Print Operators**, **Backup Operators**, **Members can bypass file security to back up files**, **Replicator**, **Current Owner**, **Current Group**. ● User accounts retained in Linux: **root**, **nogroup**, **nobody**, **ftp**, **anonymous**, **bin**, **daemon**, **sys**, **tty**, **disk**, **lp**, **www**, **kmem**, **wheel**, **mail**, **news**, **uucp**, **shadow**, **dialout**, **audio**, **floppy**, **cdrom**, **console**, **utmp**, **public**, **video**, , **games**, **xok**, **trusted**, **modem**, **man**, **users**, **nobody**, **nogroup**, **sshd**, **postfix**, **maildrop**. ● User accounts retained in a storage system: **ibc_os_hs**.	default_group
DAV *DAV can be used to manage HTTP share contents.*	-	Enable

3.9.6.3 Configuring a Network

This section describes how to use DeviceManager to configure a logical IP address for a storage system. The logical IP address is used for accessing shares.

3.9.6.3.1 (Optional) Configuring DNS-based Load Balancing Parameters (Applicable to V300R006C10 and Later Versions)

Storage arrays' DNS-based load balancing feature can detect the IP address load on the arrays in real time and use a proper IP address as the DNS response to achieve load balancing among IP addresses. This section describes how to configure DNS-based load balancing and DNS zones.

Context

Working principle:

1. When a host accesses the NAS service of a storage array using the domain name, the host first sends a DNS request to the built-in DNS server of the storage array and the DNS server obtains the IP address according to the domain name.
2. When a domain name contains multiple IP addresses, the storage array selects the IP address with a light load as the DNS response based on the configured load balancing policy and returns the DNS response to the host.
3. After receiving the DNS response, the host sends a service request to the destination IP address.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Settings** > **Storage Settings** > **File Storage Service** > **DNS-based Load Balancing**.

Step 3 Table 3-76 lists parameters related to DNS-based load balancing.

Table 3-76 DNS-based load balancing parameters

Parameter	Description	Value
DNS-based Load Balancing	Enables or disables DNS-based load balancing. **NOTE** ● When enabling the DNS-based load balancing function, you are advised to disable the global namespace forwarding function. This function affects DNS-based load balancing. ● After the DNS-based load balancing function is disabled, the domain name resolution service is unavailable and file systems cannot use the function. ● This parameter can be set only in the system view, not in the vStore view. The setting takes effect for the entire storage system.	[Example] Enable

Parameter	Description	Value
Load Balancing Policy	This parameter enables you to configure DNS-based load balancing policies. A storage system supports the following load balancing policies: ● Weighted round robin: When a client uses a domain name to initiate an access request, the storage system calculates the weight based on the performance data. Under the same domain name, IP addresses that are required to process loads have the same probability to be selected to process client services. ● CPU usage: When a client uses a domain name to initiate an access request, the storage system calculates the weight based on the CPU usage of each node. Using the weight as the probability reference, the storage system selects a node to process the client's service request. ● Bandwidth usage: When a client uses a domain name to initiate an access request, the storage system calculates the weight based on the total bandwidth usage of each node. Using the weight as the probability reference, the storage system selects a node to process the client's service request. ● Open connections: When a client uses a domain name to initiate an access request, the storage system calculates the weight based on the NAS connections of each node. Using the weight as the probability reference, the storage system selects a node to process the client's service request. ● Overall load: When a client uses a domain name to initiate an access request, the storage system selects a node to process the client's service request based on the comprehensive load. The comprehensive node load is calculated based on the CPU usage, bandwidth usage, and number of NAS connections. Less	[Example] Weighted round robin

Parameter	Description	Value
	loaded nodes are more likely to be selected. NOTE This parameter can be set only in the system view, not in the vStore view. The setting takes effect for the entire storage system.	

Step 4 Configure a DNS zone.

A DNS zone contains IP addresses of a group of logical ports. A host can use the name of a DNS zone to access shared services provided by a storage system. Services can be evenly distributed to logical ports.

NOTE

Only the logical ports whose **Role** is **Service** or **Management+Service** can be added into a DNS zone. The logical ports whose **Role** is **Management** cannot be added in to a DNS zone.

1. Add a DNS zone.
   a. Click **Add**.
   b. The **Add DNS Zone** dialog box is displayed. In **Domain Name**, type the domain name of the DNS zone you want to add and click **OK**.

      NOTE

      The domain name complexity requirements are as follows:

      - A domain name contains 1 to 255 characters and consists of multiple labels separated by periods (**.**).
      - A label contains 1 to 63 characters including letters, digits, hyphens (-), and underscores (_), and must start and end with a letter or a digit.
      - The domain name must be unique.
2. Remove a DNS zone.
   a. In the DNS zones that are displayed, select a DNS zone you want to remove.
   b. Click **Remove**.
3. Modify a DNS zone.
   a. In the DNS zones that are displayed, select a DNS zone you want to modify.
   b. Click **Modify**.
   c. The <**Modify DNS Zone** dialog box is displayed. In **Domain Name**, type the domain name of the DNS zone you want to modify and click **OK**.
4. View a DNS zone.
   a. In **DNS Zone**, type a keyword and click **Search**.
   b. In **DNS Zone**, the DNS zone names relevant to the keyword will be displayed.

      NOTE

      You can select a DNS zone to modify or remove it.

Step 5 Click **Save**. The **Warning** dialog box is displayed.

Step 6 Confirm the information in the dialog box and select **I have read and understand the consequences associated with performing this operation**.

Step 7 Click **OK**. The **Execution Result** page is displayed.

Step 8 On the **Execution Result** page, confirm the modification and click **Close**. The DNS zone configuration is complete.

----End

Follow-up Procedure

Choose **Provisioning** > **Port** > **Logical Ports** to configure **Listen DNS Query Request** and **DNS Zone** information for logical ports.

3.9.6.3.2 Creating a Logical Port

This operation enables you to create a logical port for managing and accessing file based on Ethernet ports, bond ports, or VLANs.

Precautions

The number of logical ports created for each controller is recommended not more than 64. If the number exceeds 64 and a large number of ports do not work properly, logical ports drift towards the small number of ports available. As a result, service performance deteriorates.

Procedure

Step 1 Log in to DeviceManager.

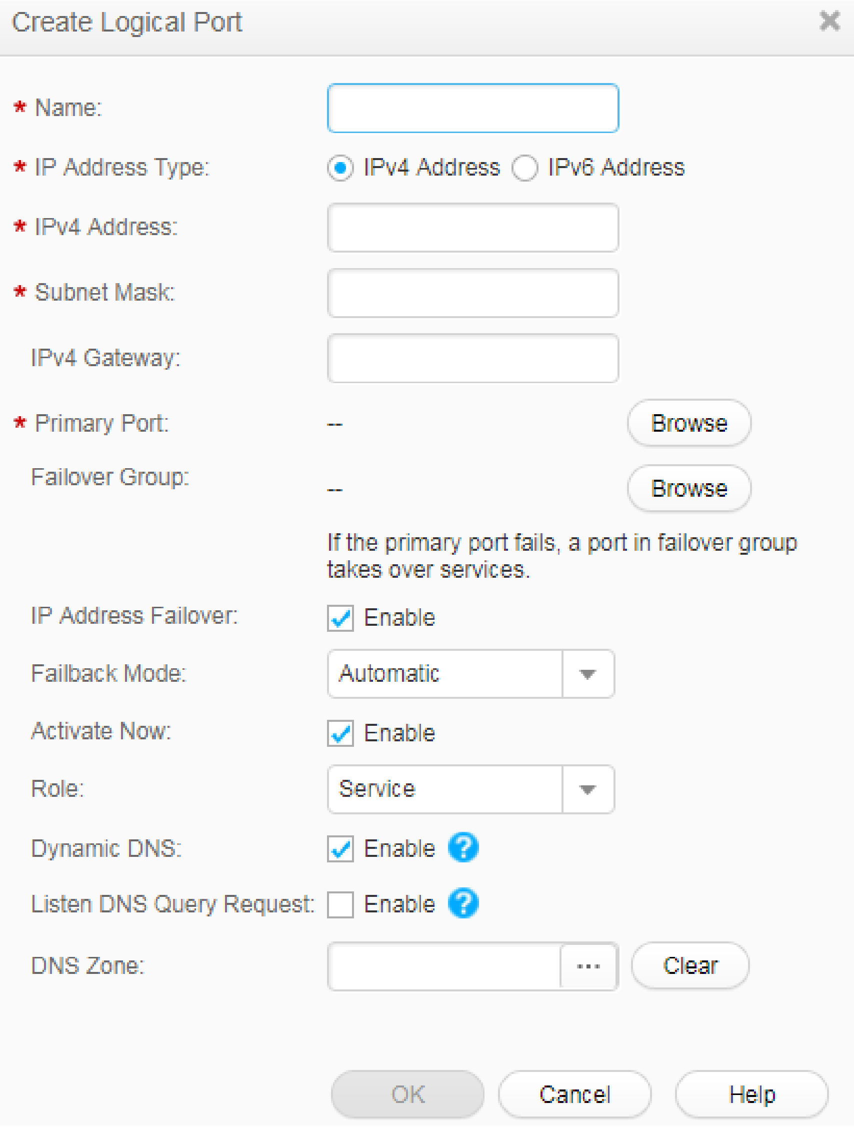
Step 2 Choose **Provisioning** > **Port** > **Logical Ports**.

Step 3 Click **Create**.

The **Create Logical Port** dialog box is displayed.

Step 4 In the **Create Logical Port** dialog box, configure related parameters.

Table 3-77 describes related parameters.



Create Logical Port

* Name:

* IP Address Type: ● IPv4 Address ○ IPv6 Address

* IPv4 Address:

* Subnet Mask:

IPv4 Gateway:

* Primary Port: -- Browse

Failover Group: -- Browse

If the primary port fails, a port in failover group takes over services.

IP Address Failover: ☑ Enable

Failback Mode: Automatic

Activate Now: ☑ Enable

Role: Service

Dynamic DNS: ☑ Enable

Listen DNS Query Request: □ Enable

DNS Zone: ... Clear

Table 3-77 Logical port parameters

Parameter	Description	Value
Name	Name of the logical port. The name must meet the following requirements so that the logical port is available to compatible applications: ● The name must be unique. ● The name can contain only letters, digits, underscores (_), periods (.), and hyphens (-). ● The name contains 1 to 31 characters.	[Example] lif01
IP Address Type	IP address type of the logical port, including IPv4 or IPv6.	[Example] IPv4
IPv4 Address	IPv4 address of the logical port.	[Example] 192.168.100.11
Subnet Mask	IPv4 subnet mask of the logical port.	[Example] 255.255.0.0
IPv4 Gateway	IPv4 gateway of the logical port.	[Example] 192.168.100.1
IPv6 Address	IPv6 address of the logical port.	[Example] fc00::1234
Prefix	IPv6 prefix length of the logical port.	[Example] 64
IPv6 Gateway	IPv6 gateway of the logical port.	[Example] fc00::1
Primary Port	Port to which the logical port belongs, including the Ethernet port, Bond port, and VLAN.	[Example] None

Parameter	Description	Value
Failover Group	Failover group name. **NOTE** ● If a failover group is specified, services on the failed primary port will be taken over by a port in the specified failover group. ● If no failover group is specified, services on the failed primary port will be taken over by a port in the default failover group.	[Example] None
IP Address Failover	After IP address failover is enabled, services are failed over to other normal ports within the failover group if the primary port fails. However, the IP address used by services remains unchanged. **NOTE** Shares of file systems do not support the multipathing mode. IP address failover is used to improve reliability of links.	[Example] Enable
Failback Mode	Mode in which services fail back to the primary port after the primary port is recovered. The mode can be manual or automatic. **NOTE** ● If **Failback Mode** is **Manual**, ensure that the link to the primary port is normal before the failback. Services will manually fail back to the primary port only when the link to the primary port keeps normal for over five minutes. ● If **Failback Mode** is **Automatic**, ensure that the link to the primary port is normal before the failback. Services will auto fail back to the primary port only when the link to the primary port keeps normal for over five minutes.	[Example] Automatic

Parameter	Description	Value
Activate Now	To activate the logical port immediately.	[Example] Enable
Role	Roles of logical ports include the following: ● Management: The port is used by a super administrator to log in to the system for management. ● Service: The port is used by a super administrator to access services such as file system CIFS shares. ● Management+Service: The port is used by a super administrator to log in to the system to manage the system and access services.	[Example] Service
Dynamic DNS	When the dynamic DNS is enabled, the DNS server will automatically and periodically update the IP address configured for the logical port.	[Example] Enable
Listen DNS Query Request	After this function is enabled, external NEs can access the DNS service provided by the storage system by using the IP address of this logical port.	[Example] Enable

Parameter	Description	Value
DNS Zone	Name of a DNS zone. **NOTE** ● If the value is blank, the logical port is not used for DNS-based load balancing. ● Only the logical ports whose **Role** is **Service** or **Management+Service** can be added into a DNS zone. The logical ports whose **Role** is **Management** cannot be added in to a DNS zone. ● One logical port can be associated with only one DNS zone. One DNS zone can be associated with multiple logical ports. ● A DNS zone can be associated with both IPv4 and IPv6 logical ports. ● The load balancing effect varies with the distribution of logical ports associated with a DNS zone. To obtain a better load balancing effect, ensure that logical ports associated with a DNS zone are evenly distributed among controllers.	[Example] None

Step 5 Click **OK**.

The **Success** dialog box is displayed indicating that the logical port has been successfully created.

Step 6 Click **OK**.

----End

3.9.6.3.3 (Optional) Creating a Bond Port

This section describes how to bond Ethernet ports on a same controller.

Prerequisites

Ethernet ports that have IP addresses cannot be bound. The IP addresses of the bonded host ports need to be cleared before bonding.

Context

- Port bonding provides more bandwidth and redundancy for links. Although ports are bonded, each host still transmits data through a single port and the total bandwidth can

be increased only when there are multiple hosts. Determine whether to bond ports based on site requirements.

- The port bond mode of a storage system has the following restrictions:
  - On the same controller, a bond port is formed by a maximum of eight Ethernet ports.
  - Only the interface modules with the same port rate (GE or 10GE) can be bonded.
  - The port cannot be bonded across controllers. Non-Ethernet network ports cannot be bonded.
  - SmartIO interface modules cannot be bonded if they work in cluster or FC mode or run FCoE service in FCoE/iSCSI mode.
  - Read-only users are unable to bind Ethernet ports.
  - Each port only allows to be added to one bonded port. It cannot be added to multiple bonded ports.
  - Ports are bonded to create a bond port that cannot be added to the port group.
- After Ethernet ports are bonded, **MTU** changes to the default value and you must set the link aggregation mode for the ports. For example, on Huawei switches, you must set the ports to the static LACP mode.

  NOTE

  The detailed link aggregation mode varies with the switches' manufacturer.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Provisioning** > **Port** > **Bond Ports**.

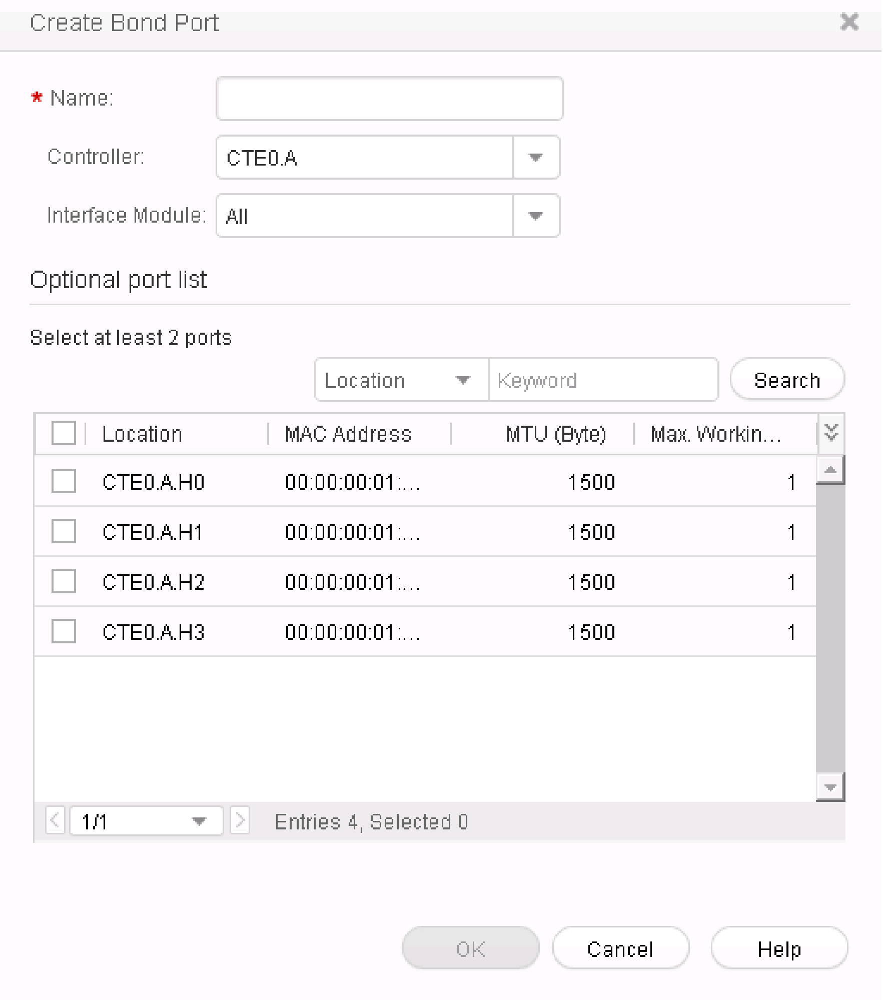
Step 3 Click **Create**.

The **Create Bond Port** dialog box is displayed.

NOTE

The port name format is **controller enclosure ID.interface module ID.port ID**.

Step 4 Set the name, interface module, and optional ports that can be bonded with the current Ethernet port.



* Name:

Controller: CTE0.A

Interface Module: All

Optional port list

Select at least 2 ports

□	Location	MAC Address	MTU (Byte)	Max. Workin...
□	CTE0.A.H0	00:00:00:01:...	1500	1
□	CTE0.A.H1	00:00:00:01:...	1500	1
□	CTE0.A.H2	00:00:00:01:...	1500	1
□	CTE0.A.H3	00:00:00:01:...	1500	1

1/1 Entries 4, Selected 0

1. In **Name**, enter a name for the bond port.

   The name:

   - Contains only letters, digits, underscores (_), periods (.), and hyphens (-).
   - Contains 1 to 31 characters.
2. From the **Controller**, select the controller the Ethernet ports own to.
3. Select the **Interface Module**.
4. From the **Optional port list**, select the Ethernet ports you want to bond.

   NOTE

   Select at least two ports.
5. Click **OK**.

   The security alert dialog box is displayed.

Step 5 Confirm that you want to bond these Ethernet ports.

1. Confirm the information of the dialog box and select **I have read and understand the consequences associated with performing this operation.**.
2. Click **OK**.

   The **Success** dialog box is displayed indicating that the operation succeeded.
3. Click **OK**.

----End

3.9.6.3.4 (Optional) Managing a Route of Logical Port

You need to configure a route when the HTTP server and the storage system are not on the same network. If the HTTP server and logical IP addresses cannot ping each other, add a route from the logical IP addresses to the network segment of the HTTP server.

Prerequisites

The logical port has been assigned an IP address.

Procedure

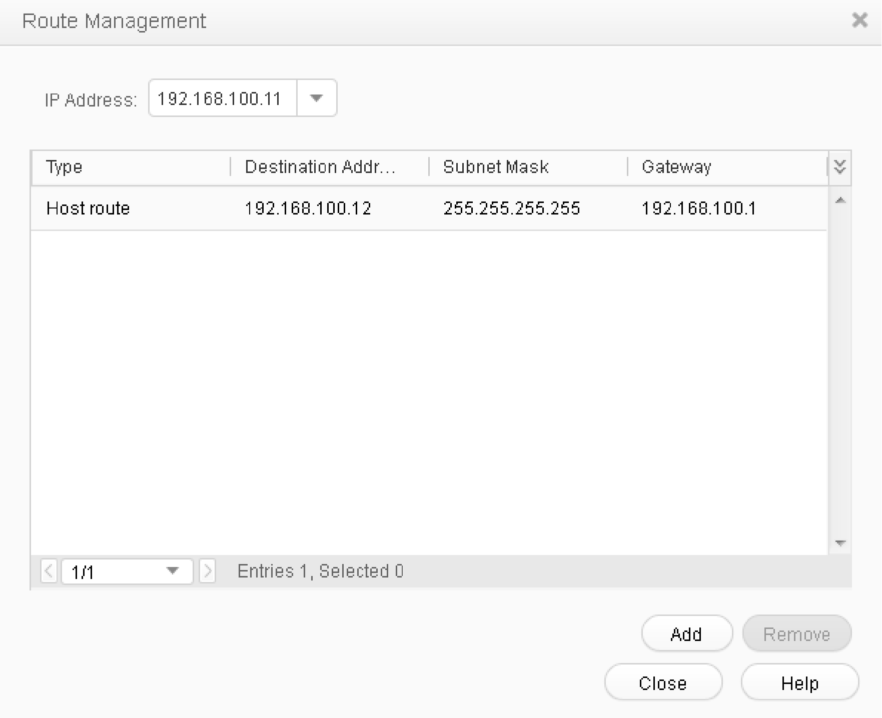
Step 1 Log in to DeviceManager.

Step 2 Go to the route management page.

You can go to the route management page by using either of the following methods:

- Choose **Provisioning** > **Port** > **Logical Ports**. Select a logical port for which you want to add a route and click **Route Management**. The **Route Management** dialog box is displayed.
- Choose **System** and click to switch to the rear view of the controller enclosure. Select the Ethernet port that you want to configure and click **Logical Port Management**. In the **Logical Port Management** dialog box that is displayed, select a logical port for which you want to add a route and click **Route Management**. The **Route Management** dialog box is displayed.

Step 3 Configure the route information for the logical port.



Route Management

IP Address: 192.168.100.11

Type	Destination Addr...	Subnet Mask	Gateway
Host route	192.168.100.12	255.255.255.255	192.168.100.1

1/1 Entries 1, Selected 0

1. In **IP Address**, select the IP address of the logical port.

2. Click **Add**.

   The **Add Route** dialog box is displayed.

   NOTICE

   The default IP addresses of the internal heartbeat on the dual-controller storage system are **127.127.127.10** and **127.127.127.11**, and the default IP addresses of the internal heartbeat on the four-controller storage system are **127.127.127.10**, **127.127.127.11**, **127.127.127.12**, and **127.127.127.13**. Therefore, the IP address of the router cannot fall within the 127.127.127.XXX segment. Besides, the IP address of the gateway cannot be **127.127.127.10**, **127.127.127.11**, **127.127.127.12**, or **127.127.127.13**. Otherwise, routing will fail. (Internal heartbeat links are established between controllers for these controllers to detect each other's working status. You do not need to separately connect cables. In addition, internal heartbeat IP addresses have been assigned before delivery, and you cannot change these IP addresses).

3. In **Type**, select the type of the route to be added.

   Possible values of **Type** are **Default route**, **Host route**, and **Network segment route**.

4. Set **Destination Address**.
   - If **IP Address** is an IPv4 address, set **Destination Address** to the IPv4 address or network segment of the application server's service network port or that of the other storage system's logical port.
   - If **IP Address** is an IPv6 address, set **Destination Address** to the IPv6 address or network segment of the application server's service network port or that of the other storage system's logical port.

5. Set **Destination Mask** (IPv4) or **Prefix** (IPv6).
   - If a **Destination Mask** is set for an IPv4 address, this parameter specifies the subnet mask of the IP address for the service network port on the application server or storage device.
   - If a **Prefix** is set for an IPv6 address, this parameter specifies the prefix of the IPv6 address for application server's service network port or that of the other storage system's logical port.

6. In **Gateway**, enter the gateway of the local storage system's logical port IP address.

Step 4 Click **OK**. The route information is added to the route list.

The security alert dialog box is displayed.

Step 5 Confirm the information of the dialog box and select **I have read and understand the consequences associated with performing this operation.**.

Step 6 Click **OK**.

The **Success** dialog box is displayed indicating that the operation succeeded.

NOTE

To remove a route, select it and click **Remove**.

Step 7 Click **Close**.

----End

3.9.6.4 Creating an HTTP Share

Hypertext Transfer Protocol (HTTP) is an application layer protocol oriented to objects. This chapter guides administrators through folder sharing over HTTP in the shared file system.

Prerequisites

Before using the web to access HTTP shares, run the **change service http enable_auto_index=yes** command on the CLI to open the directory list; otherwise, you cannot use the web to access HTTP shares.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose ⚙ **Settings** > **Storage Settings** > **File Storage Service** > **HTTP Service**.

Step 3 Configure the HTTP service parameters. The related parameters are shown in **Table 3-78**.

Table 3-78 HTTP Parameters

Parameter	Description	Setting
HTTP Service	Global control over the enable and disable status of the HTTP sharing service. If this parameter is set to disable, all the other parameter configurations become invalid. NOTE ● By default, the storage system provides the HTTPS service certificate. You are advised to replace the certificate with the private certificate before accessing HTTPS shares. After the certificate is replaced, the CA certificate of the storage system must be imported for the browser to eliminate security alarms. As the service IP address is used to access the HTTPS service, alarm **This website's address does not match the address in the security certificate** cannot be cleared. ● When the HTTP service is disabled, the system automatically deletes information about shared file systems and directories. When the HTTP service is enabled again, configure the HTTP shared file systems and directories.	[Example] Enable
Max. Number of Connections	Maximum number of HTTP share connections allowed by the system. NOTE The maximum number of connections varies depending on the device model.	[Value range] 1 to 256

Parameter	Description	Setting
HTTP Default Port	Only the HTTPS port is enabled for the storage system when the HTTP service is enabled. To enable the HTTP port, select **Enable**. **NOTE** Exercise caution when enabling the HTTP port.	[Example] Enable
File System	File system that you want to share over HTTP.	[Example] FileSystem001
Directory	Directory under the file system selected that you want to share over HTTP.	[Example] test/
Share Path	Directory that you want to share over HTTP. This parameter contains **File System** and **Directory**. **NOTE** ● The share path cannot contain space, double quotation mark ("), backslash (\), square brackets ([]), less than (<), larger than (>), plus (+), colon (:), semicolon (;), comma (,), question mark (?), asterisk (*), vertical bar (|), equal mark (=), (@), and ('), or HTTP share cannot be created. ● A share path consists of 1 to 4000 characters.	[Example] File System test_001
DAV	DAV, also known as WebDAV (Web-based Distributed Authoring and Versioning), is a communication protocol based on HTTP. Once WebDAV enabled, the system allows the DAV client to read/write the shared directory, and supports file locking, file unlocking, and file version control. **NOTE** After enabling WebDAV, resource users may have full control permissions of the HTTP sharing root directories.	[Example] Enable

Step 4 Click **Save**. The HTTP sharing service is configured.

----End

3.9.6.5 Creating a Local Authentication User

This section describes how to create a local user. For applications that use local authentication, local user accounts are used to access a share. You can add a local user to a user group and access a share as the user group.

Procedure

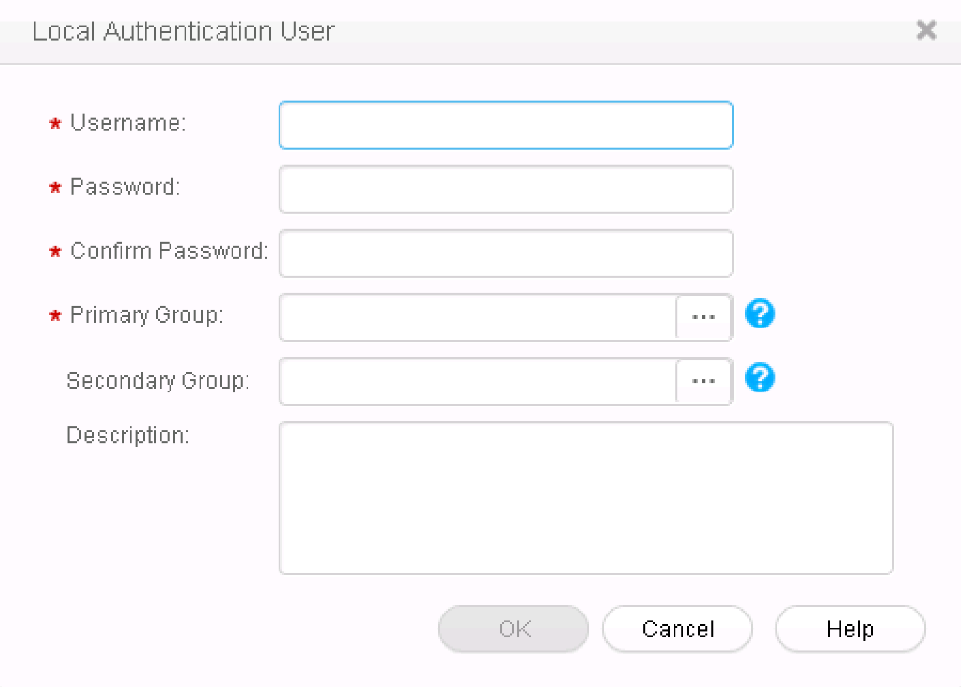
Step 1 Log in to DeviceManager.

Step 2 Choose **Provisioning** > **User Authentication**.

Step 3 Click **Local Authentication User** tab.

Step 4 Click **Create**.

The **Local Authentication User** dialog box is displayed.



Step 5 In **Username**, enter a new user name.

The user name:

- Cannot contain space, double quotation mark ("), slash (/), backslash (\), square brackets ([]), less than (<), larger than (>), plus (+), colon (:), semicolon (;), comma (,), question mark (?), asterisk (*), vertical bar (|), equal mark (=), (@), or end with a period (.).
- The user name can contain case-insensitive letters. Therefore, **aaaaaaaa** and **AAAAAAAA** cannot be created at the same time.
- The user name cannot be the same as the name of the local authentication user group.
- Contains 8 to 32 characters by default.

NOTE

You can modify the minimum length of user name in **More** > **Set Security Policies**.

Step 6 In **Password**, enter the password of the user.

The system default password requirements are:

- Contain 8 to 16 characters.
- Contain special characters. Special characters include: !"#$%&'()*+,-./:;<=>?@[\]^`{_|}~ and space.
- Contain any two types of the uppercase letters, lowercase letters, and digits.
- Cannot contain three consecutive same characters.
- Be different from the user name or the user name typed backwards.

NOTE

Click **More** and choose **Set Security Policies** to set a security policy for the password of the local authentication user in the file system. If **Password Validity Period (days)** is not selected, your password will never expire. For the security purpose, you are advised to select **Password Validity Period (days)** and set a validity period. The default validity period is 180 days. After the password expires, you cannot access shares, but you can set a password again and modify the password security policy.

Step 7 In **Confirm Password**, enter the new password again.

Step 8 Select **Primary Group**.

The **Select Primary Group** dialog box is displayed.

NOTE

The primary group to which users belong controls the users' permission for CIFS shares. A user must and can only belong to one primary group.

Step 9 Select the user group to which the user belongs to and click **OK**.

Step 10 (Optional) Select **Secondary Group**.

The **Select Secondary Group** dialog box is displayed.

NOTE

The concepts of primary group and secondary group are for local authentication users and have no relationship with each other. A local authentication user must belong to a primary group but not to a secondary group.

Step 11 Click **Add**.

The **Select User Group** dialog box is displayed.

Step 12 Select one or multiple groups which the user belongs to and click **OK**.

The system goes back to **Select Secondary Group** dialog box.

Step 13 Click **OK**.

The system goes back to **Local Authentication User** dialog box.

Step 14 **Optional:** In **Description** text box, enter the description for the local authentication user, for later management or search.

Step 15 Click **OK**.

Step 16 In the **Success** dialog box that is displayed, click **OK**.

----End

3.9.6.6 Accessing HTTP Shares

This section describes how to access an HTTP share in different ways.

Cadaver Software

Cadaver is a program that is commonly used to manage WebDAV share queries and modifications in Linux and UNIX, but HTTPS is not supported.

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

Step 2 Download and install Cadaver. For details about how to install Cadaver, see the related document.

Step 3 Run the **cadaver** *logical ip address* command. *logical ip address* indicates a logical port IP address used by the storage system to provide HTTP shares.

Step 4 Enter the user name and password of the local authentication user as prompted.

----End

Web Browser

HTTP is a non-security protocol. If the web browser supports HTTPS, you are advised to use HTTPS to connect to the storage system.

NOTE

Before using the web to access HTTP shares, run the **change service http enable_auto_index=yes** command on the CLI to open the directory list; otherwise, you cannot use the web to access HTTP shares.

Step 1 Open a web browser.

Step 2 In the address box, enter **http://*logical ip address***, where *logical ip address* indicates a logical port IP address used by the storage system to provide HTTP shares.

NOTE

- By default, the storage system provides the HTTPS service certificate. You are advised to replace the certificate with the private certificate before accessing HTTPS shares. After the certificate is replaced, the CA certificate of the storage system must be imported for the browser to eliminate security alarms. As the service IP address is used to access the HTTPS service, alarm **This website's address does not match the address in the security certificate** cannot be cleared.
- After the certificate provided by the storage system expired or is revoked, the browser displays the security alarm. Replace the certificate accordingly.

Step 3 Enter the user name and password of the local authentication user as prompted.

----End

4 Creating Storage Resources Based on Applications

About This Chapter

For 2000, 5000 and 6000 series storage systems, you can configure the storage resources for VMware and to enable the application server to use allocated storage resources.

4.1 About VMware
VMware is a set of virtualization server software developed by VMware.

4.2 Creating a VMware Instance
This operation allows you to create a VMware instance.

4.1 About VMware

VMware is a set of virtualization server software developed by VMware.

VMware can reduce operating expenses by consolidating and automating servers and minimize revenue loss through scheduled or unscheduled shutdown.

VMware mainly applies to:

- Server virtualization: Multiple operating systems run on one physical server as virtual machines. Each virtual machine can access computing resources on underlying servers.
- Storage resource virtualization: Software is used to divide storage layers. The performance and space utilization can be improved without new hardware.
- Desktop virtualization: Desktops are deployed in hosting mode, helping you quickly respond to changing requirements.
- Application virtualization: Critical service applications and platforms, such as databases, ERP, CRM, emails, collaboration systems, Java middleware, and business intelligence platforms, can be virtualized.
- Network virtualization: Software is used to reproduce physical networks completely and virtualize logical network connection devices and services (such as logical ports, switches, routers, firewalls, load balancers, and VPN). Then those virtualized resources can be used by other connected devices.

The storage system can automatically allocate storage resources based on service configurations of VMware applications.

4.2 Creating a VMware Instance

This operation allows you to create a VMware instance.

Prerequisites

The system has sufficient storage space.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Provisioning** > **Application** > **VMware**.

Step 3 Select **File System** in **Resource Type**.

Step 4 Click **Create**.

The **Create VMware Storage Resource Wizard** is displayed.

Step 5 Set basic information about the VMware instance to be created.

Table 4-1 describes related parameters.

Table 4-1 Parameters of a VMware instance

Parameter	Description	Value
Name	Name of a VMware instance. The name must meet the following requirements so that the instance is available to host applications: ● Must be unique. ● Contains only letters, digits, and underscores (_). ● Contains 1 to 22 characters.	[Example] **VMwareApp_001**
Description	Description of a VMware instance. **Description** must contains 0 to 255 characters.	[Example] -

Step 6 Click **Next** and select a virtualization type.

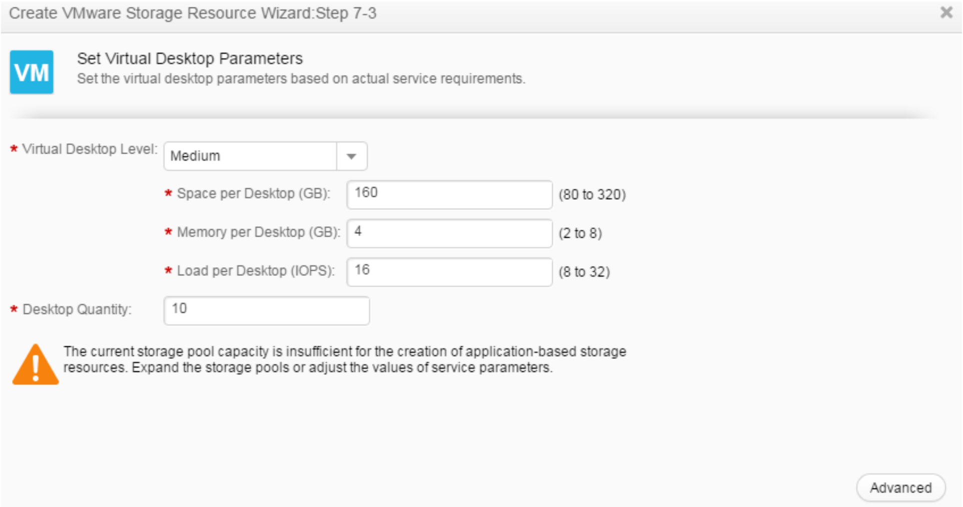
Table 4-2 describes related parameters.

Table 4-2 VMware application parameters

Parameter	Description	Value
Virtual desktop	Allows enterprise-level applications to dynamically access desktop systems remotely and implements central hosting of data centers.	[Example] Virtual desktop
Virtual server	Reduces consumption of manpower and material resources and simplifies work for small- and mid-size enterprises and enterprises that construct websites for the first time.	[Example] Virtual server

Step 7 Set related parameters based on the selected virtualization type.

- If **Virtual desktop** is selected, set virtual desktop parameters, as shown in **Table 4-3**.



Create VMware Storage Resource Wizard:Step 7-3

Set Virtual Desktop Parameters

Set the virtual desktop parameters based on actual service requirements.

* Virtual Desktop Level: Medium

* Space per Desktop (GB): 160 (80 to 320)

* Memory per Desktop (GB): 4 (2 to 8)

* Load per Desktop (IOPS): 16 (8 to 32)

* Desktop Quantity: 10

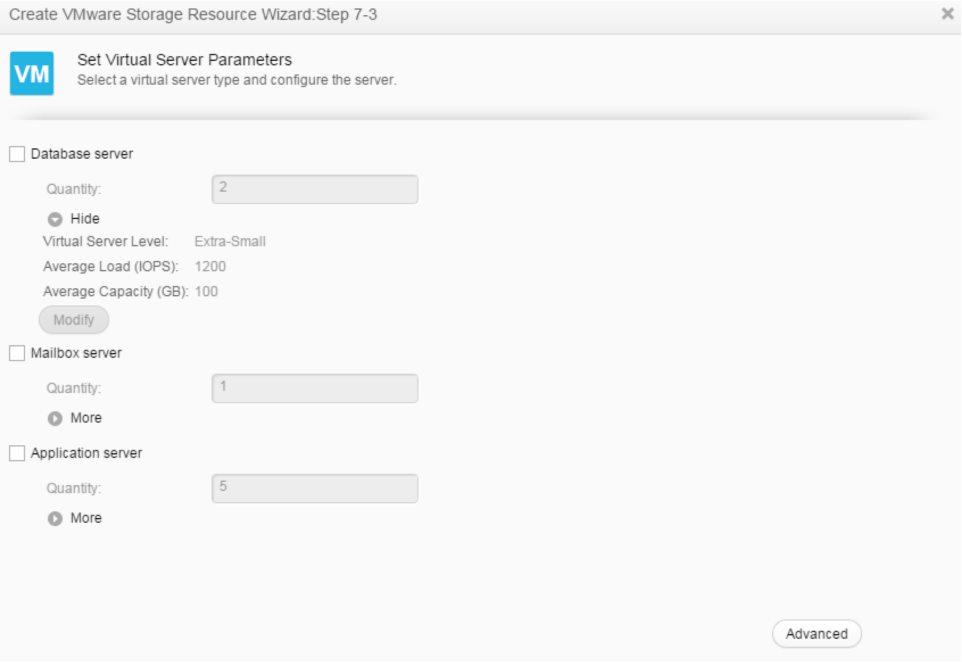
The current storage pool capacity is insufficient for the creation of application-based storage resources. Expand the storage pools or adjust the values of service parameters.

Table 4-3 Virtual desktop parameters

Parameter	Description	Value
Virtual Desktop Level	Level of the virtual desktop constructed by VMware. The value of this parameter affects the values of **Space per Desktop (GB)**, **Memory per Desktop (GB)**, and **Load per Desktop (IOPS)**.	[Value range] The value can be **Small**, **Medium**, **Large** and **Extra-Large**. [Example] Medium

Parameter	Description	Value
Space per Desktop (GB)	Maximum storage space allocated by VMware to each virtual desktop. The value of this parameter is subject to **Virtual Desktop Level** and is user-definable.	[Example] 160
Memory per Desktop (GB)	Maximum memory capacity allocated by VMware to each virtual desktop. The value of this parameter is subject to **Virtual Desktop Level** and is user-definable.	[Example] 4
Load per Desktop (IOPS)	Maximum IOPS of each virtual desktop. The value of this parameter is subject to **Virtual Desktop Level** and is user-definable.	[Example] 16
Desktop Quantity	Number of virtual desktops constructed by VMware.	[Example] 10

- If **Virtual server** is selected, set virtual server parameters, as shown in **Table 4-4**.



Create VMware Storage Resource Wizard:Step 7-3 ✕

VM Set Virtual Server Parameters
Select a virtual server type and configure the server.

□ Database server

Quantity: 2

Hide

Virtual Server Level: Extra-Small

Average Load (IOPS): 1200

Average Capacity (GB): 100

Modify

□ Mailbox server

Quantity: 1

More

□ Application server

Quantity: 5

More

Advanced

Table 4-4 Virtual server parameters

Parameter	Description	Value
Database server	Type of a VMware virtual server.	[Example] -
Mailbox server	Type of a VMware virtual server.	[Example] -
Application server	Type of a VMware virtual server.	[Example] -
Quantity	Number of virtual servers constructed by VMware.	[Value range] The number of servers is subject to **Average Load (IOPS)**, **Average Capacity (GB)**, and type. [Example] **2**
Virtual Server Level	Level of a virtual server constructed by VMware. The value of this parameter affects the values of **Average Load (IOPS)** and **Average Capacity (GB)**.	[Value range] The value can be **Extra-Small**, **Small**, **Medium**, **Large** and **Extra-Large**. [Example] **Medium**
Average Load (IOPS)	IOPS of a virtual server. The value of this parameter is subject to **Virtual Server Level** and is user-definable.	[Example] **25**
Average Capacity (GB)	Storage capacity allocated to virtual servers. The value of this parameter is subject to **Virtual Server Level** and is user-definable.	[Example] **25**

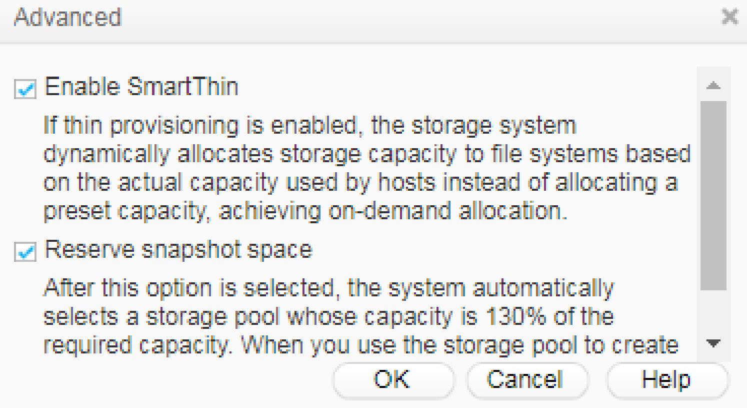
Step 8 **Optional:** Set advanced properties for VMware applications.

1. Click **Advanced**.

   The **Advanced** dialog box is displayed.

2. Set advanced properties for VMware applications.

   Table 4-5 describes related parameters.



Advanced

☑ Enable SmartThin

If thin provisioning is enabled, the storage system dynamically allocates storage capacity to file systems based on the actual capacity used by hosts instead of allocating a preset capacity, achieving on-demand allocation.

☑ Reserve snapshot space

After this option is selected, the system automatically selects a storage pool whose capacity is 130% of the required capacity. When you use the storage pool to create

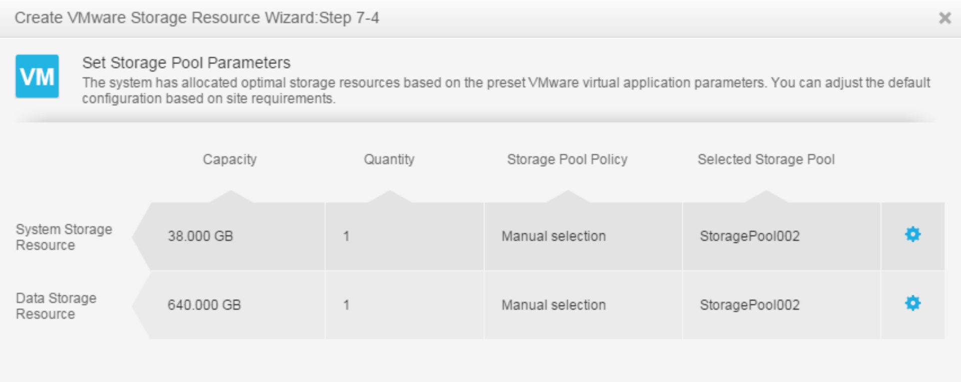
Table 4-5 Parameters in advanced properties of a VMware application

Parameter	Description	Value
Enable SmartThin	If thin provisioning is enabled, the storage system dynamically allocates storage capacity to file systems based on the actual capacity used by hosts instead of allocating a preset capacity, achieving on-demand allocation.	[Example] Enable SmartThin
Reserve snapshot space	After this option is selected, the system automatically selects a storage pool whose capacity is 130% of the required capacity. When you use the storage pool to create storage resources for applications, reserve sufficient space to create snapshots for applications.	[Example] -

3. Click **OK**.

   You are returned to the **Set Virtual Desktop Parameters** or **Set Virtual Server Parameters** page.

Step 9 Click **Next** and set parameters for VMware storage resources. The system will allocate optimal storage resources based on preset VMware parameters.



Create VMware Storage Resource Wizard:Step 7-4

Set Storage Pool Parameters

The system has allocated optimal storage resources based on the preset VMware virtual application parameters. You can adjust the default configuration based on site requirements.

	Capacity	Quantity	Storage Pool Policy	Selected Storage Pool
System Storage Resource	38.000 GB	1	Manual selection	StoragePool002
Data Storage Resource	640.000 GB	1	Manual selection	StoragePool002

Table 4-6 VMware storage resource parameters

Parameter	Description	Value
Capacity	Storage space allocated to store system data or data.	[Example] **640 GB**
Quantity	Number of file systems allocated to store system data or data.	[Example] **1**
Storage Pool Policy	The system sets storage pool allocation policies based on preset VMware parameters. The performance level of each VM is defined by **High performance**, **Performance/Cost balance**, **Low cost**, or **Manual selection**, described as follows: ● High performance: The system automatically selects a RAID 6 storage pool containing SAS disks only. If such a storage pool does not exist in the system, create one. ● Performance/Cost balance: The system automatically selects a RAID 6 storage pool containing SAS and NL-SAS disks only. If such a storage pool does not exist in the system, create one. ● Low cost: The system automatically selects a RAID 6 storage pool containing NL-SAS disks only. If such a storage pool does not exist in the system, create one. ● Manual selection: Users define storage pools that meet the VMware service requirements.	[Example] Manual selection
Selected Storage Pool	Name of the storage pool automatically allocated by the system to a VMware instance.	[Example] **StoragePool001**

Step 10 **Optional:** If no desired storage pools are available, click ⚙ and modify **Storage Pool Policy** in the displayed dialog box, or click **Create Storage Pool** to create one. **Table 4-6** describes related parameters.

Step 11 **Optional:** Set permissions for NFS share.

1. Select a client that you want to set NFS share in **Client Information**.

Click **Add** to create a client if there is no one in the client list. For details, please refer to **Adding an NFS Share Client** in *OceanStor V3 Series V300R006 Basic Storage Service Guide for File*.

2. Click **Next**.

Step 12 Confirm your settings.

1. Click **Next**.

   The **Summary** page is displayed.

2. Verify that the information about the VMware instance to be created is correct and click **Finish**.

   The **Execution Result** dialog box is displayed indicating that the operation succeeded.

3. Click **Close**. You have finished creating a VMware instance.

----End

5 Managing Basic Storage Services

About This Chapter

This chapter describes how to manage basic storage services through DeviceManager, to meet your service requirements.

5.1 Managing Access Permission of a Storage System
To ensure device and service data security, the storage systems support security policy adjustment, IP address access control, and user management.

5.2 Managing Disk Domains
A disk domain consists of the same type or different types of disks.

5.3 Managing Storage Pools
A storage pool is created under a disk domain and serves as a container of storage resources. The storage resources used by application servers are all from storage pools.

5.4 Managing a File System
This section introduces how to manage and maintain a file system that has been configured.

5.5 Managing an NFS Share
After an NFS share is configured for a storage system, you need to manage and maintain the NFS share. This section describes how to manage an NFS share.

5.6 Managing a CIFS Share
After a CIFS share is configured for a storage system, you need to manage and maintain the CIFS share. This section describes how to manage a CIFS share.

5.7 Managing a CIFS Homedir Share (Applicable to V300R006C10)
This section explains how to query, modify, and delete CIFS Homedir shares.

5.8 Managing an FTP Share
FTP shares enable permission control and file systems to be shared for specific users. FTP share management includes maintaining existing shares and controlling the global properties of the FTP feature. This chapter describes how to update existing FTP shares and how to manage the global parameters of FTP shares.

5.9 HTTP Share Management
After an HTTP share is configured for a storage system, you need to manage and maintain the HTTP share. This chapter describes how to manage an HTTP share.

5.10 Configuring and Managing Authentication Users
Authentication users are for accessing file system shares you create. Authentication users include local authentication users and user groups.

5.11 User Mapping Management
User mappings enable you to access shares across different operating systems by using the mappings created locally or in the IDMU domain. This chapter describes how to manage user mappings.

5.12 Operations
The following operations enable you to manage Ethernet ports, VLANs, FC port, FCoE port, port group, bond port and logical ports.

5.1 Managing Access Permission of a Storage System

To ensure device and service data security, the storage systems support security policy adjustment, IP address access control, and user management.

5.1.1 Configuring a Security Policy for System User

You can set the username and password policies to control the username and password complexity of new accounts. The login policy enables the system to lock the accounts with security exceptions.

Context

The storage system supports the following password policies to ensure account security.

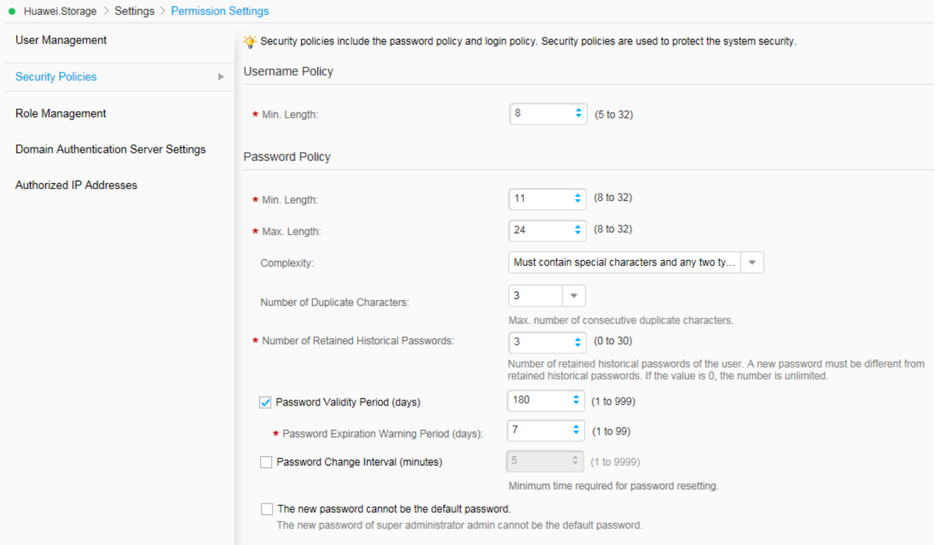
- The storage system supports strong password complexity to prevent brute-force password cracking.
- Passwords must be encrypted before they are stored and transferred.
- Passwords can be changed only after authentication and users can only change their own passwords.

Procedure

1. Log in to DeviceManager.
2. Choose **Settings** > **Permission Settings** > **Security Policies**.
   a. On the right navigation bar, click **Settings**.
   b. In the **Basic Service Settings** area on the function pane, click **Permission Settings**.

      The **Security Policies** page is displayed.
   c. In the left navigation tree, select **Security Policies**.

      The **Security Policies** page is displayed.


Huawei.Storage > Settings > Permission Settings
User Management
Security Policies
Role Management
Domain Authentication Server Settings
Authorized IP Addresses

Security policies include the password policy and login policy. Security policies are used to protect the system security.

Username Policy

* Min. Length: 8 (5 to 32)

Password Policy

* Min. Length: 11 (8 to 32)

* Max. Length: 24 (8 to 32)

Complexity: Must contain special characters and any two ty...

Number of Duplicate Characters: 3

Max. number of consecutive duplicate characters.

* Number of Retained Historical Passwords: 3 (0 to 30)

Number of retained historical passwords of the user. A new password must be different from retained historical passwords. If the value is 0, the number is unlimited.

☑ Password Validity Period (days) 180 (1 to 999)

* Password Expiration Warning Period (days): 7 (1 to 99)

□ Password Change Interval (minutes) 5 (1 to 9999)

Minimum time required for password resetting.

□ The new password cannot be the default password.

The new password of super administrator admin cannot be the default password.

3. **Table 5-1**, **Table 5-2**, **Table 5-3**, and **Table 5-4** describe the parameters related to configuration of user name, password, login, and account audit policies.

Table 5-1 User name policy

Parameter	Description	Value
Minimal length	Minimum length of a user name. The user name cannot be too simple.	[Value range] The value is an integer ranging from 5 to 32. [Example] 6

Table 5-2 Password policies

Parameter	Description	Value
Min. Length	Minimum length of a password, avoiding too short passwords.	[Value range] The value is an integer ranging from 8 to 32. [Example] 8
Max. Length	Maximum length of a password, avoiding too long passwords.	[Value range] The value is an integer ranging from 8 to 32. [Example] 16

Parameter	Description	Value
Complexity	Complexity of the password, avoiding too simple passwords.	[Value range] The password must contain special characters and at least two types among uppercase letters, lowercase letters, and digits, or the password must contain special characters, uppercase letters, lowercase letters, and digits. [Example] The password must contain special characters and at least two types among uppercase letters, lowercase letters, and digits.
Number of Duplicate Characters	Maximum number of consecutive same characters in a password.	[Value range] The value is not restricted or the value is an integer ranging from 1 to 9. [Example] 3
Number of Retained Historical Passwords	Number of historical passwords retained for a user. The new password must be different from the historical passwords. If the value is **0**, there is no restriction.	[Value range] The value is an integer ranging from 0 to 30. [Example] 3
Password Validity Period (days)	Setting of a password's validity period. After **Password Validity Period (days)** is enabled, you must set the days in which a password is valid. After the validity period of the password expires, the system prompts you to change the password in a timely manner. **NOTE** If this parameter is not selected, the password will never expire. To ensure storage system security, you are advised to select and set this parameter.	[Value range] The value is an integer ranging from 1 to 999. [Example] 90

Parameter	Description	Value
Password Expiration Warning Period (days)	Number of days prior to password expiration that the administrator receives a warning message.	[Value range] The value is an integer ranging from 1 to 99. [Example] 7
Min. Password Lifespan (minutes)	Minimum lifespan of a new password.	[Value range] The value is an integer ranging from 1 to 9999. [Example] 5
The new password cannot be the default password.	The new password of super administrator admin cannot be the default password.	[Value range] The value is an integer ranging from 1 to 9999. [Example] 5

Table 5-3 Login policies

Parameter	Description	Value
Session Timeout Duration (minutes)	Duration after which the system indicates timeout if a logged-in administrator performs no operations during the period. After you click **OK** in the event of timeout, the system returns to the login page.	[Value range] The value is an integer ranging from 1 to 100. [Example] 30
Password Lock	Locks a user if the count of consecutively inputting incorrect passwords by the user exceeds Number of Incorrect Passwords within 10 minutes.	[Value range] **Enable** or **Disable** [Example] **Enable**

Parameter	Description	Value
Number of Incorrect Passwords	Times allowed for consecutively entering incorrect passwords. The system automatically locks a user if the times of consecutively inputting incorrect passwords by the user exceed **Number of Incorrect Passwords**. NOTE ● This parameter is available only when **Password Lock** is enabled. ● After a user is locked, the super administrator can manually unlock the user. If **Lock Mode** is set to **Temporary**, the user will be automatically unlocked when the unlock time arrives.	[Value range] The value is an integer ranging from 1 to 9. [Example] 3
Lock Mode	Mode of automatically locking a user. ● In **Permanent** mode, administrators and read-only users are locked permanently. The super administrator will be automatically unlocked after 15 minutes. ● In **Temporary** mode, you can set a duration of locking administrators and read-only users.	[Value range] **Temporary** or **Permanent** [Example] **Temporary**
Automatic Unlock in (minutes)	Duration of locking a user. After the lock duration expires, the locked user is automatically unlocked. ● This parameter is available only when **Password Lock** is enabled and **Lock Mode** is **Temporary**. ● This parameter is available to automatic lock only. This parameter is unavailable if a user is manually locked. The user can be manually unlocked only. ● Automatic unlock is only applicable to administrators and read-only users. The super administrator will be automatically unlocked after 15 minutes in both **Permanent** and **Temporary** modes.	[Value range] The value is an integer ranging from 3 to 2000. [Example] 15
Lock Account When Idle	A system account will be locked if it is not used for login and the idle period exceeds the specified days.	[Value range] **Enable** or **Disable** [Example] **Enable**

Parameter	Description	Value
Idle Period (days)	Idle days of a system account.	[Value range] The value is an integer ranging from 1 to 999. [Example] 60
Login Security Info	After a user login, information about the last login (including the login time and IP address) is displayed.	[Value range] **Enable** or **Disable** [Example] **Enable**
User-Defined Info	After an account's successful login, an alarm is displayed indicating the preset information.	[Value range] **Enable** or **Disable** [Example] **Enable**
Info	The information to prompt the successful login of user account.	[Value range] The information contains 1 to 511 characters. [Example] Login successful

Table 5-4 Account audit policies

Parameter	Description	Value
User Account Audit	Periodically audits the number and permission of user accounts to ensure account security.	[Value range] **Enable** or **Disable** [Example] **Enable**
Audit Period (Days)	Periodically audits period of the account.	[Value range] The value is an integer ranging from 0 to 999. [Default] 120

4. Confirm the security policy configuration.
   a. Click **Save**.

      The **Execution Results** dialog box is displayed, indicating that the security policy configuration succeeds.
   b. Click **Close**.

5.1.2 Configuring Authorized IP Addresses

You can specify the IP addresses that can access the device from DeviceManager to prevent unauthorized access.

Prerequisites

You are a super administrator. (Only super administrators have the permission to perform this operation.)

Procedure

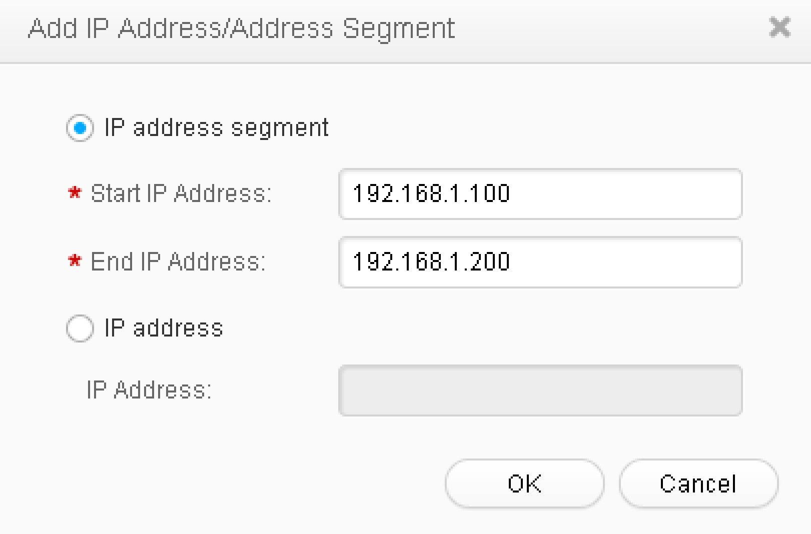
Step 1 Log in to DeviceManager.

Step 2 Choose **Settings** > **Permission Settings** > **Authorized IP Addresses**.

Step 3 Authorize IP addresses.

1. Select **Enable**.
2. Click **Add**.

   The **Add IP Address/Address Segment** dialog box is displayed.



Add IP Address/Address Segment

● IP address segment

* Start IP Address: 192.168.1.100

* End IP Address: 192.168.1.200

○ IP address

IP Address:

3. Enter the IP segment or IP address that can access the storage device.
   - To authorize an IP address segment, select **IP address segment** and set **Start IP Address** and **End IP Address**. IP addresses included in the IP address segment are allowed to access the storage device.
   - To authorize IP addresses, select **IP address** and set **IP Address**.
4. Click **OK**. The specified IP segment or IP address is added to the IP address segment/IP address list.

   NOTE

   After this function is enabled, if you want to prevent one IP address or IP address segment from accessing devices, select the IP address or IP address segment from the IP address/IP address segment list and click **Remove**. Note that at least one IP address or IP address segment must be allowed access.
5. Click **Save**, read and confirm the prompt information.

The **Execution Result** dialog box is displayed, indicating that the operation succeeded.

Step 4 Click **Close**.

----End

5.1.3 Managing Users and Their Access Permissions

To prevent misoperations from affecting device stability and service data security, the storage device defines three user levels, each with certain permission.

5.1.3.1 Creating a Local User

To ensure device stability and service data security, a super administrator can create different levels of users based on service requirements.

Procedure

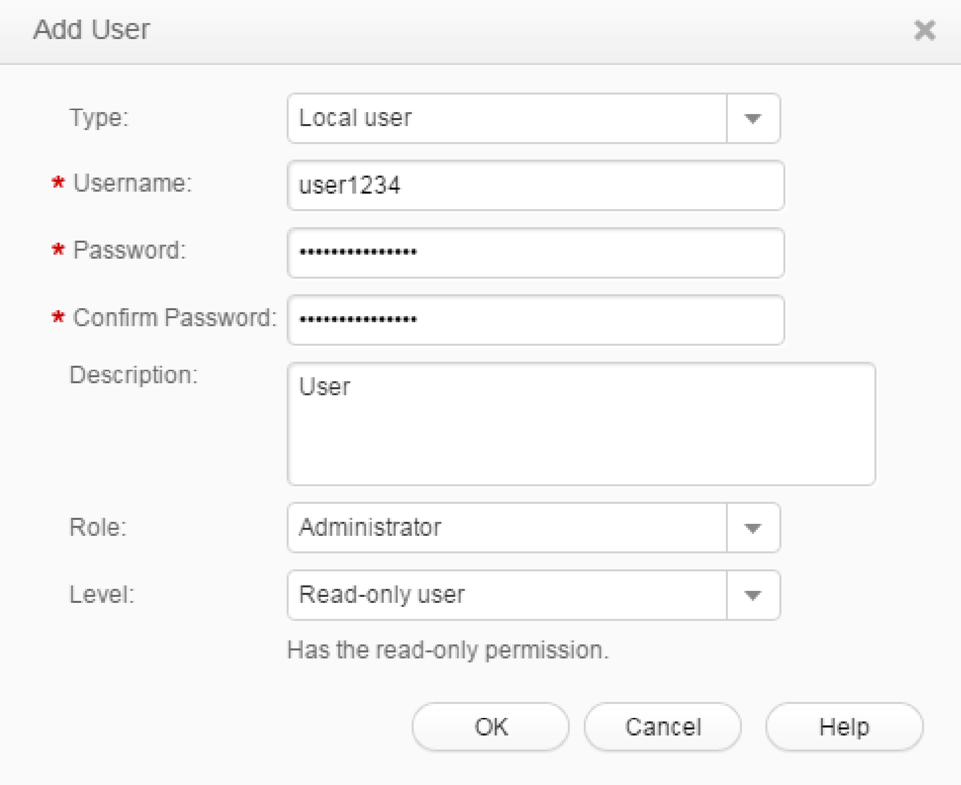
Step 1 Log in to DeviceManager.

Step 2 Choose **Settings** > **Permission Settings** > **User Management**.

Step 3 In the right function pane, click **Add**.

The **Add User** dialog box is displayed.

Step 4 Set user information. Select **Local user** in **Type** and configure relevant parameters.



Add User

Type: Local user

* Username: user1234

* Password: ••••••••••••••••

* Confirm Password: ••••••••••••••••

Description: User

Role: Administrator

Level: Read-only user

Has the read-only permission.

Table 5-5 describes the local user parameters.

Table 5-5 Local user parameters

Parameter	Description	Value
Username	Name of a newly created user.	[Value range] ● The name contains 5 to 32 characters. ● The name can only contain letters, digits, and underscores (_) and must start with a letter. ● The username must be unique. **NOTE** You can modify the username policy in **Permission Settings** > **Security Policies**. [Example] user1234
Password	Password of a newly created user.	[Value range] ● The password contains 8 to 32 characters. ● The password must contain special characters. Special characters include !"#$%&'()*+,-./:;<=>?@[\]^`{_|}~ and spaces. ● The password must contain any two types of uppercase letters, lowercase letters and digits. ● The maximum number of consecutive same characters cannot exceed 3. ● The password cannot be the same as the username or the username typed backward. **NOTE** ● You can modify the password policy in **Permission Settings** > **Security Policies**. ● Keep your password safe. [Example] a#123456

Parameter	Description	Value
Confirm password	Password for confirmation.	[Value range] The value must be the same as that of **Password**. [Example] a#123456
Description	Description of a newly created user.	[Example] User
Role	Set permissions for users. You can select a built-in role or create a self-defined role.	[Example] Administrator
Level	Level of a user. Possible values are as follows: ● Super administrator: has full administrative permissions on the storage device, and is able to create the users at all user levels. ● Administrator: has partial system administration permissions. Specifically, they cannot manage users, upgrade storage devices, modify system time, restart devices, or power off devices. ● Read-only user: has only the access permission for the storage system and can perform queries only.	[Example] Read-only user

Step 5 Confirm the user account creation.

1. Click **OK**.

   The **Success** dialog box is displayed, indicating that the operation succeeded.

2. Click **OK**.

----End

5.1.3.2 Creating a Domain User

DeviceManager allows users to log in to the storage system using the Lightweight Directory Access Protocol (LDAP) server authentication mode to centrally manage user information.

Prerequisites

Configure a domain authentication server before creating an LDAP user or LDAP user group. For details, see **Configuring Domain Authentication for a Storage System** in the *Installation Guide* of the corresponding product model.

Procedure

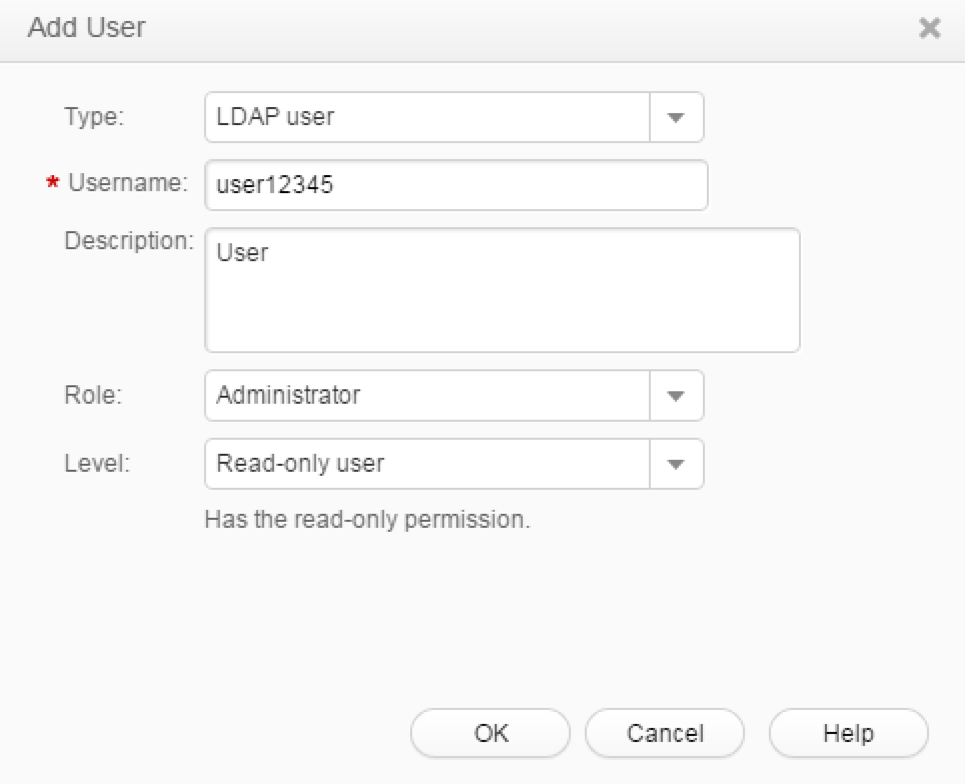
Step 1 Log in to DeviceManager.

Step 2 Choose **Settings** > **Permission Settings** > **User Management**.

Step 3 In the right function pane, click **Add**.

The **Add User** dialog box is displayed.

Step 4 Set user information. Select **LDAP user** or **LDAP user group** in **Type** and configure the relevant parameters. **Table 5-6** describes these parameters.



Add User

Type: LDAP user

* Username: user12345

Description: User

Role: Administrator

Level: Read-only user

Has the read-only permission.

Table 5-6 LDAP user or LDAP user group parameters

Parameter	Description	Value
Username	Name of a newly created LDAP user or LDAP user group. **NOTE** The LDAP user or LDAP user group to be created must reside on the LDAP domain server. Otherwise, the login will fail.	[Value range] ● The username contains 1 to 64 characters. ● The username must be unique. [Example] user12
Description	Description of a newly created user.	[Example] User
Role	Set permissions for users. You can select a built-in role or create a self-defined role.	[Example] Administrator
Level	Level of a newly created LDAP user or LDAP user group. Possible values are as follows: ● Administrator: has partial system administration permissions. Specifically, they cannot manage users, upgrade storage devices, modify system time, restart devices, or power off devices. ● Read-only user: has only the access permission for the storage system and can perform queries only.	[Example] Read-only user

Step 5 Confirm the user account creation.

1. Click **OK**.

   The **Success** dialog box is displayed, indicating that the operation succeeded.

2. Click **OK**.

----End

5.1.3.3 Managing User Levels

A super administrator can change the level of a read-only user or an administrator according to the actual requirements.

Prerequisites

- Only super administrators have the right to perform this operation.
- The super administrator can modify the level and initiate the password only for users whose **Status** is **Offline**.

Context

User levels include:

- **Administrator**: has permission to control the storage device and modify password of administrator, but cannot manage users, upgrade the storage device, modify system time, activate license files, restart device, or power off device. Local user administrator cannot import license files, and LDAP user administrator cannot perform any import or export operation.
- **Read-only user**: has permission to access the storage device and change its password. After logging in to the storage device, the read-only user can only query device information but cannot perform other operations.

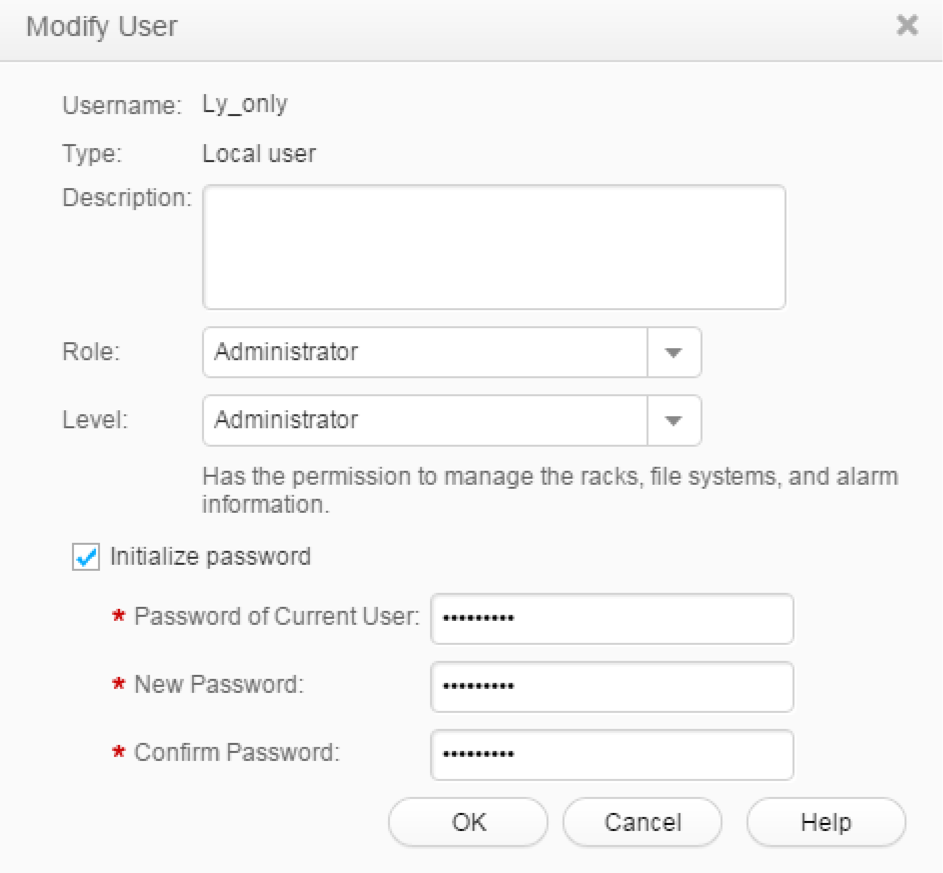
Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Settings** > **Permission Settings** > **User Management**.

Step 3 In the middle function pane, select a user that you want to modify and click **Modify**.

The **Modify User** dialog box is displayed.



Modify User

Username: Ly_only

Type: Local user

Description:

Role: Administrator

Level: Administrator

Has the permission to manage the racks, file systems, and alarm information.

☑ Initialize password

* Password of Current User: ••••••••••

* New Password: ••••••••••

* Confirm Password: ••••••••••

Step 4 Select a desired user level from the **Level** drop-down list.

NOTE

The user level determines whether a user has operation or read-only permission. For details on how to modify the scope of permission, see **Customizing User Roles**.

Step 5 Confirm the user modification.

1. Click **OK**.

   The security alert dialog box is displayed. Confirm the information in the dialog box and select **I have read and understand the consequences associated with performing this operation**.

2. Click **OK**.

   The **Execution Result** dialog box is displayed, indicating that the operation succeeded.

3. Click **Close**.

----End

5.1.3.4 Customizing User Roles

User roles control the scopes of permission for users. A super administrator can change the role of a read-only user or an administrator to adjust the user's scope of permission according to the actual requirements. After a role is assigned to a user, the user has the permission to access or operate the objects specified by the role.

Prerequisites

The super administrator can modify the level and role and initiate the password only for users whose **Status** is **Offline**.

Context

The storage system provides typical default roles. If the default roles cannot meet your requirements, you can create roles.

Procedure

Step 1 Log in to DeviceManager.

Step 2 **Optional:** Choose ⚙ **Settings** > **Permission Settings** > **Role Management** and manage user-defined roles. Table 5-7 details the operations.

NOTE

- You can create roles if the system's default roles do not meet your requirements.
- You can modify existing user-defined roles as required.
- You can delete user-defined roles that are not needed any more.

Table 5-7 Managing user-defined roles

Operation	Procedure
Adding a user-defined role	1. In the function pane, click **Add**. The **Add Role** dialog box is displayed. 2. Set relevant parameters and click **Finish**. Table 5-8 describes the parameters. 3. On the **Execution Result** page, click **Close**.

Operation	Procedure
Modifying a user-defined role	1. In the function pane, select a role and click **Modify**. The **Modify Permission** dialog box is displayed. 2. On the **General** and **Permission** tab pages, modify the parameters as required. **Table 5-8** describes the parameters. 3. Click **OK**.
Deleting a user-defined role	1. In the function pane, select a role and click **Delete**. The **Success** dialog box is displayed. 2. Click **OK**.

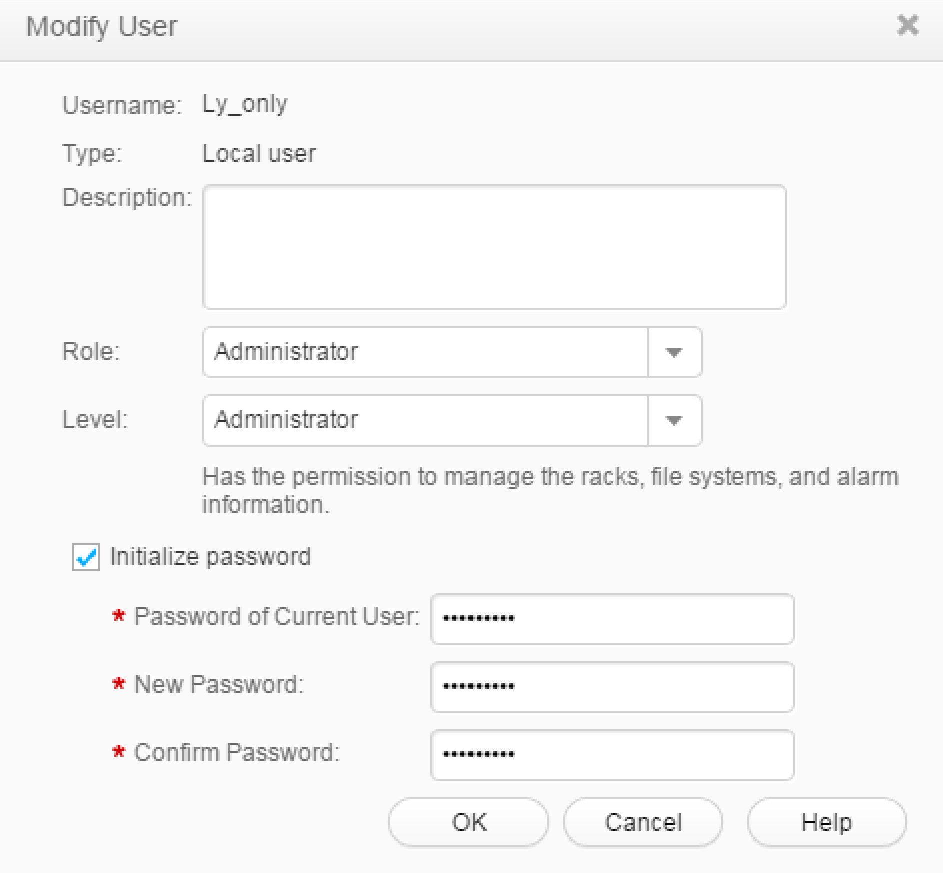
Table 5-8 User-defined role parameters

Parameter	Description
Name	Name of a role.
Owning group	The value can be **System Group** or **vStore Group**. ● If a role belongs to **System Group**, its permissions are valid in the system view. ● If a role belongs to **vStore Group**, its permissions are valid in the vStore view.
Description	Description of a role.
Object	Required object. For the object functions, see **A Permission Matrix for Self-defined Roles**.
Read/Write Permission	Read/write permission of the selected object. The value can be **Read-only** or **Readable and writable**.

Step 3 Change the user role.

1. Choose ⚙ **Settings** > **Permission Settings** > **User Management**.
2. In the middle function pane, select a user that you want to modify and click **Modify**.

   The **Modify User** dialog box is displayed.



Username: Ly_only

Type: Local user

Description:

Role: Administrator

Level: Administrator

Has the permission to manage the racks, file systems, and alarm information.

☑ Initialize password

* Password of Current User: ••••••••••

* New Password: ••••••••••

* Confirm Password: ••••••••••

3. Select a desired role from the **Role** drop-down list.

   NOTE

   You can select a built-in or user-defined role based on your actual requirements.

Step 4 Confirm the user modification.

1. Click **OK**.

   The security alert dialog box is displayed. Confirm the information in the dialog box and select **I have read and understand the consequences associated with performing this operation**.

2. Click **OK**.

   The **Execution Result** dialog box is displayed, indicating that the operation is successful.

3. Click **Close**.

----End

5.1.3.5 Locking or Unlocking a User

A super administrator can prevent a user from logging in to the storage device by locking the user. Locked users online at the time they are locked can continue using DeviceManager but will not be able to log in again after they log out.

Prerequisites

- Only super administrators have the permission to perform this operation.

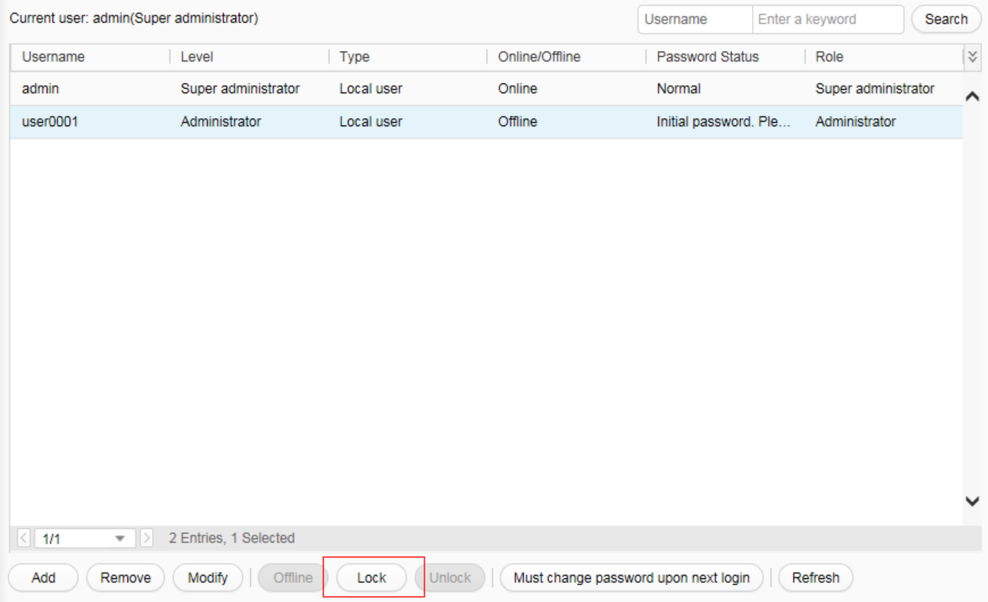
- **Lock Status** of the user to be locked is **Unlock**.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Settings** > **Permission Settings** > **User Management**.

Step 3 In the middle function pane, choose a user that you want to lock and click **Lock**.



Current user: admin(Super administrator)

Username	Level	Type	Online/Offline	Password Status	Role
admin	Super administrator	Local user	Online	Normal	Super administrator
user0001	Administrator	Local user	Offline	Initial password. Ple...	Administrator

1/1 2 Entries, 1 Selected

The **Success** dialog box is displayed indicating that the operation succeeded.

NOTE

You can also right-click the user that you want to lock and choose **Lock**.

Step 4 Click **OK**.

----End

Follow-up Procedure

A super administrator can allow the user to log in to the storage device by unlocking the user.

1. Log in to DeviceManager.
2. Choose **Settings** > **Permission Settings** > **User Management**.
3. In the middle function pane, choose a user that you want to unlock and click **Unlock**.

   NOTE

   You can also right-click the user that you want to unlock and choose **Unlock**.

   The **Permission Authentication** dialog box is displayed.
4. Enter the password of the login user, and click **OK**.

   The **Success** dialog box is displayed indicating that the operation succeeded.
5. Click **OK**.

5.1.3.6 Logging Out a User

A super administrator can prevent a logged-in user from using the storage device by forcibly logging the user out of DeviceManager.

Prerequisites

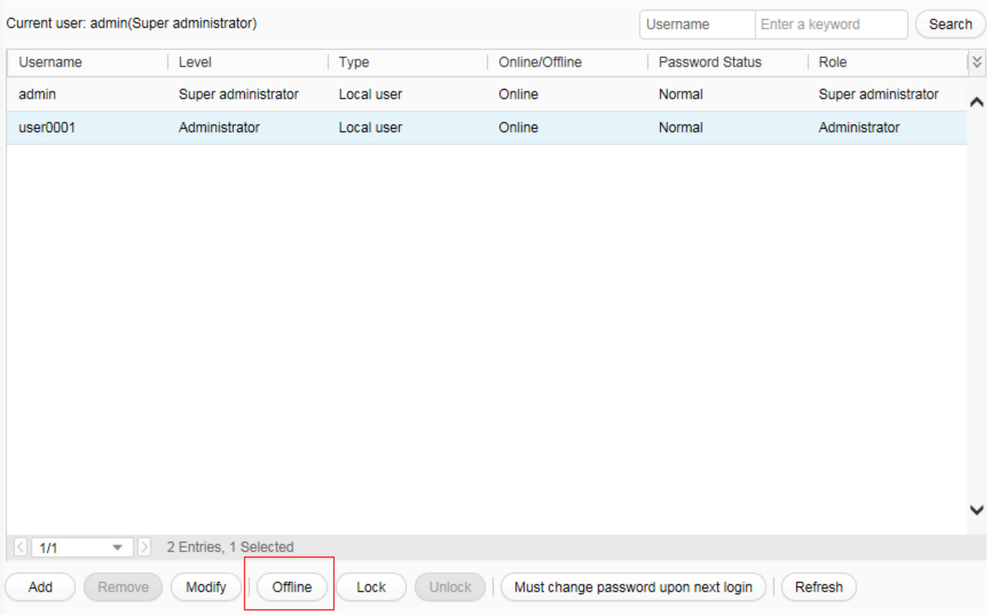
- Only a super administrator has the permission to perform this operation.
- Users whose **Status** is **Online** can be logged out.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Settings** > **Permission Settings** > **User Management**.

Step 3 In the function pane, select a user that you want to log out and click **Offline**.



Current user: admin(Super administrator)

Username	Level	Type	Online/Offline	Password Status	Role
admin	Super administrator	Local user	Online	Normal	Super administrator
user0001	Administrator	Local user	Online	Normal	Administrator

1/1 2 Entries, 1 Selected

The security alert dialog box is displayed.

NOTE

You can also right-click the user, and choose **Offline**.

Step 4 Confirm the logout of the user.

1. Carefully read the content in the dialog box and select **I have read and understand the consequences associated with performing this operation** to confirm the information.
2. Click **OK**.

   The **Success** dialog box is displayed indicating that the operation succeeded.
3. Click **OK**.

----End

5.2 Managing Disk Domains

A disk domain consists of the same type or different types of disks.

5.2.1 Viewing Disk Domain Information

This operation enables you to view disk domain information.

Prerequisites

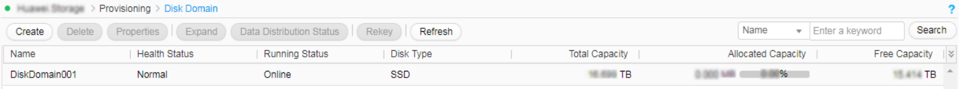
A disk domain has been created in the system.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Provisioning** > **Disk Domain**.

Step 3 View disk domain information in the upper left area. **Table 5-9** describes related parameters.



Name	Health Status	Running Status	Disk Type	Total Capacity	Allocated Capacity	Free Capacity
DiskDomain001	Normal	Online	SSD	[redacted] TB	[redacted] [redacted]%	[redacted] TB

Table 5-9 Disk domain parameters

Parameter	Description	Setting
Name	Name of a disk domain.	[Example] DiskDomain001
ID	ID of a disk domain.	[Example] 1
Health Status	Health status of a disk domain.	[Example] Normal
Running Status	Running status of a disk domain.	[Example] Online

Parameter	Description	Setting
Disk Type	Type of disks in a disk domain. The disk is categorized by its storage media and whether it is encrypted or not. ● SSD ● SSD-SED ● SAS ● SAS-SED ● NL-SAS ● NL-SAS-SED **NOTE** Self-encrypting drives (SED) means encrypted disk.	[Example] SSD
Total Capacity	Total capacity of a disk domain.	[Example] 2.00 TB
Allocated Capacity	Allocated capacity of a disk domain.	[Example] 100.00 MB
Free Capacity	Free capacity of a disk domain.	[Example] 500 GB
Anti-Wear Leveling Disk ID	If the wear degree of any disk is high, the system enters the anti-wear leveling mode, and the ID of the disk with the highest wear degree is displayed.	[Example] —

NOTE

The following operations can improve your efficiency:

- Click ︾ in the upper right part of the function pane and set the parameters to be displayed.
- In the search bar in the upper right corner of the **Disk Domain** page, enter a keyword to search for required information.

Step 4 In the lower left area of the function pane, view capacity, owning storage pool, and disk information about the disk domain. You can delete or expand the owning storage pool.

----End

5.2.2 Modifying a Disk Domain

This operation enables you to modify the name and description of a disk domain.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Provisioning** > **Disk Domain**.

Step 3 Modify the properties of a disk domain.

1. Select the disk domain you want to modify and click **Properties**.

   The **Properties of Disk Domain** dialog box is displayed.
2. Click **General** tab.
3. Rename and describe the disk domain.
4. Click **OK**.

   The **Execution Result** dialog box is displayed, indicating that the operation succeeded.
5. Click **Close**.

----End

5.2.3 Expanding a Disk Domain

This operation allows you to increase the capacity of a disk domain.

Prerequisites

Disks used for capacity expansion are available.

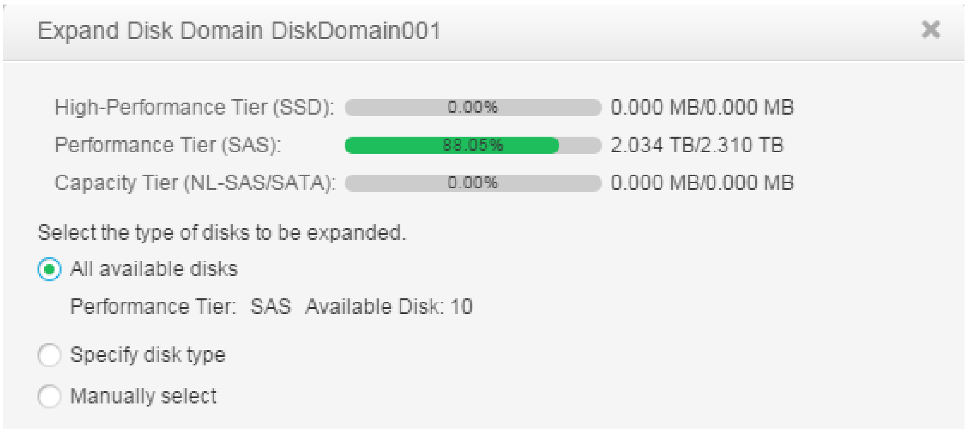
Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Provisioning** > **Disk Domain**.

Step 3 Select the disk domain you want to expand and click **Expand**.

The **Expand Disk Domain** dialog box is displayed.



Expand Disk Domain DiskDomain001

High-Performance Tier (SSD): 0.00% 0.000 MB/0.000 MB

Performance Tier (SAS): 88.05% 2.034 TB/2.310 TB

Capacity Tier (NL-SAS/SATA): 0.00% 0.000 MB/0.000 MB

Select the type of disks to be expanded.

● All available disks

Performance Tier: SAS Available Disk: 10

○ Specify disk type

○ Manually select

Step 4 Select an expansion method.

The following expansion methods are available:

- Select **All available disks** to add all available disks to the disk domain.
- Select **Specify disk type**.
- Select **Manually Select** and click **Select...**. On the **Select Disks** page, add disks from **Available Disks** to **Selected Disks** and click **OK**.

Step 5 Confirm the expansion of the disk domain.

1. Click **OK**.

   The **Success** message box is displayed, indicating that the operation succeeded.
2. Click **OK**.

----End

5.2.4 Viewing Data Distribution in a Disk Domain

This operation enables you to view data distribution in a disk domain.

Prerequisites

A disk domain has been created in the system.

Procedure

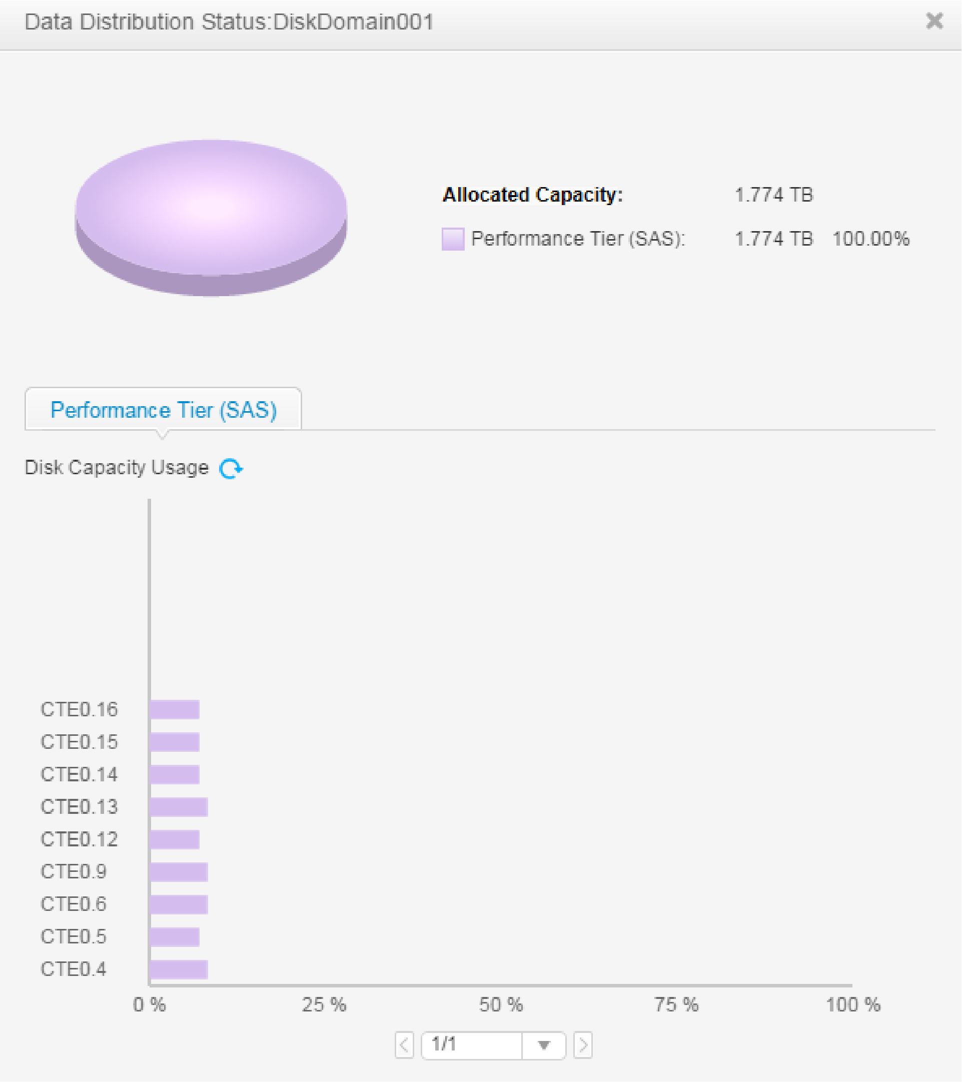
Step 1 Log in to DeviceManager.

Step 2 Choose **Provisioning** > **Disk Domain**.

Step 3 Select the disk domain you want to view.

Step 4 Click **Data Distribution Status**.

The **Data Distribution Status** page is displayed.



Step 5 View data distribution in a disk domain.

- Click **Properties** to view the used capacity and the percentage of the used capacity in each tier.
- Click **Data Distribution Status**, in the lower part, the storage tier tabs allow you to view the percentage of used disk capacity of each storage tier to the total disk capacity.

NOTE

The system refreshes disk capacity usage in each tier every 15 seconds. You can also click ⟳ to manually refresh the information.

----End

5.2.5 Modifying the Hot Spare Policy of a Disk Domain

This operation enables you to modify the hot spare policy of a disk domain.

Precautions

Note the following if you want to modify the hot spare policy of a disk domain:

- If the hot spare policy needs to be modified from **None** to **Low**, or from **Low** to **High**, the remaining capacity of the disk domain cannot be smaller than 10% of the disk domain's total capacity.
- If the hot spare policy needs to be modified from **None** to **High**, the remaining capacity of the disk domain cannot be smaller than 20% of the disk domain's total capacity.

A hot spare policy cannot be modified if the disk domain remaining capacity does not meet the previously described requirements. To modify the hot spare policy successfully, expand the disk domain.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Provisioning** > **Disk Domain**.

Step 3 Modify the properties of a disk domain.

1. Select the disk domain you want to modify and click **Properties**.

   The **Properties of Disk Domain** dialog box is displayed.
2. Click **Hot Spare Policy** tab.
3. Modify the hot spare policy in the disk domain.
4. Click **OK**.

   The security alert dialog box is displayed.

   NOTE

   Only when the level of a hot spare policy is modified from high to low, a **Danger** dialog box is displayed indicating risky operations.
5. Read the content carefully and select **I have read and understand the consequences associated with performing this operation.** and click **OK**.

   The **Execution Result** dialog box is displayed, indicating that the operation succeeded.
6. Click **Close**.

----End

5.2.6 Deleting an Unencrypted Disk Domain

This operation enables you to delete a disk domain that is no longer needed.

Prerequisites

The storage pools in the disk domain have been deleted.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Provisioning** > **Disk Domain**.

Step 3 Delete a disk domain.

1. Select the disk domain you want to delete and click **Delete**.

   The security alert dialog box is displayed.

2. Click **OK**.

   A message is displayed, indicating that the operation succeeded.

3. Click **OK**.

----End

5.3 Managing Storage Pools

A storage pool is created under a disk domain and serves as a container of storage resources. The storage resources used by application servers are all from storage pools.

5.3.1 Viewing Storage Pool Information

This operation enables you to view the information about all the storage pools on a storage system.

Prerequisites

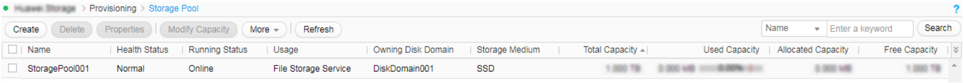
At least one **File Storage Service** type storage pool has been created on the storage system.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Provisioning** > **Storage Pool**.

Step 3 View storage pool information. **Table 5-10** describes storage pool parameters.



□ Name	Health Status	Running Status	Usage	Owning Disk Domain	Storage Medium	Total Capacity	Used Capacity	Allocated Capacity	Free Capacity
□ StoragePool001	Normal	Online	File Storage Service	DiskDomain001	SSD	[redacted]	[redacted]	[redacted]	[redacted]

Table 5-10 Storage pool parameters

Parameter	Description	Setting
Name	Name of a storage pool.	[Example] **StoragePool001**
ID	ID of a storage pool.	[Example] **1**
Health Status	Health status of a storage pool.	[Example] **Normal**
Running Status	Running status of a storage pool.	[Example] **Online**

Parameter	Description	Setting
Usage	Usage of a storage pool. The usages include: ● **Block Storage Service**: for creating LUNs. ● **File Storage Service**: for creating file systems.	[Example] **File Storage Service**
Owning Disk Domain	Name of the disk domain that a storage pool corresponds to.	[Example] **DiskDomain001**
Storage Medium	Disk types in a storage pool.	[Example] **SSD**
Total Capacity	Total capacity of a storage pool.	[Example] **2.000 TB**
Used Capacity	Sum of the allocated capacity and data protection capacity in the storage pool, that is, Used Capacity = Allocated Capacity + Data Protection Capacity. The percentage of **Used Capacity** to **Total Capacity** is displayed on DeviceManager.	[Example] **30.293 GB** **70.23%**
Allocated Capacity	Capacity actually allocated by a storage pool to file systems	[Example] **100.000 MB**
Free Capacity	Free capacity of a storage pool.	[Example] **500 GB**
Data Protection Capacity	Capacity allocated by a storage pool for data protection. NOTE For example, the snapshots are created for file systems within a storage pool. The storage space these snapshots occupy is data protection capacity.	[Example] **30.000 GB**
Migration Triggering Mode	Mode of data migration among storage tiers in a storage pool. NOTE This parameter is only applicable for storage pool with **Block Storage Service**.	[Example] **Manual**

Parameter	Description	Setting
Total Subscribed Capacity	Sum of the preset capacities of all the file systems and capacities of all the file systems' activated snapshots in the storage pool.	[Example] 46.000 GB (0.15%)
Capacity Saved by SmartDedupe	Size of storage space saved by the deduplication of data written to the file system.	[Example] 40.959 GB (50%)
Capacity Saved by SmartCompression	Size of storage space saved by the compression of data written to the file system.	[Example] 40.959 GB (50%)
Capacity Saved by SmartDedupe and SmartCompression	Total storage space saved after data written to file systems is deduplicated and compressed.	[Example] 81.919 GB (50%)

Step 4 Select a storage pool, and in the area below, view the file system information.

----End

5.3.2 Viewing General Information About a Storage Pool

This operation enables you to view the general properties of a storage pool.

Prerequisites

At least one **File Storage Service** type storage pool has been created on the storage system.

Procedure

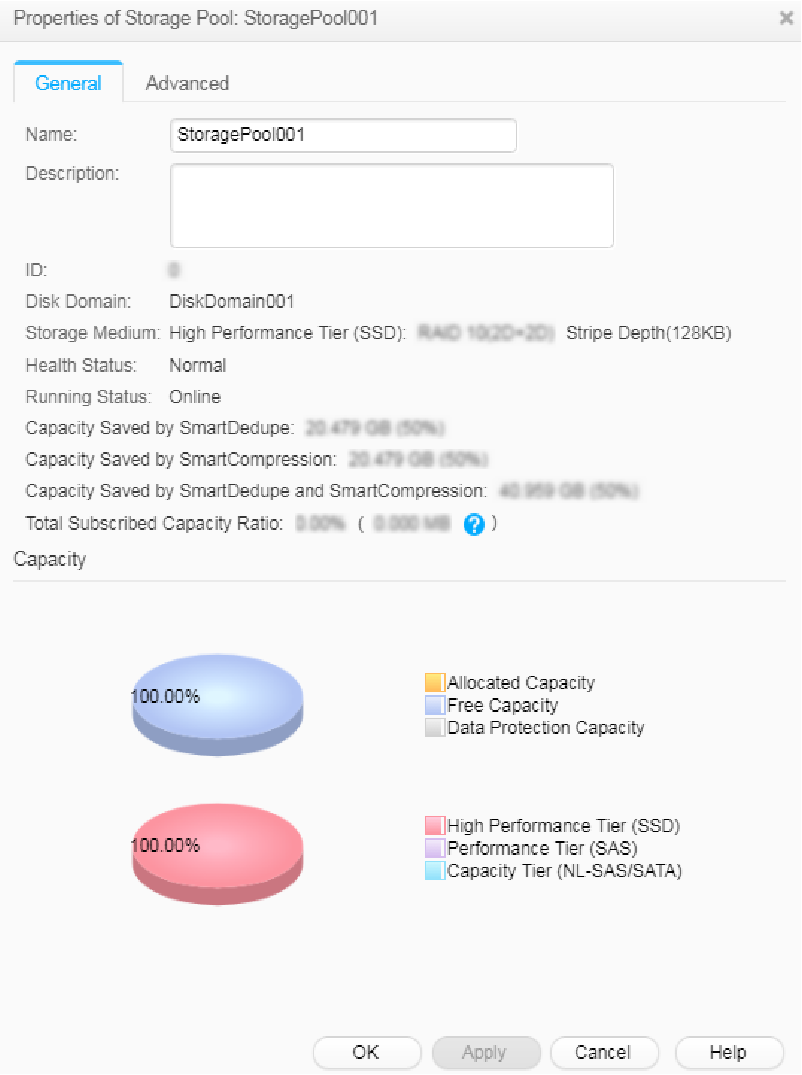
Step 1 Log in to DeviceManager.

Step 2 Choose **Provisioning** > **Storage Pool**.

Step 3 Select the storage pool whose information you want to view and click **Properties**.

The **Storage Pool Properties** dialog box is displayed.

Step 4 View the general properties of the storage pool. **Table 5-11** describes storage pool general parameters.



Properties of Storage Pool: StoragePool001

Name: StoragePool001

Description:

ID: [redacted]

Disk Domain: DiskDomain001

Storage Medium: High Performance Tier (SSD): [redacted] Stripe Depth(128KB)

Health Status: Normal

Running Status: Online

Capacity Saved by SmartDedupe: [redacted]

Capacity Saved by SmartCompression: [redacted]

Capacity Saved by SmartDedupe and SmartCompression: [redacted]

Total Subscribed Capacity Ratio: [redacted] ([redacted] ?)

Capacity

Table 5-11 Storage pool general parameters

Parameter	Description	Setting
Name	Name of a storage pool.	[Example] **StoragePool001**
Description	Description of a storage pool.	[Example] **-**
ID	ID of a storage pool.	[Example] **2**
Disk Domain	Name of the disk domain that a storage pool corresponds to.	[Example] **DiskDomain001**

Parameter	Description	Setting
Storage Medium	Storage tier information about a storage pool, such as disk type, RAID level, and strip depth.	[Example] **Performance Tier (SAS): RAID 5(4D+1P) Strip Depth(128KB)**
Health Status	Health status of a storage pool.	[Example] **Normal**
Running Status	Running status of a storage pool.	[Example] **Online**
Saved Capacity after Deduplication	Size of storage space saved by the deduplication of data written to the file system.	[Example] 40.959 GB (50%)
Saved Capacity after Compression	Size of storage space saved by the compression of data written to the file system.	[Example] 40.959 GB (50%)
Total capacity saved by Deduplication and Compression	Total storage space saved after data written to file systems is deduplicated and compressed.	[Example] 81.919 GB (50%)
Total Subscribed Capacity Ratio	Ratio of the actual capacity occupied by file systems to the total subscribed capacity.	[Example] 0.15% (46.000 GB)
Capacity	Storage pool capacity distribution.	[Example] -

NOTE

The name and description of a storage pool can be changed.

----End

5.3.3 Modifying the Advanced Properties of a Storage Pool

This operation enables you to modify the advanced properties of a storage pool.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Provisioning** > **Storage Pool**.

Step 3 Select the storage pool whose properties you want to modify and click **Properties**.

The **Properties of Storage Pool** dialog box is displayed.

Step 4 Set advanced properties for the storage pool.

1. In the **Properties of Storage Pool** dialog box, click the **Advanced** tab.

   Table 5-12 describes the related parameters.

Table 5-12 Storage pool advanced parameters

Parameter	Description	Setting
Used Capacity Alarm Threshold (%)	If the storage pool contains a file system with value-added service or a thin file system, when the percentage of the used capacity of the storage pool to the total capacity of the storage pool (the used capacity for short as below) reaches the used capacity alarm threshold, the system generates an alarm. The alarm is generated in 3 circumstances: – When the used capacity reaches the used capacity alarm threshold, the system generates an alarm informing that the capacity of storage pool is insufficient. – When the used capacity alarm threshold is no greater than 88 and the used capacity reaches 90%, the system generates an alarm informing that the storage pool is running out. – When the used capacity alarm threshold is greater than 88 and the used capacity reaches (used capacity alarm threshold +2)%, the system generates an alarm informing that the storage pool is running out. NOTE If the used capacity alarm threshold is set as 85, when the used capacity reaches 85%, the system generates an alarm informing that the capacity of storage pool is insufficient, and when the used capacity reaches 90%, the system generates an alarm informing that the storage pool is running out. If the used capacity alarm threshold is set as 91, when the used capacity reaches 93%, the system generates an alarm informing that the storage pool is running out. A proper used capacity alarm threshold helps you monitor the capacity usage of a storage pool.	[Value range] 1 to 95 [Default Value] 80

Parameter	Description	Setting
Data Protection Capacity Alarm Threshold (%)	When ratio the data protection capacity of the storage pool to the total capacity of the storage pool exceeds the capacity alarm threshold, the system generates an alarm.	[Value range] 1 to 100 [Default Value] 100

2. Click **OK**.

   The **Execution Result** dialog box is displayed indicating that the operation succeeded.

3. Click **Close**.

----End

5.3.4 Modifying Capacity of a Storage Pool

When the storage pool capacity is insufficient, you can expand it to meet actual needs. When the storage pool is with surplus capacity, you can reduce it to release storage space.

Prerequisites

- The **Health Status** of the storage pool is **Normal**.
- The reduced capacity must be smaller than maximum capacity for reduction.
- The disk domain has available storage space for capacity expansion of the storage pool

Procedure

Step 1 Log in to DeviceManager.

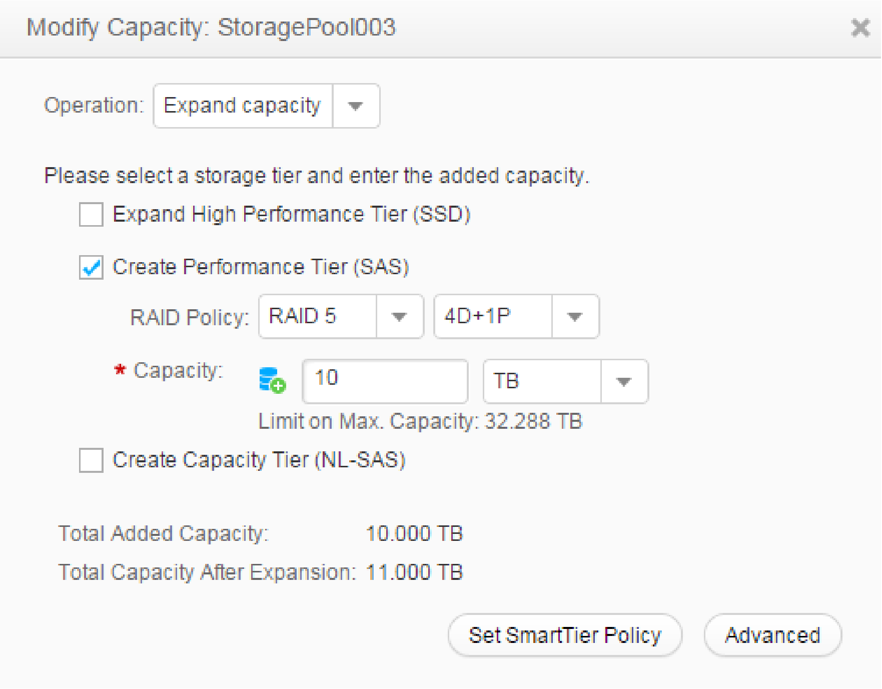
Step 2 Choose **Provisioning** > **Storage Pool**.

Step 3 Select the storage pool you want to expand and click **Modify Capacity**.

The **Modify Capacity** dialog box is displayed.

Step 4 In **Operation**, select the mode of modifying capacity. The modes are **Expand capacity** and **Reduce capacity**.

- Expand the capacity of a storage pool.
  a. Select the storage tier you want to expand or create.
  b. To create a storage tier, configure the RAID policy and in **Capacity**, enter the capacity of the storage tier.



Modify Capacity: StoragePool003

Operation: Expand capacity

Please select a storage tier and enter the added capacity.

□ Expand High Performance Tier (SSD)

☑ Create Performance Tier (SAS)

RAID Policy: RAID 5 4D+1P

* Capacity: 10 TB

Limit on Max. Capacity: 32.288 TB

□ Create Capacity Tier (NL-SAS)

Total Added Capacity: 10.000 TB

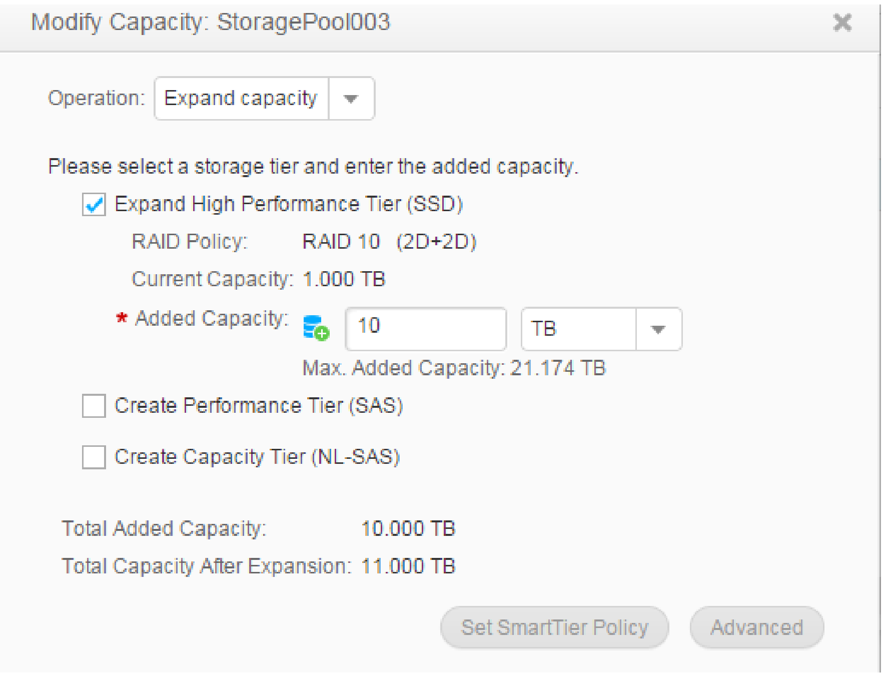
Total Capacity After Expansion: 11.000 TB

Table 5-13 Storage tier parameters

Parameter	Description	Setting
RAID Policy	RAID level. The system supports RAID 0, RAID 1, RAID 10, RAID 3, RAID 5, RAID 50, and RAID 6. **NOTE** RAID 0 only supports configuration in CLI mode. For details, see the *Command Reference* of the corresponding product model.	Select a RAID policy based on the planned solution. The default RAID policy of a storage tier varies with the number of disks allocated to the storage tier. ■ If the number of disks allocated to a storage tier is smaller than 10: ○ Default RAID policy of the high performance tier: RAID 10 ○ Default RAID policy of the performance tier: RAID 5 (4D+1P) ○ Default RAID policy of the capacity tier: RAID 6 (4D+2P) ■ If the number of disks allocated to a storage tier is equal to 10: ○ Default RAID policy of the high performance tier: RAID 10 ○ Default RAID policy of the performance tier: RAID 5 (8D+1P) ○ Default RAID policy of the capacity tier: RAID 6 (4D+2P) ■ If the number of disks allocated to a storage tier is greater than 10: ○ Default RAID policy of the high

Parameter	Description	Setting
		performance tier: RAID 10 ○ Default RAID policy of the performance tier: RAID 5 (8D+1P) ○ Default RAID policy of the capacity tier: RAID 6 (8D+2P) **NOTE** If the number of SSDs in a disk domain is two or three, you are advised to configure the corresponding high-performance tier to RAID 1 (2D).
Capacity	The capacity that the storage tier provides for the storage pool. Two capacity levels are provided: TB, GB.	The capacity must be not larger than the available capacity of the storage tier.

c. To expand a storage tier, in **Added Capacity**, enter the added capacity of the storage tier.


Modify Capacity: StoragePool003

Operation: Expand capacity

Please select a storage tier and enter the added capacity.

☑ Expand High Performance Tier (SSD)

RAID Policy: RAID 10 (2D+2D)

Current Capacity: 1.000 TB

* Added Capacity: 10 TB

Max. Added Capacity: 21.174 TB

□ Create Performance Tier (SAS)

□ Create Capacity Tier (NL-SAS)

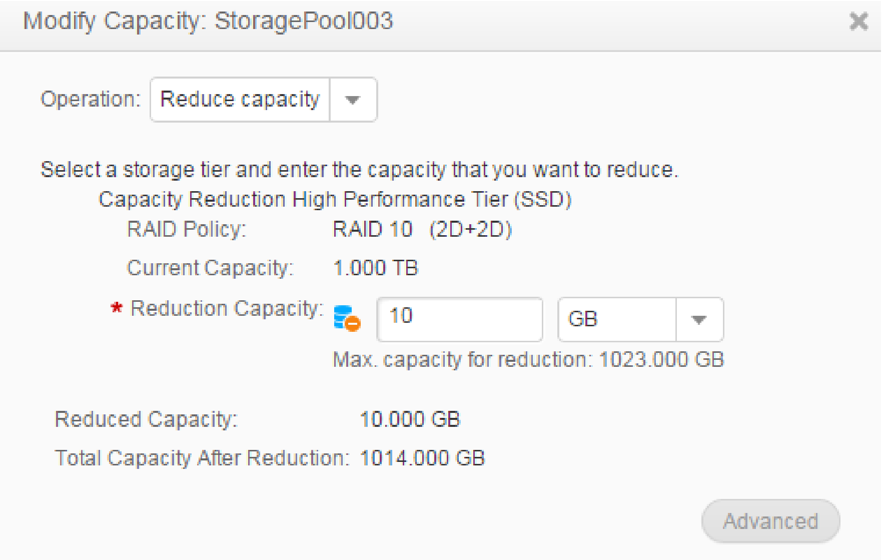
Total Added Capacity: 10.000 TB

Total Capacity After Expansion: 11.000 TB

- Reduce the capacity of a storage pool.

a. Select the storage tier you want to reduce.

b. In **Reduction Capacity**, enter the capacity of the storage tier to be reduced.



Modify Capacity: StoragePool003

Operation: Reduce capacity

Select a storage tier and enter the capacity that you want to reduce.

Capacity Reduction High Performance Tier (SSD)

RAID Policy: RAID 10 (2D+2D)

Current Capacity: 1.000 TB

* Reduction Capacity: 10 GB

Max. capacity for reduction: 1023.000 GB

Reduced Capacity: 10.000 GB

Total Capacity After Reduction: 1014.000 GB

NOTE

- You can create a storage tier or expand the existing storage tier to expand storage pools.
- You can configure RAID policy only for new created storage tier. For the storage tier exists in the storage pool, you cannot modify its RAID policy.
- The number of RAID data disks of different storage pool tiers must be a multiple of 1, 2, 4, or 8.

Step 5 **Optional:** If there are multiple storage tiers, you are advised to set a SmartTier policy. The policy enables data to migrate among different types of disks, optimizing storage performance distribution. **Table 5-14** lists SmartTier policies of a storage pool.

Table 5-14 SmartTier policy of the storage pool

Parameter	Description	Setting
Service Monitoring Period	Period of time during which the service is monitored and hotspot statistics is collected after you select **Enable I/O monitoring**. The statistics serves as guidance for data to migrate among different storage tiers. You can specify the period by setting days, **Start Time**, and **Duration**.	[Default value] **I/O monitoring disabled**

Parameter	Description	Setting
Data Migration Plan	The trigger policy of data relocation between the storage layers in a storage pool. The policies include: ● Manual: You must manually trigger the data relocation among storage tiers. The data relocation process is transparent to application servers. Manual data relocation can be performed anytime. ● Periodical: You must specify the start time and duration of data relocation for the storage system to perform data relocation automatically at the specified time. This reduces the management cost and complexity. The data relocation process is transparent to application servers. Automatic data relocation is performed only at the specified time.	[Default value] **Manual**

NOTE

- If **Data Migration Plan** is set to **Periodical**, I/Os are monitored on a 7x24 basis by default.
- SmartTier policy is only applicable when **Usage** of a storage pool is configured as **Block Storage Service**.
- If the remaining capacity in a storage pool is equal to or smaller than 10% of the total capacity, data does not migrate in the storage pool.

Step 6 **Optional:** If there are multiple storage tiers, click **Advanced** to set the stripe depth.

Click **Advanced**, the **Modify Capacity** dialog box is displayed. **Table 5-15** lists related parameters.

Table 5-15 Modify Capacity

Parameter	Description	Setting
Strip Depth	Strip refers to continuous data that is divided into data blocks of the same size and data blocks are distributed on different disks of storage devices. In this way, I/O loads are balanced among disks, improving read/write performance. Strip depth refers to strip size, indicating the size of data blocks on each disk. Smaller strip size indicates smaller data blocks. These data blocks are distributed on more disks, improving transmission performance. However, more time is required to find different data blocks, decreasing disk locating performance. On the contrary, fewer data blocks indicate lower transmission performance but higher disk locating performance. The value of this parameter can be: ● System auto select The system selects the optimal strip depth based on the RAID policy of the storage tier and data migration granularity. ● 32 KB ● 64 KB ● 128 KB 128 KB is recommended for random read/write services (such as in database scenarios). ● 256 KB ● 512 KB 512 KB is recommended for sequential read/write services (such as media asset scenarios)	[Default value] System auto select

Parameter	Description	Setting
	NOTE The parameter value cannot be changed after being determined.	

Step 7 Confirm the capacity modification of the storage pool.

1. Click **OK**.

   The security alert dialog box is displayed.

2. Confirm the information in the dialog box and select **I have read and understand the consequences associated with performing this operation.**.
3. Click **OK**.

   The **Execution Result** dialog box is displayed indicating that the operation succeeded.

4. Click **Close**.

----End

5.3.5 Deleting a Storage Pool

This operation enables you to delete an unwanted storage pool.

Prerequisites

Before deleting a storage pool, ensure that file systems in the storage pool have been deleted.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Provisioning** > **Storage Pool**.

Step 3 Delete a storage pool.

1. Select the storage pool you want to delete and click **Delete**.

   The security alert dialog box is displayed.

2. Click **OK**.

   The **Success** dialog box is displayed, indicating that the operation succeeded.

3. Click **OK**.

----End

5.4 Managing a File System

This section introduces how to manage and maintain a file system that has been configured.

5.4.1 Viewing File System Information

You can view information about basic file system information.

Prerequisites

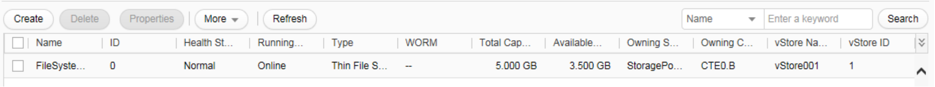
At least one file system is created.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Provisioning** > **File System**.

Step 3 View basic file system information. **Table 5-16** describes the related parameters.



☐	Name	ID	Health St...	Running...	Type	WORM	Total Cap...	Available...	Owning S...	Owning C...	vStore Na...	vStore ID
☐	FileSyste...	0	Normal	Online	Thin File S...	--	5.000 GB	3.500 GB	StoragePo...	CTE0.B	vStore001	1

Table 5-16 Basic file system information

Parameter	Description	Value
Name	Name of the file system.	[Example] FileSystem001
ID	ID of the file system.	[Example] 1
Health Status	Health status of the file system.	[Example] Normal
Running Status	Running status of the file system.	[Example] Online
Type	Configuration type of the file system.	[Example] Thick file system
WORM	WORM mode of the file system.	[Example] Regulatory compliance
Total Capacity	Total capacity of the file system.	[Example] 1.000 GB
Available Capacity	Available capacity of the file system.	[Example] 500.000 MB
Owning Storage Pool	Owning storage pool of the file system.	[Example] StoragePool000
Owning Controller	Owning controller of the file system.	[Example] CTE0.A
vStore Name	Name of the vStore.	[Example] vStore001

Parameter	Description	Value
vStore ID	ID of the vStore.	[Example] 1
Clone	Whether the file system is a clone.	[Example] No

Step 4 Select a file system. In the function pane, view information about **Quota Tree**, **Quota**, **Snapshot**, **Remote Replication**, **HyperMetro**, and **HyperVault**.

----End

5.4.2 Modifying General Properties of a File System

This operation enables you to modify general properties of a file system, such as names and descriptions.

Prerequisites

At least one file system is created.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Provisioning** > **File System**.

Step 3 Select a file system whose general properties you want to modify and click **Properties**.

The **File System Properties** dialog box is displayed.

Step 4 Modify general properties of the file system.

1. In the **Name** text box, enter a file system name.

   NOTE

   The name must meet the following requirements so that the snapshot is available to host applications:

   – The name must be unique.

   – For V300R006C00 and V300R006C10, the name can only contain letters, digits, and underscores (_).

   – The name can be 1 to 255 characters in length.

2. In the **Description** text box, enter the description of the file system.
3. Change the file system type in the **Type** drop-down list.
   - Thin file system:

     A thin file system is configured with an initial capacity when being created and dynamically allocated required storage resources when its available capacity is insufficient.
   - Thick file system:

     A thick file system is allocated a fixed capacity of storage resources according to the capacity specified when being created using the thin provisioning technology.

NOTE

Clone file system or file system that enabled SmartDedupe & SmartCompression feature do not support modifying the file system type.

4. Click **Apply**.

   The **Execution Result** dialog box is displayed indicating that the operation succeeded.

5. Click **Close**.

Step 5 Modify snapshot space ratio.

1. In the **Snapshot Space Ratio (%)** text box, enter percentage of the file system snapshot space to the file system space.

   NOTE

   The value is an integer ranging from 0 to 50.

2. Click **OK**.

   The **Execution Result** dialog box is displayed indicating that the operation succeeded.

3. Click **Close**.

Step 6 Click **OK**.

----End

5.4.3 Modifying a Periodic Snapshot Policy

This operation enables you to modify the time policy of a file system periodic snapshot, ensuring the snapshot is created at a specified time.

Prerequisites

At least one file system is created.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Provisioning** > **File System**.

Step 3 Select a file system whose general properties you want to modify and click **Properties**.

The **File System Properties** dialog box is displayed.

Step 4 Modify policy of the periodic snapshot.

1. Click **Timing Snapshot Policy** tab.
2. **Optional:** Select **Hours** and **Minute** to execute the timing snapshot. Begin calculating at 0 o'clock everyday. For example, if **Every 6 Hours 10 Minute** is specified, then timing snapshot will be executed at **06:10**, **12:20**, and **18:30** every day.
3. **Optional:** Select **Daily** and set **Hours** and execution start time. For example, if **Hours: 01:00** and **17:00** are specified, and **Minute: 1** is specified, then timing snapshot will be executed at **01:01** and **17:01** every day.
4. **Optional:** Select **Weekly** and set **Week** and execution start time. For example, if **Week: Day 3**, and **Time: 11:50** is specified, then timing snapshot will be executed at **11:50** on **Sunday** and **Wednesday** every week.

5. **Optional:** Select **Monthly** and set **Date** and execution start time. For example, if **Date: 2** and **30** are specified, and **Time: 12:10** is specified, then timing snapshot will be executed at **12:10** on dates **2** and **30** every month.

Step 5 Click **OK**.

The **Execution Result** dialog box is displayed indicating that the operation succeeded.

Step 6 Click **Close**.

----End

5.4.4 Modifying a SmartQoS Policy

This operation enables you to modify the SartPartition policy of a file system and view details about the policy.

Prerequisites

- At least one file system is created.
- SmartQoS license is purchased and activated.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Provisioning** > **File System**.

Step 3 Select a file system whose SmartQoS policy you want to modify and click **Properties**.

The **File System Properties** dialog box is displayed.

Step 4 Modify the SmartQoS policy.

1. Click the **SmartQoS** tab.
2. In **Priority Control**, select a priority policy.

   The value can be **Low**, **Medium**, or **High**. By default, **Low** is selected.
3. In **Traffic Control**, select a control policy.

   NOTE

   Select **None** to disable traffic control.
4. Click **OK**.

   The **Execution Result** dialog box is displayed indicating that the operation succeeded.

Step 5 Click **Close**.

----End

5.4.5 Modifying a SmartPartition Policy

You can modify the SmartPartition policy of a file system and view details about the policy.

Prerequisites

At least one file system is created.

Context

Reducing the capacity of SmartPartition is not supported when the SmartPartition partition is allocated to the file system.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Provisioning** > **File System**.

Step 3 Select a file system whose SmartPartition policy you want to modify and click **Properties**.

The **File System Properties** dialog box is displayed.

Step 4 Modify the SmartPartition policy.

1. Click the **SmartPartition** tab.
2. In **SmartPartition**, select SmartPartition to which the file system belongs.

   NOTE

   Click **Properties** and set SmartPartition control properties based on site requirements.
3. Click **OK**.

   The **Warning** dialog box is displayed.
4. Select **I have read and understand the consequences associated with performing this operation** and click **OK**.

   The **Execution Result** message box is displayed indicating that the operation succeeded.

Step 5 Click **Close**.

----End

5.4.6 Viewing SmartCache Information

This operation enables you to view details about the SmartCache policy.

Prerequisites

A SmartCache partition has been created for the file system.

NOTE

SmartCache is not supported by 2000F, 5000F, 6000F, 18000F series storage systems.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Provisioning** > **File System**.

Step 3 Select the file system whose properties you want to view and click **Properties**.

The **File System Properties** dialog box is displayed.

Step 4 Click **SmartCache** tab.

Step 5 View the information of the SmartCache information. The related parameters are shown in **Table 5-17**.

Table 5-17 SmartCache Parameters

Parameter	Description
SmartCache Partition	Name of the SmartCache partition.
ID	ID of the SmartCache partition.
Expect Capacity	The capacity of the SmartCache partition you expect to use.
Used Capacity	Used capacity of the SmartCache partition.
SSD Real-Time Hit Ratio (%)	Every 10 seconds, the ratio of read I/O hits of data in the SmartCache partition to the total read I/O requests the SmartCache partition receives. For example, the SmartCache partition received 10 read I/O requests, 5 of them obtain the data from the partition, therefore the SSD real-time hit ratio is 50%.

----End

5.4.7 Modifying a SmartDedupe&SmartCompression Policy

You can modify the deduplication or data compression policy of a file system and learn about deduplication amount or data reduction amount of the file system. OceanStor 2200 V3 storage system does not support this function.

Prerequisites

A file system with thin features exists and the SmartDedupe license file is imported.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Provisioning** > **File System**.

Step 3 Select a file system whose SmartDedupe policy you want to modify, and click **Properties**.

The **File System Properties** dialog box is displayed.

Step 4 Choose **More** > **SmartDedupe&SmartCompression** tab.

Step 5 Modify data compression and deduplication policies.

Table 5-18 and **Table 5-19** describe the related parameters.

Table 5-18 Data compression parameters

Parameter	Description	Value
Enable data compression	Whether to enable the data compression function.	[Example] Enable data compression
Saved Space after Compression	Storage space saved by using data compression. NOTE This parameter is available only after you select **Enable data compression**.	[Example] 10.000 MB(%)

Table 5-19 Deduplication parameters

Parameter	Description	Value
Enable deduplication	Whether to enable the deduplication function.	[Example] Enable deduplication
Saved Space after Deduplication	Storage space saved by using deduplication. NOTE This parameter is available only after you select **Enable deduplication**.	[Example] 10.000 MB(1%)

Step 6 Click **OK**.

The **Execution Result** dialog box is displayed.

Step 7 Click **Close** to finish modifying data compression and deduplication policies.

----End

5.4.8 Modifying Advanced Properties of a File System

This operation enables you to modify advanced properties of a file system.

Prerequisites

At least one file system is created.

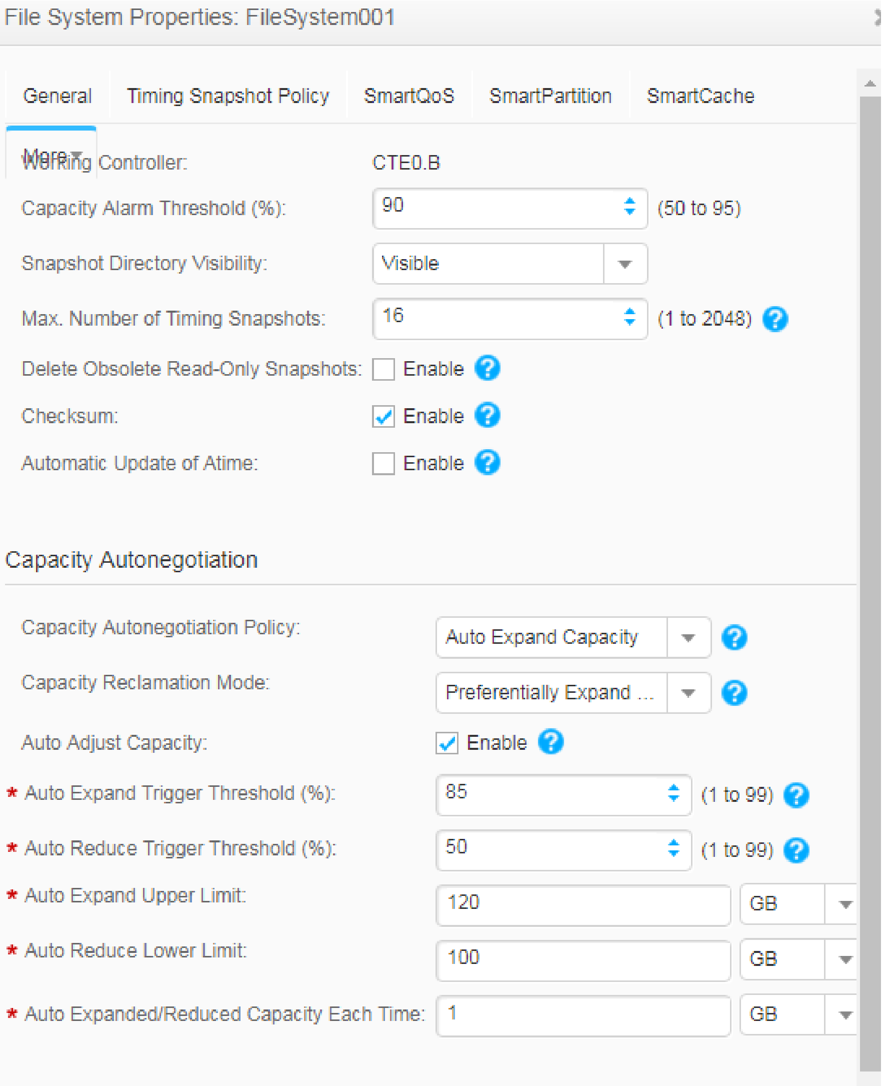
Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Provisioning** > **File System**.

Step 3 Select a file system whose advanced properties you want to modify and click **Properties**.

The **File System Properties** dialog box is displayed.



File System Properties: FileSystem001

Working Controller: CTE0.B

Capacity Alarm Threshold (%): 90 (50 to 95)

Snapshot Directory Visibility: Visible

Max. Number of Timing Snapshots: 16 (1 to 2048)

Delete Obsolete Read-Only Snapshots: □ Enable

Checksum: ☑ Enable

Automatic Update of Atime: □ Enable

Capacity Autonegotiation

Capacity Autonegotiation Policy: Auto Expand Capacity

Capacity Reclamation Mode: Preferentially Expand ...

Auto Adjust Capacity: ☑ Enable

* Auto Expand Trigger Threshold (%): 85 (1 to 99)

* Auto Reduce Trigger Threshold (%): 50 (1 to 99)

* Auto Expand Upper Limit: 120 GB

* Auto Reduce Lower Limit: 100 GB

* Auto Expanded/Reduced Capacity Each Time: 1 GB

Step 4 Change advanced properties of the file system.

1. Select **Advanced** in the **More** tab.
2. Change advanced properties of the file system. **Table 5-20** describes related parameters.

Table 5-20 Advanced properties of a file system

Parameter	Description	Value
Capacity Alarm Threshold (%)	Alarm threshold of the file system capacity.	[Value range] The value is an integer ranging from 50 to 95. [Example] 90 [Default] 90

Parameter	Description	Value
Snapshot Directory Visibility	Specifies whether snapshot directories are visible.	[Value range] The value can be **Visible** or **Invisible**. [Example] Visible [Default] Visible
Snapshot Space Ratio (%)	Space ratio of the file system snapshot.	[Value range] The value is an integer ranging from 0 to 50. [Example] 20 [Default] 20
Max. Number of Timing Snapshots	Upper limit of the file system timing snapshots. When the number of created snapshots reaches the upper limit, the system automatically deletes the earliest timing snapshots.	[Value range] The value is an integer ranging from 1 to 2048. [Example] 16 [Default] 16
Delete Obsolete Read-Only Snapshots	Specifies whether **Delete Obsolete Read-Only Snapshots** is enabled. When used space of a file system reaches the Capacity alarm threshold and used space of snapshots is larger than reserved space for snapshots, the system automatically deletes the earliest read-only snapshots.	[Example] Enable [Default] Disable
Checksum	Specifies whether **Checksum** is enabled. This function is used to check data integrity. When it is enabled, checksum will be automatically calculated when data is being written, ensuring integrity of the data to be accessed.	[Example] Enable [Default] Enable

Parameter	Description	Value
Automatic Update of Atime	Specifies whether **Automatic Update of Atime** is enabled. Atime is a time when file systems are accessed. After this function is enabled, Atime will be updated every time data on file systems is accessed.	[Example] Enable [Default] Disable
Capacity Autonegotiation Policy	A storage system supports the following capacity autonegotiation policies: – **Not Use Capacity Autonegotiation**: The storage capacity used by a file system is fixed and is not flexibly adjusted by the storage system. – **Auto Expand Capacity**: increases file system capacity and meets users' requirements in data write when the available space of a file system is about to run out and the storage pool has available space. – **Auto Reduce or Expand Capacity**: The storage system automatically adjusts the file system capacity based on file system space usage. When the available space of a file system is about to run out and the storage pool has available space, automatic capacity expansion will be used to increase file system capacity. When the file system's storage space is released, it can be reclaimed into a storage pool and used by other file systems in data write requests.	[Example] Auto Expand Capacity [Default] Not Use Autonegotiation

Parameter	Description	Value
Capacity Reclamation Mode	A storage system supports the following capacity reclamation modes: – **Preferentially Expand Capacity**: Expand the capacity to increase the file system capacity. – **Preferentially Delete Old Snapshot**: Delete old snapshots to reclaim space for increasing the file system capacity. If HyperReplication and HyperMetro are configured for storage systems, the capacity autonegotiation policy of the primary storage system will be synchronized to the secondary storage system. If Preferentially Delete Old Snapshot is adopted, ensure that **Delete Obsolete Read-Only Snapshots** is enabled for the secondary storage system.	[Example] Preferentially Expand Capacity [Default] Preferentially Expand Capacity
Auto Adjust Capacity	After you select **Auto Adjust Capacity**, automatic capacity expansion or reduction policy for a file system will take effect during the service running.	[Example] Enable [Default] Enable
Auto Expand Trigger Threshold (%)	When the ratio of the used capacity to the total capacity of the file system is greater than the preset value, the storage system automatically triggers file system capacity expansion.	[Value range] The value is an integer ranging from 1 to 99. [Example] 85 [Default] 85
Auto Reduce Trigger Threshold (%)	When the ratio of the used capacity to the total capacity of the file system is smaller than the preset value, the storage system automatically triggers file system space reclamation and reduces file system capacity.	[Value range] The value is an integer ranging from 1 to 99. [Example] 50 [Default] 50

Parameter	Description	Value
Auto Expand Upper Limit	Set the auto expand upper limit.	[Value range] The value is an integer ranging from file system capacity to 16PB. [Example] 120GB [Default] File system capacity * 120%
Auto Reduce Lower Limit	Set the auto reduce lower limit.	[Value range] The value is an integer ranging from 1GB to **Auto Expand Upper Limit**. [Example] 100GB [Default] File system capacity
Auto Expanded/ Reduced Capacity Each Time	Set the auto expanded or reduced capacity for each time.	[Value range] The value is an integer ranging from 64MB to 100GB. [Example] 1GB [Default] 1GB

3. Click **OK**.

   The **Execution Result** dialog box is displayed indicating that the operation succeeded.

Step 5 Click **Close**.

----End

5.4.9 Modifying File System Capacity

This operation expands or reduces file system capacity to meet service requirements.

How to Modify File System Capacity

A user with the super administrator permission can modify file system capacity on DeviceManager and allocate the added capacity to an application server. For details, see **Expanding a File System** and **Shrinking a File System** in the *Capacity Expansion Guide* specific to your product.

NOTE

You can log in to Huawei's technical support website (http://support.huawei.com/enterprise/) and enter the product model + document name in the search box to search for, browse, and download the desired documents.

You can also use this method to search for, browse, and download other involved documents.

5.4.10 Viewing Quota Tree Information

This operation enables you to view detailed quota tree information.

Prerequisites

At least one file system and quota tree are created.

Context

Root Quota Tree is the quota tree created for the file system by default. This quota tree cannot be deleted and you cannot modify its name.

Root Quota Tree is only available when creating user quota or user group quota for file system. It is not available for directory quota.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Provisioning** > **File System**.

Step 3 Select a file system whose quota tree information you want to view. In the **Details** area, click the **Quota Tree** tab.

The quota tree management page is displayed.

Step 4 View quota tree information. **Table 5-21** describes the related parameters.

Table 5-21 Quota tree parameters

Parameter	Description	Value
Name	Name of the quota tree.	[Example] a123456
Quota	Specifies whether quota function is enabled. The value can be **Enable** or **Closed**.	[Example] Enable

----End

5.4.11 Modifying the Properties of a Quota Tree

This operation enables you to modify quota tree properties.

Prerequisites

At least one file system and quota tree are created.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Provisioning** > **File System**.

Step 3 Select a file system whose quota tree properties you want to modify. In the **Details** area, click the **Quota Tree** tab.

Step 4 Select a quota tree whose properties you want to modify and click **Properties**.

The **Quota Tree Property** dialog box is displayed.

Step 5 Modify quota tree properties. Table 5-22 describes the related parameters.

Table 5-22 Quota tree properties

<table>
<tr><th>Parameter</th><th>Description</th><th>Value</th></tr>
<tr><td>Name</td><td>Name of the quota tree.</td><td>[Value range]
● The name must be unique.
● For V300R006C00, the name can only contain letters, digits, and underscores (_).
● For V300R006C10, the name can only contain letters, digits and special characters. Special characters include !"#$ %&'()*+-.;<=>? @[\]^`{_|}~ and spaces. On the CLI, some characters need to be entered as escape characters. For example, \| indicates |, || indicates \, \q indicates ?, and \s indicates spaces.
● The name can be 1 to 127 characters in length.
[Example]
a123456</td></tr>
</table>

Parameter	Description	Value
Quota	After quota is enabled, the system restricts the number of files and file size of quota tree.	[Example] Enable

Step 6 Click **OK**.

The security alert dialog box is displayed.

NOTE

This message will be displayed only after the quota function is enabled.

Step 7 Confirm the information in the dialog box and select **I have read and understand the consequences associated with performing this operation**, click **OK**.

The **Execution Result** dialog box is displayed indicating that the operation succeeded.

Step 8 Click **Close**.

----End

5.4.12 Deleting a Quota Tree

This operation enables you to delete an unnecessary quota tree.

Prerequisites

At least one file system and quota tree are created.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Provisioning** > **File System**.

Step 3 Select a file system whose quota tree you want to delete. In the **Details** area, click the **Quota Tree** tab.

The quota tree management page is displayed.

Step 4 Select the quota tree you want to delete and click **Delete**.

The **Info** dialog box is displayed.

NOTE

You can also right-click the quota tree you want to delete and choose **Delete**.

Step 5 Click **OK**.

The **Execution Result** dialog box is displayed indicating that the operation succeeded.

Step 6 Click **Close**.

----End

5.4.13 Viewing Quota Information

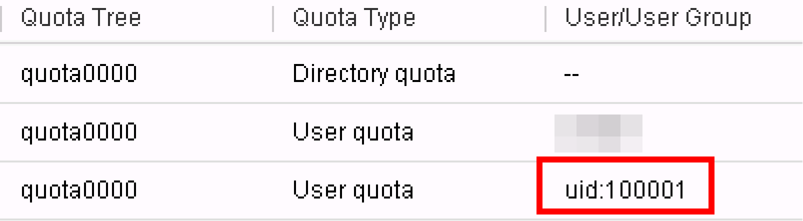
You can view detailed quota information.

Prerequisites

At least one file system and quota are created.

Precautions

If the user or user group of the user or user group quota does not exist, **User/User Group** of the quota displays as **uid:**<*the ID of original user/user group*> (for example, uid:100001), indicating that the quota is invalid. You are advised to delete the quota.



Quota Tree	Quota Type	User/User Group
quota0000	Directory quota	--
quota0000	User quota	[redacted]
quota0000	User quota	uid:100001

Procedure

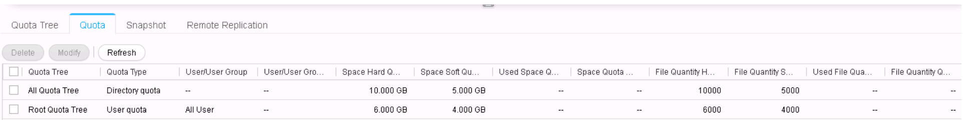
Step 1 Log in to DeviceManager.

Step 2 Choose **Provisioning** > **File System**.

Step 3 Select a file system whose quota information you want to view. In the **Details** area, click the **Quota** tab.

The quota management page is displayed.

Step 4 View quota information. **Table 5-23** describes the related parameters.



Quota Tree	Quota Type	User/User Group	User/User Gro...	Space Hard Q...	Space Soft Qu...	Used Space Q...	Space Quota ...	File Quantity H...	File Quantity S...	Used File Qua...	File Quantity Q...
☐ All Quota Tree	Directory quota	--	--	10.000 GB	5.000 GB	--	--	10000	5000	--	--
☐ Root Quota Tree	User quota	All User	--	6.000 GB	4.000 GB	--	--	6000	4000	--	--

Table 5-23 Quota parameters

Parameter	Description	Value
Quota Tree	Name of the quota tree.	[Example] Root Quota Tree
Quota Type	Type of the file system quota. The value can be **Directory Quota**, **User Quota** or **User Group Quota**.	[Example] User Quota
User/User Group	Name of the user/user group of file system quota.	[Example] All User

Parameter	Description	Value
User/User Group Type	Type of the user/user group of file system quota. The value can be **Local** or **Domain**. The type of the user/user group is **--** when the name of the user/user group is **All user/All Group**.	[Example] --
Space Hard Quota	If the space quota exceeds the hard quota, the system immediately forbids write operations and prevents users from using extra file space.	[Example] 6.000 GB
Space Soft Quota	If the space quota exceeds the soft quota, the system generates an alarm but still allows write operations. After exceeding the hard quota, the system immediately forbids write operations.	[Example] 4.000 GB
Used Space Quota	Used space quota.	[Example] --
Space Quota Usage (%)	Percentage of the used space quota to the hard quota.	[Example] --
File Quantity Hard Quota	If the file quantity quota exceeds the hard quota, the system immediately forbids write operations and prevents users from using extra files.	[Example] 6000
File Quantity Soft Quota	If the file quantity quota exceeds the soft quota, the system generates an alarm but still allows write operations. After exceeding the hard quota, the system immediately forbids write operations.	[Example] 6000
Used File Quantity Quota	Used file quantity quota	[Example] --
File Quantity Quota Usage (%)	Percentage of the used file quantity quota to the hard quota.	[Example] --

----End

5.4.14 Modifying a Quota

This operation enables you to modify quota properties.

Prerequisites

At least one file system and quota are created.

Procedure

Step 1 Log in to DeviceManager.

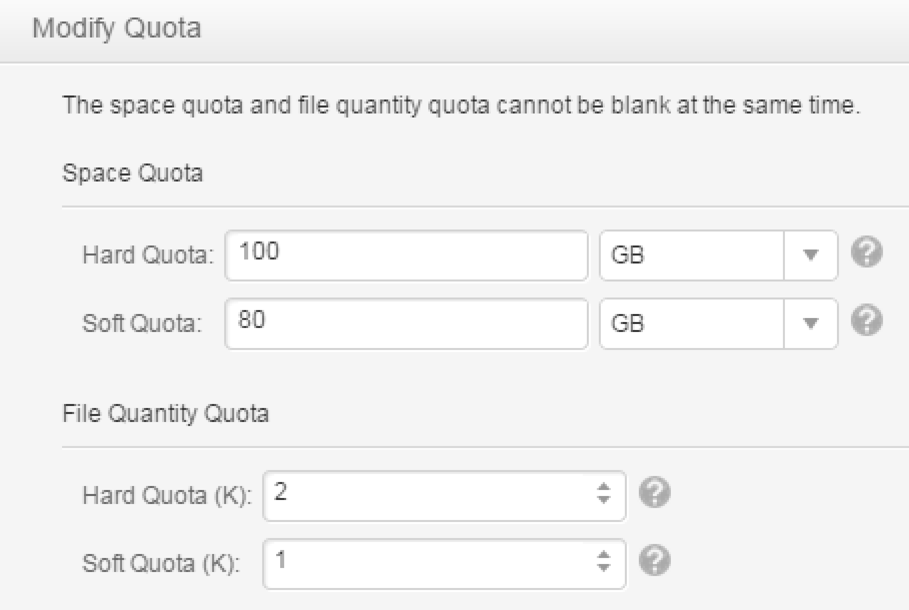
Step 2 Choose **Provisioning** > **File System**.

Step 3 Select a file system whose quota properties you want to modify. In the **Details** area, click the **Quota** tab.

Step 4 Select a quota whose properties you want to modify and click **Modify**.

The **Modify Quota** dialog box is displayed.

Step 5 Modify quota properties. Table 5-24 describes the related parameters.



Modify Quota

The space quota and file quantity quota cannot be blank at the same time.

Space Quota

Hard Quota: 100 GB

Soft Quota: 80 GB

File Quantity Quota

Hard Quota (K): 2

Soft Quota (K): 1

Table 5-24 Quota properties

Parameter	Description	Value
Hard Quota	If the space quota exceeds the hard quota, the system immediately forbids write operations and prevents users from using extra file space.	[Value range] The value must be greater than the space soft quota, and smaller than or equal to **Maximum capacity of a file system**. NOTE ● You can query **Maximum capacity of a file system** in section "Software Specifications" in the *Product Description* specific to your product. ● The space quota is not limited by the file system capacity, and can be greater than or smaller than the file system capacity. [Example] 100 GB
Soft Quota	If the space quota exceeds the soft quota, the system generates an alarm but still allows write operations. After exceeding the hard quota, the system immediately forbids write operations.	[Value range] The value must be smaller than the space hard quota. If the space hard quota is not entered, the value must be smaller than or equal to **Maximum capacity of a file system**. NOTE ● You can query **Maximum capacity of a file system** in section "Software Specifications" in the *Product Description* specific to your product. ● The space quota is not limited by the file system capacity, and can be greater than or smaller than the file system capacity. [Example] 80 GB
Hard Quota (K)	If the file quantity quota exceeds the hard quota, the system immediately forbids write operations and prevents users from using extra files. The unit of the hard quota is set to **K**.	[Value range] The value must be greater than the soft quota of file quantity, and smaller than or equal to 2,000,000. [Example] 2

Parameter	Description	Value
Soft Quota (K)	If the file quantity quota exceeds the soft quota, the system generates an alarm but still allows write operations. After exceeding the hard quota, the system immediately forbids write operations. The unit of the soft quota is set to **K**.	[Value range] The value must be smaller than the hard quota of file quantity. If the hard quota of file quantity is not specified, the value must be smaller than or equal to 2,000,000. [Example] 1

Step 6 Click **OK**.

The **Success** dialog box is displayed indicating that the operation succeeded.

Step 7 Click **OK**.

----End

5.4.15 Deleting a Quota

This operation enables you to delete an unnecessary quota.

Prerequisites

At least one file system and quota are created.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Provisioning** > **File System**.

Step 3 Select a file system whose quota you want to delete. In the **Details** area, click the **Quota** tab.

The quota management page is displayed.

Step 4 Select the quota you want to delete and click **Delete**.

The **Warning** dialog box is displayed.

Step 5 Confirm the information in the dialog box and select **I have read and understand the consequences associated with performing this operation.**, click **OK**.

The **Execution Result** dialog box is displayed indicating that the operation succeeded.

Step 6 Click **Close**.

----End

5.4.16 Deleting a File System

This operation enables you to delete an unnecessary file system.

Prerequisites

Services on the file system that you want to delete have been stopped, the file system is not shared, and no value-added feature is configured for it.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Provisioning** > **File System**.

Step 3 Select a file system that you want to delete and click **Delete**.

The **Warning** dialog box is displayed.

Step 4 Confirm the information in the dialog box and select **I have read and understand the consequences associated with performing this operation.**, click **OK**.

The **Execution Result** dialog box is displayed indicating that the operation succeeded.

Step 5 Click **Close**.

----End

5.5 Managing an NFS Share

After an NFS share is configured for a storage system, you need to manage and maintain the NFS share. This section describes how to manage an NFS share.

5.5.1 Viewing NFS Share Information

You can view NFS share information to understand NFS share lists, clients, and share options.

Prerequisites

An NFS share has been created.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Provisioning** > **Share** > **NFS (Linux/UNIX/MAC)**.

Step 3 In NFS share list, view the NFS share information. **Table 5-25** describes the related parameters.

Table 5-25 NFS share information

Parameter	Description
Share Name	Name of the NFS share.
Share Path	Path of the NFS share.

Parameter	Description
ID	ID of the NFS share.
Description	Description of the NFS share.
Character Encoding	Clients communicate with the storage system using codes. Codes configured on the NFS share should be the same as that of the client. These codes apply to names and metadata of shared files, but do not change the codes of file data. Codes include: ● UTF-8 International code set ● EUC-JP euc-j*[ja] code set ● JIS JIS code set ● S-JIS cp932*[ja_jp.932] code set ● ZH Simplified Chinese code set, in compliance with GB2312 ● GBK Simplified Chinese code set, in compliance with GB2312 ● EUC-TW Traditional Chinese code set, in compliance with CNS11643 ● BIG5 cp950 traditional Chinese code set ● DE German character set, in compliance with ISO8859-1 ● PT Portuguese character set, in compliance with ISO8859-1 ● ES Spanish character set, in compliance with ISO8859-1 ● FR French character set, in compliance with ISO8859-1 ● IT Italian character set, in compliance with ISO8859-1 ● KO cp949 Korean code set

Step 4 In NFS share list, select an NFS share. In **Client Information**, check the permission of the client for this NFS share. The related parameters are shown in **Table 5-26**.

Table 5-26 Client Information

Parameter Name	Description
Name	Name or service IP address of the NFS share client.
Type	Client type of the NFS share. Types include: ● Host Applicable to the client in non-domain environment. ● Network group Applicable to client in LDAP or NIS domain.
Permission Level	The permission for client to access the NFS share. The permissions include: ● Read-only Only reading the files in the share is allowed. ● Read-write Any operation is allowed.
ID	Client ID of the NFS share.

----End

5.5.2 Modifying the Properties of an NFS Share

This operation enables you to modify the description of an NFS share.

Prerequisites

An NFS share has been created.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Provisioning** > **Share** > **NFS (Linux/UNIX/MAC)**.

Step 3 Select the NFS share whose properties you want to modify and click **Properties**.

The **NFS Share Properties** dialog box is displayed.

Step 4 Modify the NFS share information.

NOTE

Parameters for an NFS GNS share cannot be modified.

Table 5-27 describes the related parameters.

Table 5-27 Parameters for an NFS share

Parameter	Description	Value
Description	Description about the NFS share.	[Value range] Contains 0 to 255 characters. [Example] Share for user 1.

Parameter	Description	Value
Character Encoding	Clients communicate with the storage system using codes. Codes configured on the NFS share should be the same as that of the client. These codes apply to names and metadata of shared files, but do not change the codes of file data. Codes include: ● UTF-8 International code set ● EUC-JP euc-j*[ja] code set ● JIS JIS code set ● S-JIS cp932*[ja_jp. 932] code set ● ZH Simplified Chinese code set, in compliance with GB2312 ● GBK Simplified Chinese code set, in compliance with GB2312 ● EUC-TW Traditional Chinese code set, in compliance with CNS11643 ● BIG5 cp950 traditional Chinese code set ● DE German character set, in compliance with ISO8859-1 ● PT	[Default value] UTF-8

Parameter	Description	Value
	Portuguese character set, in compliance with ISO8859-1 ● ES Spanish character set, in compliance with ISO8859-1 ● FR French character set, in compliance with ISO8859-1 ● IT Italian character set, in compliance with ISO8859-1 ● KO cp949 Korean code set **NOTE** ● The storage system automatically lists codes supported by the file system. ● The following describes method of querying character encoding on clients (for example, in Linux): run the **locale** command to view character encoding of current system.	

Step 5 Confirm that you want to modify the properties of the NFS share.

1. Click **OK**.
   - If **Character Encoding** is modified, the security alert dialog box is displayed. Carefully read the contents of the dialog box, select **I have read and understand the consequences associated with performing this operation.**, and click **OK** to confirm the information. The **Execution Result** dialog box is displayed indicating that the operation succeeded.
   - If only **Description** is modified, the **Execution Result** dialog box will be displayed indicating that the operation succeeded.
2. Click **Close**.

----End

5.5.3 Modifying an NFS Share Client

This section describes how to modify the properties of an NFS share client.

Prerequisites

An NFS share client has been created.

Procedure

Step 1 Log in to DeviceManager.

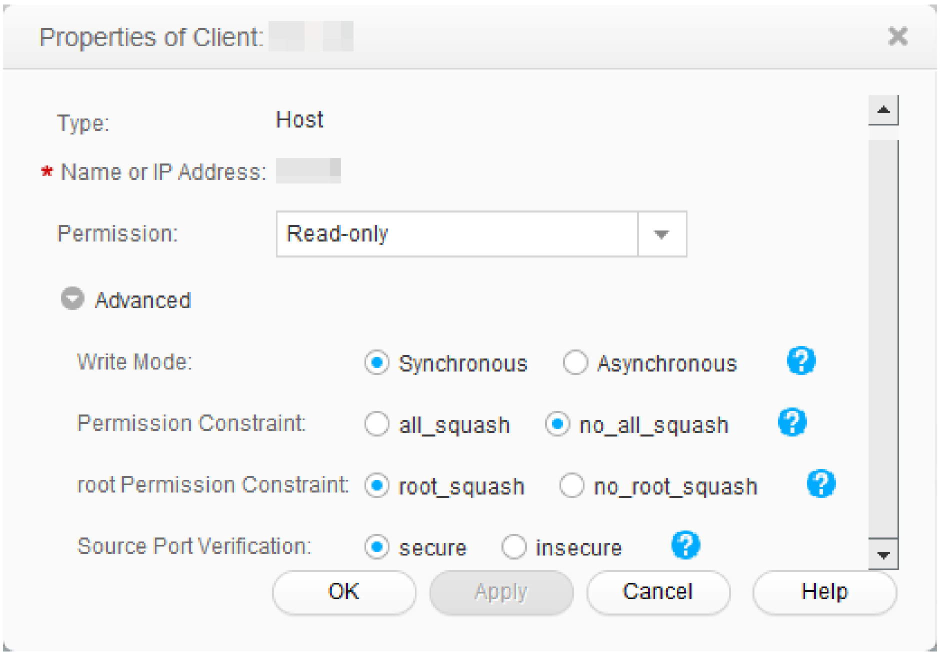
Step 2 Choose **Provisioning** > **Share** > **NFS (Linux/UNIX/MAC)**.

Step 3 Select the NFS share whose client properties you want to modify.

Step 4 In the **Client List** area, select a client whose properties you want to modify and click **Properties**.

The **Properties of Client** dialog box is displayed.

Step 5 Modify the client properties. **Table 5-28** describes related parameters.



Properties of Client: [redacted]

Type: Host

* Name or IP Address: [redacted]

Permission: Read-only

Advanced

Write Mode: ● Synchronous ○ Asynchronous

Permission Constraint: ○ all_squash ● no_all_squash

root Permission Constraint: ● root_squash ○ no_root_squash

Source Port Verification: ● secure ○ insecure

Table 5-28 NFS share client properties

Parameter	Description	Value
Permission	The permission for client to access the NFS share. The permissions include: ● Read-only: Only reading the files in the share is allowed. ● Read-write: Any operation is allowed.	[Default value] Read-only
Write Mode (Optional)	Write mode of the NFS share client. The modes include: ● Synchronous: the data written to the share is written into the disk immediately. ● Asynchronous: the data written to the share is written into the cache first, then into the disk. **NOTE** The asynchronous write mode delivers higher write performance. However, if the client and storage system fail at the same time, there are data loss risks.	[Default value] Synchronous
Permission Constraint (Optional)	Determine whether to retain the user identity (UID) and group ID (GID) of a shared directory. ● all_squash: The user ID (UID) and group ID (GID) of a shared directory are mapped to user **nobody** and are applicable to public directories. ● no_all_squash: The UID and GID of a shared directory are reserved.	[Default value] no_all_squash

Parameter	Description	Value
Root Permission Constraint (Optional)	Control the root permission of a client. ● root_squash: The client cannot access the storage system as user **root**. If a client accesses the storage system as user root, the client will be mapped as user **nobody**. ● no_root_squash: A client can access the storage system as user root and user **root** can fully manage and access the root directory.	[Default value] root_squash
Source Port Verification (Optional)	Determine whether to enable source port verification. ● secure: If secure is selected, clients can use ports 1 to 1023 to access NFS shares. ● insecure: If insecure is selected, clients can use any port to access NFS shares.	[Default value] secure

Step 6 Click **OK**.

----End

5.5.4 Removing an NFS Share Client

This section describes how to remove an NFS share client.

Prerequisites

An NFS share client has been created.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Provisioning** > **Share** > **NFS (Linux/UNIX/MAC)**.

Step 3 Select the NFS share from which you want to remove a client.

The **Client List** page is displayed.

Step 4 Select the NFS share client and click **Remove**.

The security alert dialog box is displayed.

Step 5 Confirm the information in the dialog box and select **I have read and understand the consequences associated with performing this operation.**, Click **OK**.

The **Execution Result** dialog box is displayed indicating that the operation succeeded.

Step 6 Click **Close**.

----End

5.5.5 Deleting an NFS Share

This section describes how to delete an NFS share. After an NFS share is deleted, it becomes unavailable and all services provided using the NFS share are interrupted. Exercise caution when deleting an NFS share.

Prerequisites

No services are running on the NFS share.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Provisioning** > **Share** > **NFS (Linux/UNIX/MAC)**.

Step 3 Select the NFS share and click **Delete**.

The security alert dialog box is displayed.

NOTE

Alternatively, you can right-click the NFS share and choose **Delete**.

Step 4 Confirm the information in the dialog box and select **I have read and understand the consequences associated with performing this operation.**, Click **OK**.

The **Execution Result** dialog box is displayed indicating that the operation succeeded.

Step 5 Click **Close**.

----End

5.5.6 Disabling the NFS Service

By performing this operation, you can disable the NFS service of a storage system.

Precautions

If you disable the NFS service, it will be unavailable. Before performing this operation, ensure that you do not need the NFS service.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Settings** > **Storage Settings** > **File Storage Service** > **NFS Service**.

Step 3 Deselect **Enable NFSv3**. Alternatively, click **Advanced** and deselect **Enable NFSv4**.

Step 4 Click **Save**.

The **Warning** dialog box is displayed.

Step 5 Confirm the information in the dialog box and select **I have read and understood the consequences associated with performing this operation**. Then click **OK**.

The **Success** dialog box is displayed.

Step 6 Click **OK**.

----End

5.6 Managing a CIFS Share

After a CIFS share is configured for a storage system, you need to manage and maintain the CIFS share. This section describes how to manage a CIFS share.

5.6.1 Viewing CIFS Share Information

By viewing CIFS share information, you can have the information about the share path and access permission of user or user group for this CIFS share.

Prerequisites

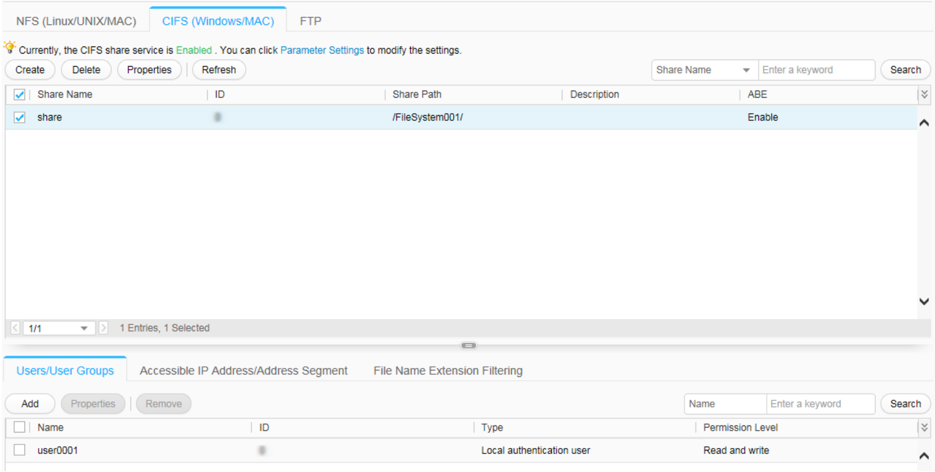
A CIFS share is created.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Provisioning** > **Share** > **CIFS (Windows/MAC)**.

Step 3 In CIFS share list, view the CIFS share information. The related parameters are as shown in **Table 5-29**.



Currently, the CIFS share service is Enabled . You can click Parameter Settings to modify the settings.

☑	Share Name	ID	Share Path	Description	ABE
☑	share	[redacted]	/FileSystem001/		Enable

□	Name	ID	Type	Permission Level
□	user0001	[redacted]	Local authentication user	Read and write

Table 5-29 CIFS Share Information

Parameter Name	Description
Share Name	The name of CIFS share.
ID	The ID of CIFS share.
Share Path	The directory of CIFS share.
Description	The description of CIFS share.
ABE	Whether the ABE function of CIFS share is enabled.

Step 4 In CIFS share list, select a CIFS share. In **Users/User Groups** tab, check the permission of the user or user group of this CIFS share. The related parameters are shown in **Table 5-30**.

Table 5-30 User/User Group Information

Parameter Name	Description
Name	The name of a user or a user group.
ID	The ID of share permission.
Type	The type of a user or user group. The types include: ● Everyone Every user has the access permission. ● Local authentication user The authentication user created in the storage system. ● Local authentication user group The authentication user group created in the storage system. ● Domain user The user in AD domain server. ● Domain user group The user group in AD domain server.
Permission Level	The CIFS share access permission. The permissions include: ● **Full control**: have all rights for CIFS share. ● **Read-only**: only have read right for CIFS share. (Default value) ● **Read and write**: have read and write right for CIFS share. ● **Forbidden**: access is forbidden.

Step 5 Click the **Accessible IP Address/Address Segment** tab. Query the IP addresses and IP address segments that are allowed to access the CIFS share. **Table 5-31** explains the related parameters.

Table 5-31 Accessible IP address/address segment

Parameter Name	Description
IP Address/Address Segment	IP addresses and IP address segments that are allowed to access the CIFS share

Step 6 Click the **File Name Extension Filtering** tab. Query the file name extension filter rule. **Table 5-32** explains the related parameters.

Table 5-32 File name extension filter rule

Parameter Name	Description
ID	ID of the file name extension filter rule
File Name Extension	File name extension (file type) to be filtered
Rule Type	Permission rules, including: ● Denied only: Files with the specified extension do not have access permission. ● Allowed only: Only files with the specified extension have access permission.

----End

5.6.2 Modifying Permissions for Accessing a CIFS Share

This section describes how to modify the permissions of a local authentication user or user group, domain user or user group for accessing CIFS shared resources to meet service requirements.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Provisioning** > **Share** > **CIFS (Windows/MAC)**.

Step 3 In the CIFS share list, select the CIFS share whose user or user group you want to modify.

Step 4 In **Users/User Groups**, select the user or user group whose permission you want to modify and click **Properties**.

Step 5 Select a new permission for the user or user group.

A user's possible permissions to access a CIFS share include:

- **Full control**: The user has full permission for the CIFS share.
- **Read-only**: The user can only read the CIFS share.
- **Read and write**: The user can read and write the CIFS share.
- **Forbidden**: The user is forbidden to access the CIFS share.

Step 6 Click **OK**.

The **Execution Result** dialog box is displayed.

Step 7 Click **Close** to finish modifying the permission for accessing a CIFS share.

----End

5.6.3 Modifying the Properties of IP Address/Address Segment for a CIFS Share

This operation allows you to modify the IP addresses or IP address segments that can access a CIFS share.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Provisioning** > **Share** > **CIFS (Windows/MAC)**.

Step 3 From the CIFS share list, select the CIFS share whose IP address or IP address segment you want to modify.

Step 4 In **Accessible IP Address/Address Segment**, select the IP address or IP address segment that you want to remove and click **Properties**.

Step 5 In **IP Address/Address Segment**, specify the IP addresses or IP address segments that you want to add.

NOTE

- The IP address segment is in the format of IP address/mask, for example, 192.168.1.100/16. A mixed IP address segment (IPv4 and IPv6) is not supported. The mask of IPv4 ranges from 1 to 32, and the mask of IPv6 ranges from 1 to 128.
- The IP address or IP address segment can be:
  - A single IPv4 or IPv6 address, for example, 192.168.1.100.
  - An IP address segment, for example, 192.168.1.100/16 or 192.168.1.10~192.168.1.11/30.
- A maximum of 32 IP addresses or IP address segments can be added.

Step 6 Click **OK**.

The **Success** dialog box is displayed.

Step 7 Click **OK**.

----End

5.6.4 Modifying the Properties of File Name Extension Filter Rules

File name extension filter rules can control the types of files that users access on a CIFS share.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Provisioning** > **Share** > **CIFS (Windows/MAC)**.

Step 3 From the CIFS share list, select the CIFS share whose file name extension filter rule is to be modified.

NOTE

If file name extension filtering rules are modified, the enabling and modification will take effect when the next new CIFS service request is initiated (such as refreshing directories, creating files, renaming files, performing failover retries, and querying file attributes).

Step 4 Click the **File Name Extension Filtering** tab.

Step 5 Select the filter rule to be modified and click **Properties**.

The **Properties of File Name Extension Filtering Rule** dialog box is displayed.

Step 6 Modify an existing file name extension filter rule.

NOTE

File name extension filtering rules are valid only for the current share.

1. In **File Name Extension**, add a file name extension (file type) to be filtered.

   NOTE

   – The file name extension contains 1 to 127 visible ASCII characters, and contains only digits, letters, space, and special characters (!\"#$%&\'()*+\,-.\/\:;\<=\>?@[\\]^_`{\|}~). Wildcard character * can only be the last character. For example, the file name extension can be txt, TXT, T?X, or Tx*.

   – The maximum number of filtering items supported by a share is 128.

   – The maximum number of filtering items supported by a storage system is 120,000.

   – The following are recommended configurations: One share has a maximum of seven file name extension filtering rules, and one file name extension contains 1 to 32 characters (excluding wildcards). The recommended configurations minimize the adverse impact on CIFS service performance. If the recommended configurations are not used, CIFS performance may greatly deteriorate.

   – When configuring a file name extension filtering rule, ensure that the rule does not affect the storage of temporary files that may be generated when application software is running. For example, some application software may generate files with the .tmp file name extension. In this case, add the .tmp extension to the file name extension filtering rule. For details about specific temporary file name extension of application software, contact the corresponding software vendor.

2. Select a new permission rule from the **Rule Type** drop-down list.

   NOTE

   – **Denied only**: Files with the specified extension do not have access permission.

   – **Allowed only**: Only files with the specified extension have access permission.

Step 7 Click **OK**.

The **Success** dialog box is displayed, indicating that the filter rule is successfully modified.

Step 8 Click **OK**.

----End

5.6.5 Modifying Properties of a CIFS Share

This operation enables you to modify the properties of a CIFS share to improve the sharing efficiency.

Procedure

Step 1 Log in to DeviceManager.

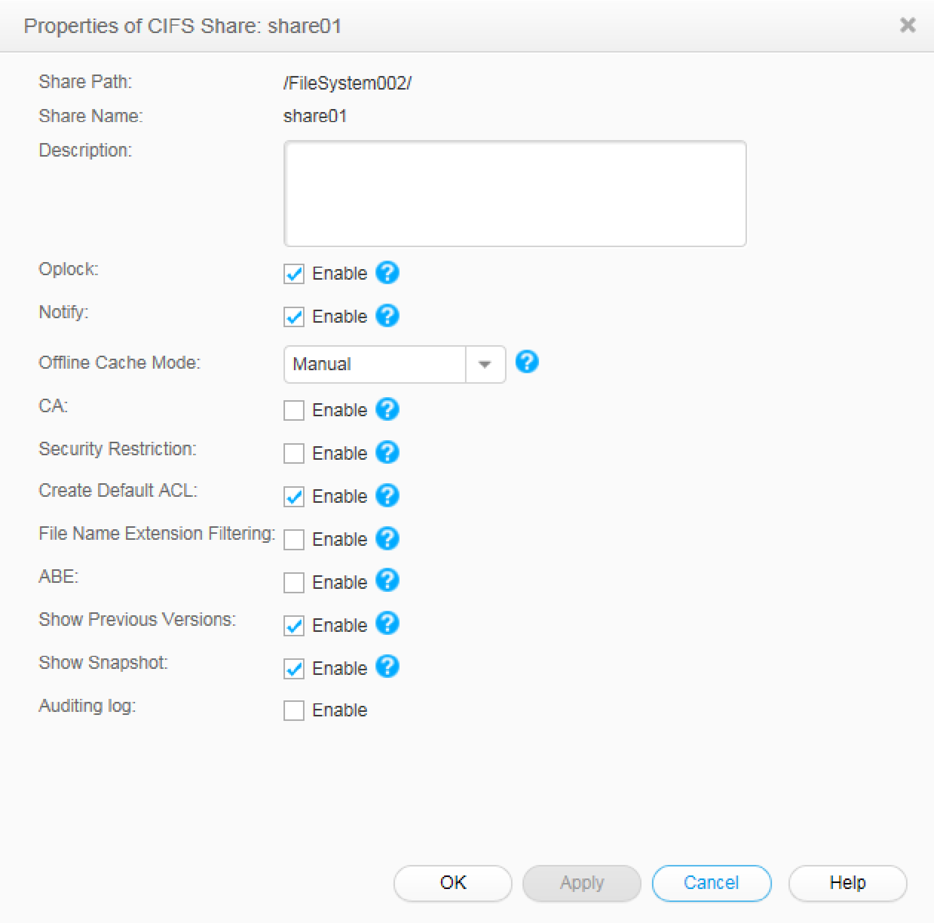
Step 2 Choose **Provisioning** > **Share** > **CIFS (Windows/MAC)**.

Step 3 Select the CIFS shared resource whose properties you want to modify.

Step 4 Click **Properties**.

The **Properties of CIFS Share** dialog box is displayed.

Step 5 Modify the following parameters based on site requirements.



Properties of CIFS Share: share01

Share Path: /FileSystem002/
Share Name: share01
Description:
Oplock: ☑ Enable
Notify: ☑ Enable
Offline Cache Mode: Manual
CA: ☐ Enable
Security Restriction: ☐ Enable
Create Default ACL: ☑ Enable
File Name Extension Filtering: ☐ Enable
ABE: ☐ Enable
Show Previous Versions: ☑ Enable
Show Snapshot: ☑ Enable
Auditing log: ☐ Enable

The **Table 5-33** describes the related parameters.

Table 5-33 Parameters for a CIFS share

Parameter	Description	Value
Description	Description of the created CIFS share.	[Value range] The name contains 0 to 255 characters. [Example] Share for user 1.

Parameter	Description	Value
Oplock	Opportunistic lock (Oplock) is a mechanism used to adjust cache policies of clients, improving performance and network utilization. This function is not recommended in the following scenarios: ● Scenarios that have high requirements for data integrity: Local cache loss will occur if your network is interrupted or your client breaks down after Oplock is enabled. If the upper-layer service software does not have a mechanism to ensure data integrity, recovery, or retry, data loss may occur. ● Scenarios where multiple clients access the same file: If Oplock is enabled, the system performance will be adversely affected.	[Default value] Enabled
Notify	After this parameter is enabled, a client's operations on a directory, such as adding a sub-directory, adding a new file, modifying the directory, and modifying a file, can be sensed by other clients that are accessing this directory or the parent directory of this directory.	[Default value] Enabled

Parameter	Description	Value
Offline Cache Mode	Cache files to be accessed in different offline cache modes to local clients so that files can be operated offline. The following offline cache modes are supported: ● None Files and programs in the shared directory cannot be cached to local clients. Therefore, these files and programs cannot be operated offline. This mode prevents the offline file function of clients from creating duplicates of files in the shared directory. ● Manual Specified files and programs in the shared directory can be cached to local clients and operated offline. ● Documents If a user accesses the shared directory and opens a file or program in the shared directory, the file or program is automatically cached to a local client so that the user can operate it offline. Files and programs that can be operated offline are saved in the cache of clients and they are synchronized with those in the shared directory until the cache is full or users delete them. Files and programs that have not been opened cannot be cached locally. ● Programs Performance is optimized based on the Documents mode. If an executable file (EXE or DLL) in the shared directory is executed by a local client, the file is automatically cached to the client. If the client needs to run the executable file online or offline next time, it accesses the cached file instead of that in the shared directory. **NOTE** The offline file function of clients must be enabled so that files and programs can be automatically cached.	[Default value] Manual

Parameter	Description	Value
CA	This option is for SMB3.0 continuous availability, only applied to the share for Hyper-V. This feature depends on Oplock, ensure that Oplock is enabled.	[Default value] Disabled
Security Restriction	After security restriction is enabled, only the added IP addresses can be used to access devices. If security restriction is not enabled, all IP addresses can be used to access devices.	[Default value] Disabled
Create Default ACL	This function creates a default ACL (full control rights to everyone; applied to the current directory, its subdirectories, and files in them) for a shared CIFS root directory if the directory has no ACL. You can change the default ACL in follow-up operations. If you want to retain the UNIX MODE rights, disable this function. **NOTE** This function cannot be enabled for modifying GNS.	[Default value] Enabled
File Name Extension	After file name extension filtering is enabled, the types of files that users access on a CIFS share are controlled. **NOTE** ● SMB2 and SMB3 support file name extension filtering while SMB1 does not support it. ● File name extension filtering is used for common CIFS share, excluding Homedir share. ● If file name extension filtering is enabled, the enabling and modification will take effect when the next new CIFS service request is initiated (such as refreshing directories, creating files, renaming files, performing failover retries, and querying file attributes).	[Default value] Disabled
ABE	After Access Based Enumeration (ABE) is enabled, files and folders that users have no access permission are not displayed. **NOTE** ● SMB2 and SMB3 support ABE while SMB1 does not support it. ● ABE is used for common CIFS share, excluding Homedir share.	[Default value] Disabled

Parameter	Description	Value
Audit Log	After the audit function is enabled, the system can record audit logs of the shared directory. The audit log items include **Open**, **Create**, **Read**, **Write**, **Close**, **Delete**, **Rename**, **Obtain properties**, **Set properties**, **Obtain security properties**, **Set security properties**, **Obtain extension properties**, and **Set extension properties**. After the audit function is enabled, by default, the system records **Create**, **Write**, **Delete**, and **Rename** operations of the shared directory. **NOTE** Before configuring this function, choose **Settings** > **Monitor Settings** > **Audit Log Settings**, and enable the **Audit Log Settings** function.	[Default value] Disabled

Step 6 Click **OK**.

The **Execution Result** dialog box is displayed.

Step 7 Click **Close** to finish modifying the CIFS properties.

----End

5.6.6 Deleting a CIFS Share

This operation enables you to delete CIFS shared resources. After the shared resources are deleted, users cannot access the resources.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Provisioning** > **Share** > **CIFS (Windows/MAC)**.

Step 3 Select the CIFS shared resource that you want to delete.

Step 4 Click **Delete**.

The security alert dialog box is displayed.

Step 5 Confirm the information in the dialog box and select **I have read and understand the consequences associated with performing this operation**. Then click **OK**.

The **Execution Result** dialog box is displayed.

Step 6 Click **Close** to finish deleting the CIFS shared resource.

----End

5.6.7 Disabling the CIFS Service

By performing this operation, you can disable the CIFS service of a storage system.

Precautions

If you disable the CIFS service, it will be unavailable. Before performing this operation, ensure that you do not need the CIFS service.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Settings** > **Storage Settings** > **File Storage Service** > **CIFS Service**.

Step 3 In **CIFS Service**, deselect **Enable**.

Step 4 Click **Save**.

The **Warning** dialog box is displayed.

Step 5 Confirm the information in the dialog box and select **I have read and understood the consequences associated with performing this operation**. Then click **OK**.

The **Success** dialog box is displayed.

Step 6 Click **OK**.

----End

5.7 Managing a CIFS Homedir Share (Applicable to V300R006C10)

This section explains how to query, modify, and delete CIFS Homedir shares.

5.7.1 Viewing CIFS Homedir Share Information

By viewing CIFS Homedir share information, you can have the information about the relative directory and access permission of user or user group for this CIFS Homedir share.

Prerequisites

A CIFS share is created.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Provisioning** > **Share** > **CIFS Homedir**.

Step 3 In CIFS Homedir share list, view the CIFS Homedir share information. The related parameters are as shown in **Table 5-34**.

Table 5-34 CIFS Share Information

Parameter Name	Description
Share Name	The name of CIFS Homedir share.
ID	The ID of CIFS Homedir share.
Relative Directory	The relative directory of CIFS Homedir share.
Description	The description of CIFS Homedir share.
ABE	Whether the ABE function of CIFS Homedir share is enabled.

Step 4 In CIFS Homedir share list, select a CIFS Homedir share. In **Users/User Groups** tab, check the permission of the user or user group of this CIFS Homedir share. The related parameters are shown in **Table 5-35**.

Table 5-35 User/User Group Information

Parameter Name	Description
Name	The name of a user or a user group.
ID	The ID of share permission.
Type	The type of a user or user group. The types include: ● Everyone Every user has the access permission. ● Local authentication user The authentication user created in the storage system. ● Local authentication user group The authentication user group created in the storage system. ● Domain user The user in AD domain server. ● Domain user group The user group in AD domain server.
Permission Level	The CIFS share access permission. The permissions include: ● **Full control**: have all rights for CIFS share. ● **Read-only**: only have read right for CIFS share. (Default value) ● **Read and write**: have read and write right for CIFS share. ● **Forbidden**: access is forbidden.

Step 5 Click the **Accessible IP Address/Address Segment** tab. Query the IP addresses and IP address segments that are allowed to access the CIFS share. **Table 5-36** explains the related parameters.

Table 5-36 Accessible IP address/address segment

Parameter Name	Description
IP Address/Address Segment	IP addresses and IP address segments that are allowed to access the CIFS share

Step 6 Click the **File Name Extension Filtering** tab. Query the file name extension filter rule. **Table 5-37** explains the related parameters.

Table 5-37 File name extension filter rule

Parameter Name	Description
ID	ID of the file name extension filter rule
File Name Extension	File name extension (file type) to be filtered
Rule Type	Permission rules, including: ● Denied only: Files with the specified extension do not have access permission. ● Allowed only: Only files with the specified extension have access permission.

Step 7 Click the **CIFS Homedir Mapping Rule** tab to view mapping rules of file system paths. **Table 5-38** describes related parameters.

Table 5-38 CIFS Homedir Mapping Rule

Parameter Name	Description
Username	User name of a CIFS Homedir mapping rule
ID	ID of the CIFS Homedir mapping rule
Share Path	**Share Path** consists of the values of **File System**, **Quota Tree** and **Directory**.
Priority	Priority of the CIFS Homedir mapping rule
AutoCreate	If **AutoCreate** is enabled but no relative directory exists under the CIFS Homedir share path. The system will automatically create a relative directory.

----End

5.7.2 Modifying Permissions for Accessing a CIFS Homedir Share

This section describes how to modify the permissions of a local authentication user or user group, domain user or user group for accessing CIFS Homedir shared resources to meet service requirements.

Procedure

Step 1 Log in to DeviceManager.

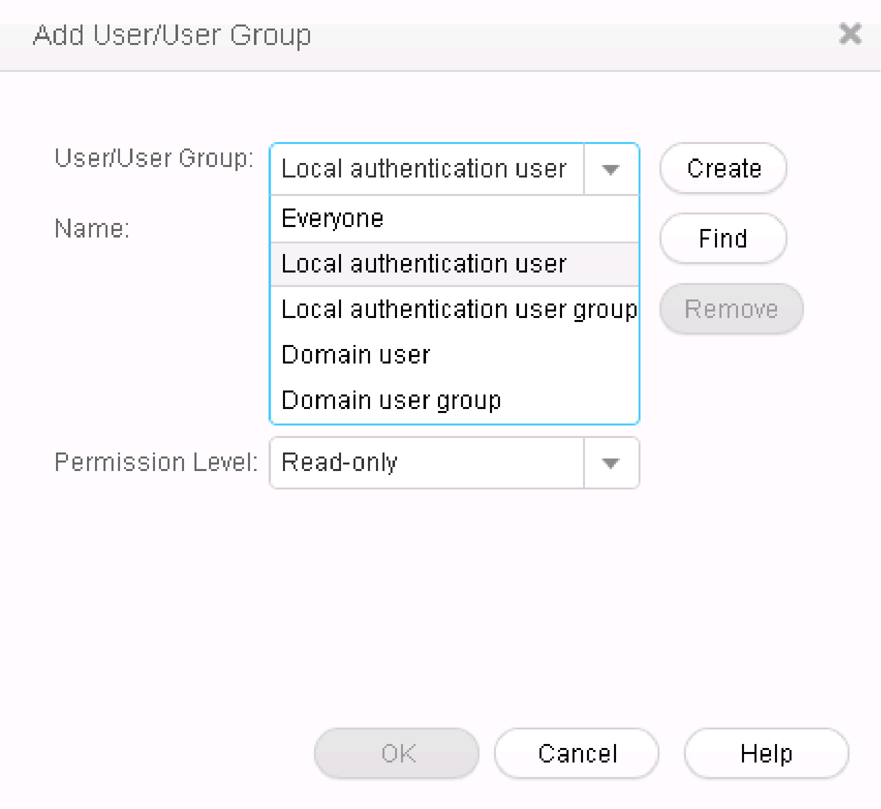
Step 2 Choose **Provisioning** > **Share** > **CIFS Homedir**.

Step 3 In the CIFS Homedir share list, select the CIFS Homedir share whose user or user group you want to modify.

Step 4 Add user or user group for accessing the CIFS Homedir share.

1. In **Users/User Groups** area, click **Add**.

   The **Add User/User Group** dialog box is displayed.



Add User/User Group

User/User Group: Local authentication user

Name:

Permission Level: Read-only

2. In **User/User Group**, select user type or user group type.

   The values include: **Everyone**, **Local authentication user**, **Local authentication user group**, **Domain user** and **Domain user group**.

3. If you select **Everyone**, click **Add**.

   The system adds **Everyone** to the list.

   NOTE

   Everyone means every user has the access permission.

4. If you select **Local authentication user** or **Local authentication user group**, click **Find**, in the pop-up **Add User** or **Add User Group** dialog boxes to select the user or user group you want to add. Click **OK**.
5. If you select **Domain user** or **Domain user group**, enter the corresponding name in **Name**, and click **Add**.

   NOTE

   The name format is **Domain name\Domain user name** or **Domain name\Domain user group name**.
6. In **Permission Level**, select the CIFS Homedir access permission for the user or user group added.

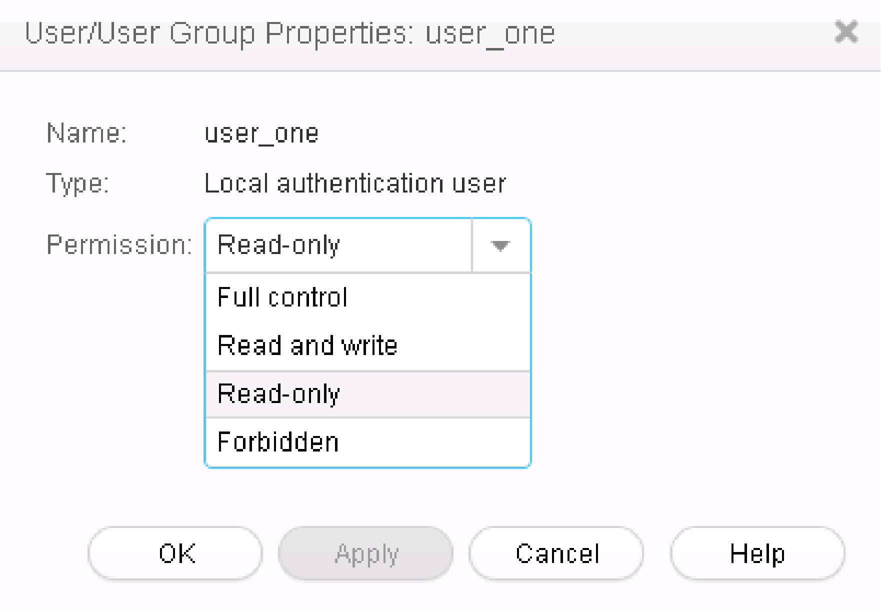
   The CIFS Homedir access permission levels include:
   - **Full control**: have all rights for CIFS Homedir share.
   - **Read-only**: only have read right for CIFS Homedir share. (Default value)
   - **Read and write**: have read and write right for CIFS Homedir share.
   - **Forbidden**: access is forbidden.
7. Click **OK**.

   The **Execution Result** dialog box is displayed.
8. Click **Close** to finish adding new local authentication user or user group.

Step 5 Modify the permission of a user or user group.

1. In **Users/User Groups**, select the user or user group whose permission you want to modify and click **Properties**.

   The **User/User Group Properties** dialog box is displayed.



User/User Group Properties: user_one

Name: user_one

Type: Local authentication user

Permission: Read-only

2. Select a new permission for the user or user group.

   A user's possible permissions to access a CIFS share include:
   - **Full control**: The user has full permission for the CIFS share.
   - **Read-only**: The user can only read the CIFS share.
   - **Read and write**: The user can read and write the CIFS share.
   - **Forbidden**: The user is forbidden to access the CIFS share.

3. Click **OK**.

   The **Execution Result** dialog box is displayed.

4. Click **Close** to finish modifying the permission for accessing a CIFS share.

Step 6 Remove a user or user group.

1. In **Users/User Groups**, select the user or user group you want to remove and click **Remove**.

   The security alert dialog box is displayed.

2. Confirm the information in the dialog box and select **I have read and understand the consequences associated with performing this operation**. Then click **OK**.

   The **Execution Result** dialog box is displayed.

3. Click **Close** to finish removing the user or user group.

----End

5.7.3 Modifying the Properties of Accessible IP Address/Address Segment for a CIFS Share

This operation allows you to modify the IP addresses or IP address segments that can access a CIFS Homedir share.

Procedure

Step 1 Log in to DeviceManager.

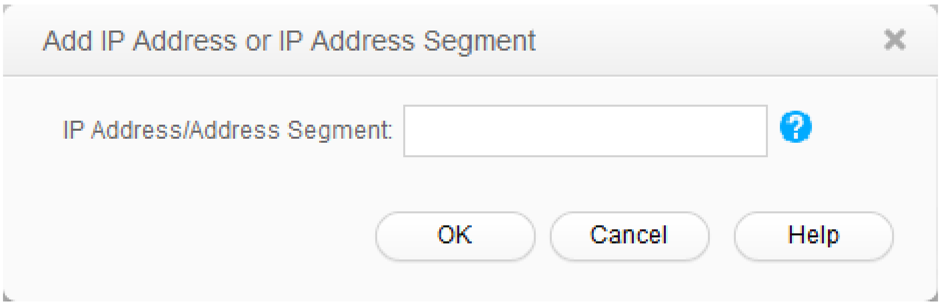
Step 2 Choose **Provisioning** > **Share** > **CIFS Homedir**.

Step 3 From the CIFS share list, select the CIFS Homedir share whose IP address or IP address segment you want to modify.

Step 4 Add accessible IP addresses or IP address segments.

1. In the **Accessible IP Address/IP Address Segment** area, click **Add**.

   The **Add IP Address or IP Address Segment** dialog box is displayed.


Add IP Address or IP Address Segment
×
IP Address/Address Segment:
?
OK
Cancel
Help

2. In **IP Address/Address Segment**, specify the IP addresses or IP address segments that you want to add.

NOTE

- The IP address segment is in the format of IP address/mask, for example, 192.168.1.100/16. A mixed IP address segment (IPv4 and IPv6) is not supported. The mask of IPv4 ranges from 1 to 32, and the mask of IPv6 ranges from 1 to 128.
- The IP address or IP address segment can be:
  - A single IPv4 or IPv6 address, for example, 192.168.1.100.
  - An IP address segment, for example, 192.168.1.100/16 or 192.168.1.10~192.168.1.11/30.
- A maximum of 32 IP addresses or IP address segments can be added.

3. Click **OK**.

   The **Success** dialog box is displayed, indicating that the accessible IP addresses or IP address segments are added successfully.

4. Click **OK**.

   You can view added IP addresses or IP address segments in the **Accessible IP Address/IP Address Segment** list.

Step 5 Modify an IP address or IP address segment.

1. In **Accessible IP Address/IP Address Segment**, select the IP address or IP address segment that you want to remove and click **Properties**.

   The **Properties of Accessible IP Address/IP Address Segment** dialog box is displayed.

2. In **IP Address/Address Segment**, specify the IP addresses or IP address segments that you want to add.

   NOTE

   - The IP address segment is in the format of IP address/mask, for example, 192.168.1.100/16. A mixed IP address segment (IPv4 and IPv6) is not supported. The mask of IPv4 ranges from 1 to 32, and the mask of IPv6 ranges from 1 to 128.
   - The IP address or IP address segment can be:
     - A single IPv4 or IPv6 address, for example, 192.168.1.100.
     - An IP address segment, for example, 192.168.1.100/16 or 192.168.1.10~192.168.1.11/30.
   - A maximum of 32 IP addresses or IP address segments can be added.

3. Click **OK**.

   The **Success** dialog box is displayed.

4. Click **OK**.

Step 6 Remove an IP address or IP address segment.

1. In **Accessible IP Address/IP Address Segment**, select the IP address or IP address segment that you want to remove and click **Remove**.

   The security alert dialog box is displayed.

2. Carefully read the content of the dialog box and select **I have read and understand the consequences associated with performing this operation**. Then click **OK**.

   The **Execution Result** dialog box is displayed.

3. Click **Close**. You have finished deleting the IP address or IP address segment.

----End

5.7.4 Modifying the Properties of File Name Extension Filter Rules

File name extension filter rules can control the types of files that users access on a CIFS Homedir share.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Provisioning** > **Share** > **CIFS Homedir**.

Step 3 From the CIFS Homedir share list, select the CIFS Homedir share whose file name extension filter rule is to be modified.

NOTE

If file name extension filtering rules are modified, the enabling and modification will take effect when the next new CIFS Homedir service request is initiated (such as refreshing directories, creating files, renaming files, performing failover retries, and querying file attributes).

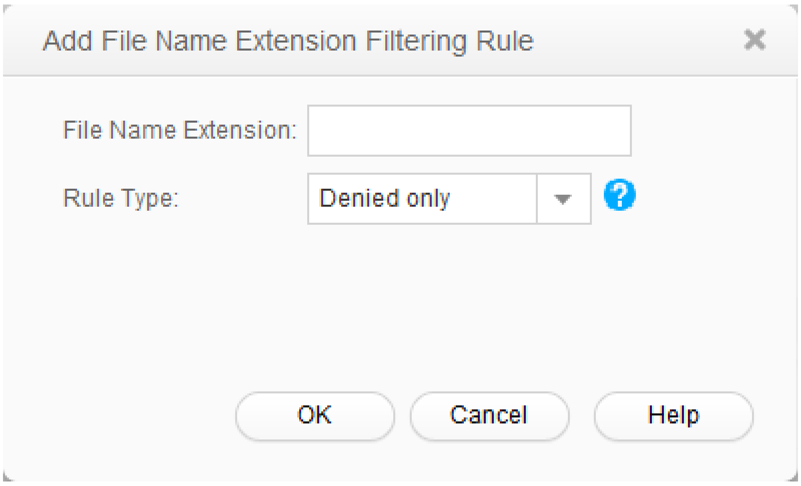
Step 4 Add a file name extension filter rule.

NOTE

File name extension filtering rules are valid only for the current share.

1. Click the **File Name Extension Filtering Rule** tab.
2. Click **Add**.

   The **Add File Name Extension Filtering Rule** dialog box is displayed.



Add File Name Extension Filtering Rule

File Name Extension:

Rule Type: Denied only

3. In **File Name Extension**, specify the file name extension (file type) to be filtered.

NOTE

- The file name extension contains 1 to 127 visible ASCII characters, and contains only digits, letters, space, and special characters (!\"#$%&\'()*+\,-.\/\:;\<=\>?@[\\]^_`{\|}~). Wildcard character * can only be the last character. For example, the file name extension can be txt, TXT, T?X, or Tx*.
- The maximum number of filtering items supported by a share is 128.
- The maximum number of filtering items supported by a storage system is 120,000.
- The following are recommended configurations: One share has a maximum of seven file name extension filtering rules, and one file name extension contains 1 to 32 characters (excluding wildcards). The recommended configurations minimize the adverse impact on CIFS service performance. If the recommended configurations are not used, CIFS performance may greatly deteriorate.
- When configuring a file name extension filtering rule, ensure that the rule does not affect the storage of temporary files that may be generated when application software is running. For example, some application software may generate files with the .tmp file name extension. In this case, add the .tmp extension to the file name extension filtering rule. For details about specific temporary file extension of application software, contact the corresponding software vendor.

4. Select the permission rule from the **Rule Type** drop-down list.

   NOTE

   - **Denied only**: Files with the specified extension do not have access permission.
   - **Allowed only**: Only files with the specified extension have access permission.

5. Click **OK**.

   The **Success** dialog box is displayed, indicating that the filter rule is successfully added.

6. Click **OK**.

   On the **File Name Extension Filtering Rule** tab page, query the added filter rule.

Step 5 Modify an existing file name extension filter rule.

NOTE

File name extension filtering rules are valid only for the current share.

1. Click the **File Name Extension Filtering Rule** tab.
2. Select the filter rule to be modified and click **Properties**.

   The **Properties of File Name Extension Filtering Rule** dialog box is displayed.

3. In **File Name Extension**, add a file name extension (file type) to be filtered.

NOTE

- The file name extension contains 1 to 127 visible ASCII characters, and contains only digits, letters, space, and special characters (!\"#$%&\'()*+\,-.\/\:;\<=\>?@[\\]^_`{\|}~). Wildcard character * can only be the last character. For example, the file name extension can be txt, TXT, T?X, or Tx*.
- The maximum number of filtering items supported by a share is 128.
- The maximum number of filtering items supported by a storage system is 120,000.
- The following are recommended configurations: One share has a maximum of seven file name extension filtering rules, and one file name extension contains 1 to 32 characters (excluding wildcards). The recommended configurations minimize the adverse impact on CIFS service performance. If the recommended configurations are not used, CIFS performance may greatly deteriorate.
- When configuring a file name extension filtering rule, ensure that the rule does not affect the storage of temporary files that may be generated when application software is running. For example, some application software may generate files with the .tmp file name extension. In this case, add the .tmp extension to the file name extension filtering rule. For details about specific temporary file name extension of application software, contact the corresponding software vendor.

4. Select a new permission rule from the **Rule Type** drop-down list.

   NOTE

   - **Denied only**: Files with the specified extension do not have access permission.
   - **Allowed only**: Only files with the specified extension have access permission.

5. Click **OK**.

   The **Success** dialog box is displayed, indicating that the filter rule is successfully modified.

6. Click **OK**.

Step 6 Delete an existing file name extension filter rule.

NOTE

When removing a file name extension filtering rule, ensure that the removal does not affect the storage of temporary files that may be generated when application software is running. For details about specific temporary file extension of application software, contact the corresponding software vendor.

1. Click the **File Name Extension Filtering Rule** tab.
2. Select the filter rule to be deleted and click **Remove**.

   The **Confirm** dialog box is displayed.

3. Click **OK**.

   The **Execution Result** dialog box is displayed.

4. Click **Close**. The file name extension filter rule is successfully deleted.

----End

5.7.5 Modifying the Properties of CIFS Homedir Mapping Rules

The CIFS Homedir mapping rule consists of user name, file system, Quota Tree, priority, and AutoCreate option. Only users who match mapping rules can access the Homedir directory under the filesystem.

Procedure

Step 1 Log in to DeviceManager.

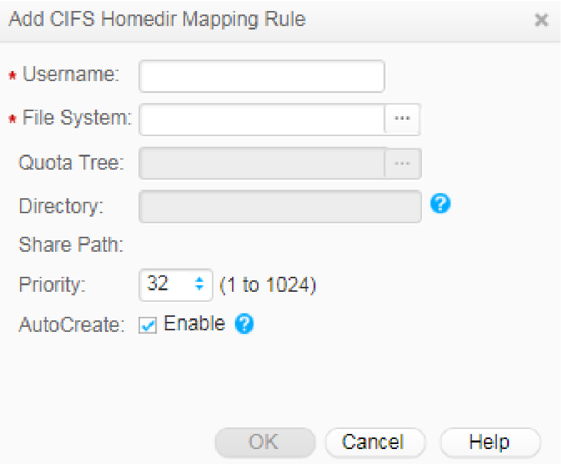
Step 2 Choose **Provisioning** > **Share** > **CIFS Homedir**.

Step 3 From the CIFS Homedir share list, select the CIFS Homedir share whose mapping rule you want to modify.

Step 4 Add a CIFS Homedir mapping rule.

1. Click the **CIFS Homedir Mapping Rule** tab.
2. Click **Add**.

   The **Add CIFS Homedir Mapping Rule** dialog box is displayed.



Add CIFS Homedir Mapping Rule

* Username:

* File System:

Quota Tree:

Directory:

Share Path:

Priority: 32 (1 to 1024)

AutoCreate: ☑ Enable

3. In **Username**, fill the user name of the CIFS Homedir mapping rule.

   NOTE

   – The value contains 1 to 255 characters.

   – The value can be names of common or domain users. Use a slash (\) to connect the domain name and user name. Only one slash (\) is allowed.

   – Wildcard character * is allowed. The user name can contain only one wildcard character and the wildcard character must be at the end of the user name. For example, **china*** indicates all users in the **china** domain.

   – The user name cannot contain spaces or special characters including **"/[]<>+:;,?=|**, and cannot end with a period (**.**).

4. In **File System**, select the file system for which you want to create a mapping rule.
   - In the file system list, select a file system and click **OK**.
   - If your desired file system does not exist, click **Create** to create one. After the file system is created, select the file system and click **OK**.
5. **Optional:** In **Quota Tree**, select a quota tree.
   - In the quota tree list of the file system, select quota trees and click **OK**.
   - If your desired quota tree does not exist, click **Create** to create one. **Table 5-39** describes the related parameters.

Table 5-39 Quota tree parameters

<table>
<tr><th>Parameter</th><th>Description</th><th>Value</th></tr>
<tr><td>Name</td><td>Quota tree name.</td><td>[Value range]
■ The name must be unique.
■ For V300R006C00, the name can only contain letters, digits, and underscores (_).
■ For V300R006C10, the name can only contain letters, digits and special characters. Special characters include !"#$ %&'()*+-.;<=>? @[\]^`{_|}~ and spaces. On the CLI, some characters need to be entered as escape characters. For example, \| indicates |, || indicates \, \q indicates ?, and \s indicates spaces.
■ The name can be 1 to 127 characters in length.
[Example]
quotatree001</td></tr>
<tr><td>Quantity</td><td>Number of quota trees that you want to create in batch. Set this parameter based on site requirements.</td><td>[Value range]
1 to 500
[Example]
5</td></tr>
<tr><td>Owning file system</td><td>File system to which the newly created quota tree belongs.</td><td>[Example]
filesystem_001</td></tr>
</table>

Parameter	Description	Value
Quota	This parameter specifies the number and size of files in the quota tree. NOTE ■ If the file system for which you want to create a quota tree has requirements for quotas, you are advised to enable the quota function. ■ After selecting the option to enable the quota function, a dialog box indicating danger will be displayed when you confirm the quota tree creation. Confirm the information of the dialog box and select **I have read and understand the consequences associated with performing this operation.** Then click **OK** to complete the creation.	[Example] Enable

6. **Optional:** In **Directory**, enter an accessible directory.
7. **Share Path** of a file system consists of the values of **File System**, **Quota Tree** and **Directory**.
8. In **Priority**, set the priority of the mapping rule.
   - The value of **Priority** ranges from 1 to 1024.
   - Mappings rules are sorted by priority in descending order. If two mapping rules have the same priority, the one that is created earlier is placed in the front. Users match mapping rules in sequence.
9. Determine whether to enable **AutoCreate**.
   - If **AutoCreate** is enabled but no relative directory exists under the CIFS Homedir share path. The system will automatically create a relative directory.
   - **AutoCreate** is enabled by default. You can disable it. If **AutoCreate** is disabled and the relative directory does not exist, users fail to match this rule and will match the next one.
10. Click **OK**.

    The **Success** dialog box is displayed, indicating that the CIFS Homedir mapping rule is added successfully.
11. Click **OK**.

    On the **CIFS Homedir** tab page, view the newly added mapping rule.

Step 5 Modify a CIFS Homedir mapping rule.

1. Click the **CIFS Homedir Mapping Rule** tab.
2. Select the CIFS Homedir mapping rule that you want to modify and click **Properties**.

   The **Properties of CIFS Homedir Mapping Rule** dialog box is displayed.

3. In **Priority**, adjust the priority of the mapping rule.
   - The value of **Priority** ranges from 1 to 1024.
   - Mappings rules are sorted by priority in descending order. If two mapping rules have the same priority, the one that is created earlier is placed in the front. Users match mapping rules in sequence.
4. Determine whether to enable **AutoCreate**.
   - If **AutoCreate** is enabled but no relative directory exists under the CIFS Homedir share path. The system will automatically create a relative directory.
   - **AutoCreate** is enabled by default. You can disable it. If **AutoCreate** is disabled and the relative directory does not exist, users fail to match this rule and will match the next one.
5. Click **OK**.

   The **Success** dialog box is displayed, indicating that the CIFS Homedir mapping rule is modified successfully.
6. Click **OK**.

Step 6 Remove a CIFS Homedir mapping rule.

1. Click the **CIFS Homedir Mapping Rule** tab.
2. Select the CIFS Homedir mapping rule that you want to remove and click **Remove**.

   The **Warning** dialog box is displayed.
3. Click **OK**.

   The **Execution Result** dialog box is displayed.
4. Click **Close**. The CIFS Homedir mapping rule is removed successfully.

----End

5.7.6 Modifying Properties of a CIFS Homedir Share

This operation enables you to modify the properties of a CIFS Homedir share to improve the sharing efficiency.

Procedure

Step 1 Log in to DeviceManager.

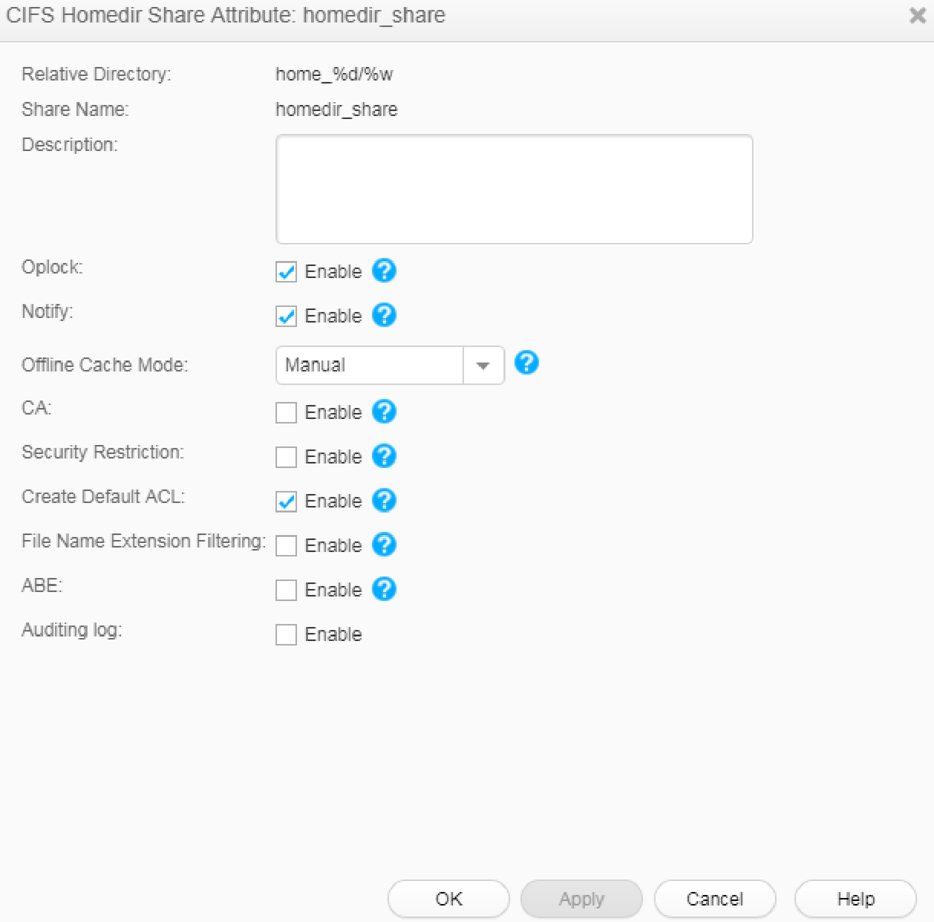
Step 2 Choose **Provisioning** > **Share** > **CIFS Homedir**.

Step 3 Select the CIFS Homedir shared resource whose properties you want to modify.

Step 4 Click **Properties**.

The **CIFS Homedir Share Attribute** dialog box is displayed.

Step 5 Modify the following parameters based on site requirements.



CIFS Homedir Share Attribute: homedir_share

Relative Directory: home_%d/%w

Share Name: homedir_share

Description:

Oplock: ☑ Enable

Notify: ☑ Enable

Offline Cache Mode: Manual

CA: □ Enable

Security Restriction: □ Enable

Create Default ACL: ☑ Enable

File Name Extension Filtering: □ Enable

ABE: □ Enable

Auditing log: □ Enable

The **Table 5-40** describes the related parameters.

Table 5-40 Parameters for a CIFS Homedir share

Parameter	Description	Value
Description	Description of the created CIFS Homedir share.	[Value range] The name contains 0 to 255 characters. [Example] Share for user 1.

Parameter	Description	Value
Oplock	Opportunistic lock (Oplock) is a mechanism used to adjust cache policies of clients, improving performance and network utilization. This function is not recommended in the following scenarios: ● Scenarios that have high requirements for data integrity: Local cache loss will occur if your network is interrupted or your client breaks down after Oplock is enabled. If the upper-layer service software does not have a mechanism to ensure data integrity, recovery, or retry, data loss may occur. ● Scenarios where multiple clients access the same file: If Oplock is enabled, the system performance will be adversely affected.	[Default value] Enabled
Notify	After this parameter is enabled, a client's operations on a directory, such as adding a sub-directory, adding a new file, modifying the directory, and modifying a file, can be sensed by other clients that are accessing this directory or the parent directory of this directory.	[Default value] Enabled

Parameter	Description	Value
Offline Cache Mode	Cache files to be accessed in different offline cache modes to local clients so that files can be operated offline. The following offline cache modes are supported: ● None Files and programs in the shared directory cannot be cached to local clients. Therefore, these files and programs cannot be operated offline. This mode prevents the offline file function of clients from creating duplicates of files in the shared directory. ● Manual Specified files and programs in the shared directory can be cached to local clients and operated offline. ● Documents If a user accesses the shared directory and opens a file or program in the shared directory, the file or program is automatically cached to a local client so that the user can operate it offline. Files and programs that can be operated offline are saved in the cache of clients and they are synchronized with those in the shared directory until the cache is full or users delete them. Files and programs that have not been opened cannot be cached locally. ● Programs Performance is optimized based on the Documents mode. If an executable file (EXE or DLL) in the shared directory is executed by a local client, the file is automatically cached to the client. If the client needs to run the executable file online or offline next time, it accesses the cached file instead of that in the shared directory. **NOTE** The offline file function of clients must be enabled so that files and programs can be automatically cached.	[Default value] Manual

Parameter	Description	Value
CA	This option is for SMB3.0 continuous availability, only applied to the share for Hyper-V. This feature depends on Oplock, ensure that Oplock is enabled.	[Default value] Disabled
Security Restriction	After security restriction is enabled, only the added IP addresses can be used to access devices. If security restriction is not enabled, all IP addresses can be used to access devices.	[Default value] Disabled
Create Default ACL	This function creates a default ACL (full control rights to everyone; applied to the current directory, its subdirectories, and files in them) for a shared CIFS root directory if the directory has no ACL. You can change the default ACL in follow-up operations. If you want to retain the UNIX MODE rights, disable this function.	[Default value] Enabled
File Name Extension	After file name extension filtering is enabled, the types of files that users access on a CIFS share are controlled. **NOTE** ● SMB2 and SMB3 support file name extension filtering while SMB1 does not support it. ● If file name extension filtering is enabled, the enabling and modification will take effect when the next new CIFS Homedir service request is initiated (such as refreshing directories, creating files, renaming files, performing failover retries, and querying file attributes).	[Default value] Disabled
ABE	After Access Based Enumeration (ABE) is enabled, files and folders that users have no access permission are not displayed. **NOTE** SMB2 and SMB3 support ABE while SMB1 does not support it.	[Default value] Disabled
Show Previous Versions	If the function of showing historical versions is enabled, clients can show and roll back historical versions.	[Default value] Enabled
Show Snapshot	If the function of showing snapshots is enabled, clients can show and traverse snapshot directories.	[Default value] Enabled

Parameter	Description	Value
Audit Log	After the audit function is enabled, the system can record audit logs of the shared directory. The audit log items include **Open**, **Create**, **Read**, **Write**, **Close**, **Delete**, **Rename**, **Obtain properties**, **Set properties**, **Obtain security properties**, **Set security properties**, **Obtain extension properties**, and **Set extension properties**. After the audit function is enabled, by default, the system records **Create**, **Write**, **Delete**, and **Rename** operations of the shared directory.	[Default value] Disabled

Step 6 Click **OK**.

The **Execution Result** dialog box is displayed.

Step 7 Click **Close** to finish modifying the CIFS properties.

----End

5.7.7 Deleting a CIFS Homedir Share

This operation enables you to delete CIFS Homedir shared resources. After the shared resources are deleted, users cannot access the resources.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Provisioning** > **Share** > **CIFS Homedir**.

Step 3 Select the CIFS Homedir shared resource that you want to delete.

Step 4 Click **Delete**.

The security alert dialog box is displayed.

Step 5 Confirm the information in the dialog box and select **I have read and understand the consequences associated with performing this operation**. Then click **OK**.

The **Execution Result** dialog box is displayed.

Step 6 Click **Close** to finish deleting the CIFS Homedir shared resource.

----End

5.7.8 Disabling the Homedir Service

By performing this operation, you can disable the Homedir service of a storage system.

Precautions

If you disable the Homedir service, it will be unavailable. Before performing this operation, ensure that you do not need the Homedir service.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Settings** > **Storage Settings** > **File Storage Service** > **CIFS Service**.

Step 3 In **Homedir**, deselect **Enable**.

Step 4 Click **Save**.

A dialog box is displayed for your confirmation.

Step 5 Click **OK**.

----End

5.8 Managing an FTP Share

FTP shares enable permission control and file systems to be shared for specific users. FTP share management includes maintaining existing shares and controlling the global properties of the FTP feature. This chapter describes how to update existing FTP shares and how to manage the global parameters of FTP shares.

5.8.1 Viewing the Properties of an FTP Share

This operation enables you to view the properties of an FTP share.

Prerequisites

You have logged in to the DeviceManager as an administrator that has the permission to view the file system structure. The following administrators have the permission:

- Super administrator
- Administrator

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Provisioning** > **Share** > **FTP**.

Step 3 In the shared directory list of the middle function pane, select the shared item whose properties you want to view and click **Properties**.

Step 4 In the **Properties of FTP Share** dialog box that is displayed, view the properties of the selected FTP shared item. For details about the property parameters, see FTP share parameters in previous topics.

----End

5.8.2 Modifying the Properties of an FTP Share

You can reset access permissions to an FTP shared directory by modifying the properties of the FTP share.

Prerequisites

- You have logged in to the DeviceManager as an administrator that has the permission to view the file system structure. The following administrators have the permission:
  - Super administrator
  - Administrator
- An FTP shared item has been created.

Procedure

Step 1 Log in to DeviceManager.

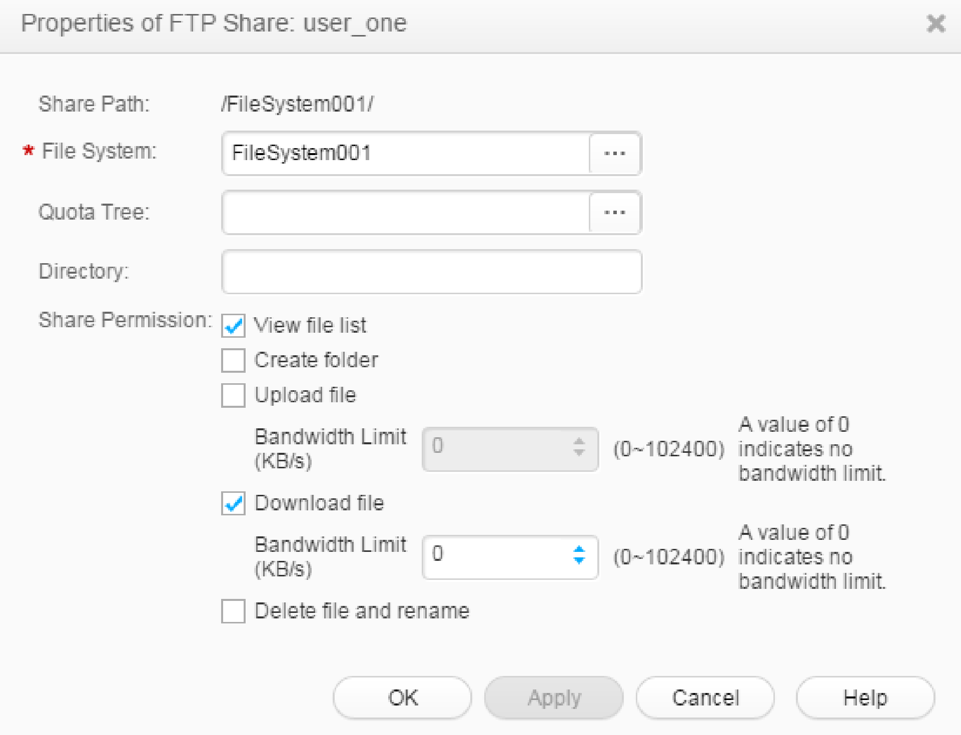
Step 2 Choose **Provisioning** > **Share** > **FTP**.

Step 3 In the shared list of the middle function pane, select the item whose properties you want to modify and click **Properties**.

Step 4 In the **Properties of FTP Share** dialog box that is displayed, modify the properties of the FTP shared item.

You can perform the following operations:

- Modify the file system and quota tree.
- Modify the share permission.



Properties of FTP Share: user_one

Share Path: /FileSystem001/

* File System: FileSystem001

Quota Tree:

Directory:

Share Permission:
☑ View file list
□ Create folder
□ Upload file
Bandwidth Limit (KB/s) 0 (0~102400) A value of 0 indicates no bandwidth limit.
☑ Download file
Bandwidth Limit (KB/s) 0 (0~102400) A value of 0 indicates no bandwidth limit.
□ Delete file and rename

Parameter	Description	Value
Share Path	The share path of a file system consists of **File System**, **Quota Tree** and **Directory**.	[Example] /Filesystem001/Share/Share01
File System	File system to be shared. You can select a file system by clicking	[Example] Filesystem001
Quota Tree	Quota tree is Level-1 directory under the root directory of the file system.	[Example] Share
Directory	Directory or subdirectory under the file system root directory.	[Example] Share01
Share permission	The share permissions include: ● View file list ● Create folder ● Upload file After this item is selected, the maximum upload speed (bandwidth) needs to be set for a single file. By default, the bandwidth is 0 KB/s. That is, the bandwidth is not limited. ● Download file After this item is selected, the maximum download speed (bandwidth) needs to be set for a single file. By default, the bandwidth is 0 KB/s. That is, the bandwidth is not limited. ● Delete file and rename	[Value range] ● The upload speed (bandwidth) ranges from 0 to 102,400 (unit: KB/s). ● The download speed (bandwidth) ranges from 0 to 102,400 (unit: KB/s). [Default value] ● View file list ● Download file

NOTE

The share path consists of file system and quota tree. The share path cannot contain space, double quotation mark ("), backslash (\), square brackets ([]), less than (<), larger than (>), plus (+), colon (:), semicolon (;), comma (,), question mark (?), asterisk (*), vertical bar (|), equal mark (=), (@), and ('), or FTP share cannot be modified.

Step 5 Click **OK** to finish modifying the properties of FTP share.

----End

5.8.3 Deleting an FTP Share

After an FTP share is deleted, the shared item is no longer available.

Prerequisites

- You have logged in to the DeviceManager as an administrator that has the permission to view the file system structure. The following administrators have the permission:
  - Super administrator
  - Administrator
- An FTP shared item has been created.

Impact on the System

Access to the deleted FTP shared item is interrupted.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Provisioning** > **Share** > **FTP**.

Step 3 In the shared list of the middle function pane, select shared items and click **Delete**.

The security alert dialog box is displayed.

NOTE

You can delete multiple shared items at a time.

Step 4 Click **OK**.

The **Execution Result** dialog box is displayed.

Step 5 Click **Close**.

----End

5.8.4 Disabling the FTP Service

By performing this operation, you can disable the FTP service of a storage system.

Precautions

If you disable the FTP service, it will be unavailable. Before performing this operation, ensure that you do not need the FTP service.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Settings** > **Storage Settings** > **File Storage Service** > **FTP Service**.

Step 3 Deselect **Enable**.

Step 4 Click **Save**.

The **Warning** dialog box is displayed.

Step 5 Confirm the information in the dialog box and select **I have read and understood the consequences associated with performing this operation**. Then click **OK**.

The **Success** dialog box is displayed.

Step 6 Click **OK**.

----End

5.9 HTTP Share Management

After an HTTP share is configured for a storage system, you need to manage and maintain the HTTP share. This chapter describes how to manage an HTTP share.

5.9.1 Enabling the HTTP Service

This operation enables you to enable the HTTP service.

Prerequisites

A file system whose HTTP service must be enabled has been created.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Settings** > **Storage Settings** > **File Storage Service** > **HTTP Service**.

Step 3 In **HTTP Service**, select **Enable**.

Step 4 In **Max. Number of Connections**, enter the number that the FTP share support.

NOTE

The maximum number of connections varies depending on the device model.

Step 5 **Optional:** In **HTTP Default Port**, select **Enable**.

Exercise caution when enabling the HTTP port.

Step 6 In **File System**, select the file system whose HTTP service you want to enable.

Step 7 **Optional:** In **Directory**, enter an accessible directory under the file system selected that you want to share over HTTP.

NOTE

Share Path contains **File System** and **Directory**.

Step 8 **Optional:** In **DAV**, select **Enable**.

NOTE

- DAV, also known as WebDAV (Web-based Distributed Authoring and Versioning), is a communication protocol based on HTTP. Once WebDAV enabled, the system allows the DAV client to read/write the shared directory, and supports file locking, file unlocking, and file version control.
- After enabling WebDAV, resource users may have full control permissions of the HTTP sharing root directories.

Step 9 Click **Save**.

The **Success** dialog box is displayed.

Step 10 Click **OK**.

----End

5.9.2 Modifying the Parameters of an HTTP Share

This operation enables you to modify the parameters of an HTTP share, including the setting the maximum number of connections and enabling or disabling DAV.

Prerequisites

- An administrator account that obtains the operation permission has been used to log in to OceanStor DeviceManager. The following administrators have the permission:
  - Super administrator
  - Administrator
- An HTTP share directory has been created.

Preparing Data

Parameter	Description	Setting
HTTP Service	Global control over the enable and disable status of the HTTP sharing service. If this parameter is set to disable, all the other parameter configurations become invalid. **NOTE** ● By default, the storage system provides the HTTPS service certificate. You are advised to replace the certificate with the private certificate before accessing HTTPS shares. After the certificate is replaced, the CA certificate of the storage system must be imported for the browser to eliminate security alarms. As the service IP address is used to access the HTTPS service, alarm **This website's address does not match the address in the security certificate** cannot be cleared. ● When the HTTP service is disabled, the system automatically deletes information about shared file systems and directories. When the HTTP service is enabled again, configure the HTTP shared file systems and directories.	[Example] Enable
Max. Number of Connections	Maximum number of HTTP share connections allowed by the system. **NOTE** The maximum number of connections varies depending on the device model.	[Value range] 1 to 256

Parameter	Description	Setting
HTTP Default Port	Only the HTTPS port is enabled for the storage system when the HTTP service is enabled. To enable the HTTP port, select **Enable**. NOTE Exercise caution when enabling the HTTP port.	[Example] Enable
Share Path	Share Path that you want to share over HTTP. This parameter contains **File System** and **Folder**. ● File System, File system that owns the directory that you want to share over HTTP. ● **Optional:** Folder, Folder that you want to share over HTTP.	[Example] File System test_001
DAV	DAV, also known as WebDAV (Web-based Distributed Authoring and Versioning), is a communication protocol based on HTTP. Once WebDAV enabled, the system allows the DAV client to read/write the shared directory, and supports file locking, file unlocking, and file version control.	[Example] Enable

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Settings** > **Storage Settings** > **File Storage Service** > **HTTP Service**.

Step 3 Modify HTTP service parameters based on the planned data.

Step 4 Click **Save**.

----End

5.9.3 Disabling the HTTP Service

By performing this operation, you can disable the HTTP service of a storage system.

Precautions

If you disable the HTTP service, it will be unavailable. Before performing this operation, ensure that you do not need the HTTP service.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Settings** > **Storage Settings** > **File Storage Service** > **HTTP Service**.

Step 3 In **HTTP Service**, deselect **Enable**.

Step 4 Click **Save**.

The **Warning** dialog box is displayed.

Step 5 Confirm the information in the dialog box and select **I have read and understood the consequences associated with performing this operation**. Then click **OK**.

The **Success** dialog box is displayed.

Step 6 Click **OK**.

----End

5.10 Configuring and Managing Authentication Users

Authentication users are for accessing file system shares you create. Authentication users include local authentication users and user groups.

5.10.1 Viewing Local Authentication User Group Information

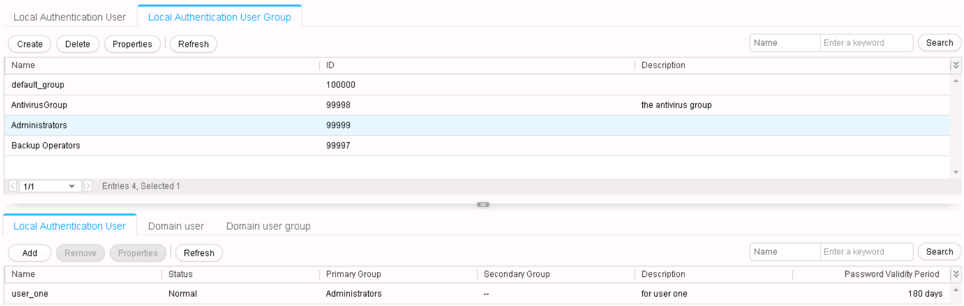
View the information about a local authentication user group. The information includes user group name, description and information of users in this group.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Provisioning** > **User Authentication** > **Local Authentication User Group**.

Step 3 Check the local authentication user group information. The parameters are as shown in **5.10.1 Viewing Local Authentication User Group Information**.



Name	ID	Description
default_group	100000	
AntivirusGroup	99998	the antivirus group
Administrators	99999	
Backup Operators	99997	

Entries 4, Selected 1

Name	Status	Primary Group	Secondary Group	Description	Password Validity Period
user_one	Normal	Administrators	--	for user one	180 days

Table 5-41 Local Authentication User Group Information

Parameter	Description
Name	The name of a local authentication user group.

Parameter	Description
ID	The ID of a local authentication user group.
Description	The description of a local authentication user group.

Step 4 In the user group list, select a user group you want to check. Select the **Local Authentication User** tab, check the information of local users in this user group. The parameters are as shown in **Table 5-42**.

Table 5-42 Local Authentication User Information

Parameter	Description
Name	The name of a local authentication user.
Status	The status of a local authentication user. The status includes: ● Normal: the user can access the share. ● Lock: the user cannot access the share.
Primary Group	The primary user group a local authentication user belongs to.
Secondary Group	The secondary user group a local authentication user belongs to. The secondary user group can be empty.
Description	The description of a local authentication user.
Password Validity Period	The password validity days. When the password is beyond the validity days, it displays as **Expired**. NOTE The local authentication user with expired password cannot access share. You need to reset the password to access the share normally.

Step 5 In the user group list, select a user group you want to check. Select the **Domain User** tab, check the information of domain users in this user group. The parameters are as shown in **Table 5-43**.

Table 5-43 Domain User Information

Parameter	Description
Name	The name of a domain user.
ID	The ID of a domain user.

Step 6 In the user group list, select a user group you want to check. Select the **Domain User Group** tab, check the information of domain user groups in this user group. The parameters are as shown in **Table 5-44**.

Table 5-44 Domain User Group Information

Parameter	Description
Name	The name of a domain user group.
ID	The ID of a domain user group.

----End

5.10.2 Viewing Local Authentication User Information

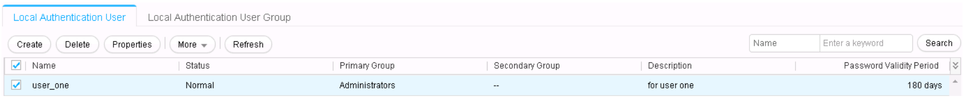
View the information about a local authentication user. The information includes name, status, primary group, secondary group, description and so on.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Provisioning** > **User Authentication**.

Step 3 Check the local authentication user information. The parameters are shown as in **5.10.2 Viewing Local Authentication User Information**.



☑ Name	Status	Primary Group	Secondary Group	Description	Password Validity Period
☑ user_one	Normal	Administrators	--	for user one	180 days

Table 5-45 Local Authentication User Information

Parameter	Description
Name	The name of a local authentication user.
Status	The status of a local authentication user. The status includes: ● Normal: the user can access the share. ● Lock: the user cannot access the share.
ID	The ID of a local authentication user.
Primary Group	The primary user group a local authentication user belongs to.
Secondary Group	The secondary user group a local authentication user belongs to. The secondary user group can be empty.

Parameter	Description
Description	The description of a local authentication user.
Password Validity Period	The password validity days. When the password is beyond the validity days, it displays as **Expired**. NOTE The local authentication user with expired password cannot access share. You need to reset the password to access the share normally.

----End

5.10.3 Deleting a Local Authentication User

After a local authentication user is deleted, it can no longer access a CIFS share. You can delete related Homedir share of a local authentication user when deleting the local authentication user.

Context

If the local user that you want to delete has been added to a local group, the local user is removed from the local group after the local user is deleted.

The change of the local authentication user or domain user (including the user is disabled or deleted, user password is changed or expires, and the owning group of the user is changed) that access a CIFS/FTP/NFS share takes effect after the user is authenticated again. You can mount the share again to trigger the authentication.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Provisioning** > **User Authentication**.

Step 3 Select the local authentication user that you want to delete.

Step 4 Click **Delete**.

The security alert dialog box is displayed.

Step 5 Confirm the information in the dialog box and select **I have read and understand the consequences associated with performing this operation**. Then click **OK**.

The **Execution Result** dialog box is displayed.

Step 6 Click **Close** to finish deleting a local authentication user.

----End

5.10.4 Deleting a Local Authentication User Group

After a local authentication user group is deleted, the user group cannot access a CIFS share any more, but users in the user group can access CIFS shared resources as authentication users.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Provisioning** > **User Authentication** > **Local Authentication User Group**.

Step 3 Select the local authentication user group that you want to delete.

Step 4 Click **Delete**.

The security alert dialog box is displayed.

Step 5 Confirm the information in the dialog box and select **I have read and understand the consequences associated with performing this operation**. Then click **OK**.

The **Success** dialog box is displayed.

Step 6 Click **OK** to finish deleting a local authentication user group.

----End

5.10.5 Locking a Local Authentication User

To prevent a local authentication user from accessing a share, lock the user. A locked local authentication user cannot access any share. You can enable the authentication user for the user to access shares.

Prerequisites

The local authentication user must be unlocked, therefore the **Status** of a local authentication user is **Normal**.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Provisioning** > **User Authentication**.

Step 3 Select a local authentication user and choose **More** > **Lock**.

The **Execution Result** dialog box is displayed.

Step 4 Check the execution result and click **Close** to finish locking a local authentication user.

The **Status** of the user is **Lock**.

----End

5.10.6 Enabling a Local Authentication User

A locked local authentication user cannot access any share. You can enable the authentication user for it to access shares.

Prerequisites

The local authentication user must be locked, therefore the **Status** of a local authentication user is **Lock**.

Context

A newly created local authentication user is enabled by default. The **Status** of this user is **Normal**.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Provisioning** > **User Authentication**.

Step 3 Select a local authentication user and choose **More** > **Enable**.

The **Execution Result** dialog box is displayed.

Step 4 Check the execution result and click **Close** to finish enabling a local authentication user.

Status of the user is **Normal**.

----End

5.10.7 Modifying the Properties of Local Authentication User

This operation enables you to change the password, modify the primary group and the description of a local authentication user.

Context

The change of the local authentication user or domain user (including the user is disabled or deleted, user password is changed or expires, and the owning group of the user is changed) that access a CIFS/FTP/NFS share takes effect after the user is authenticated again. You can mount the share again to trigger the authentication.

Procedure

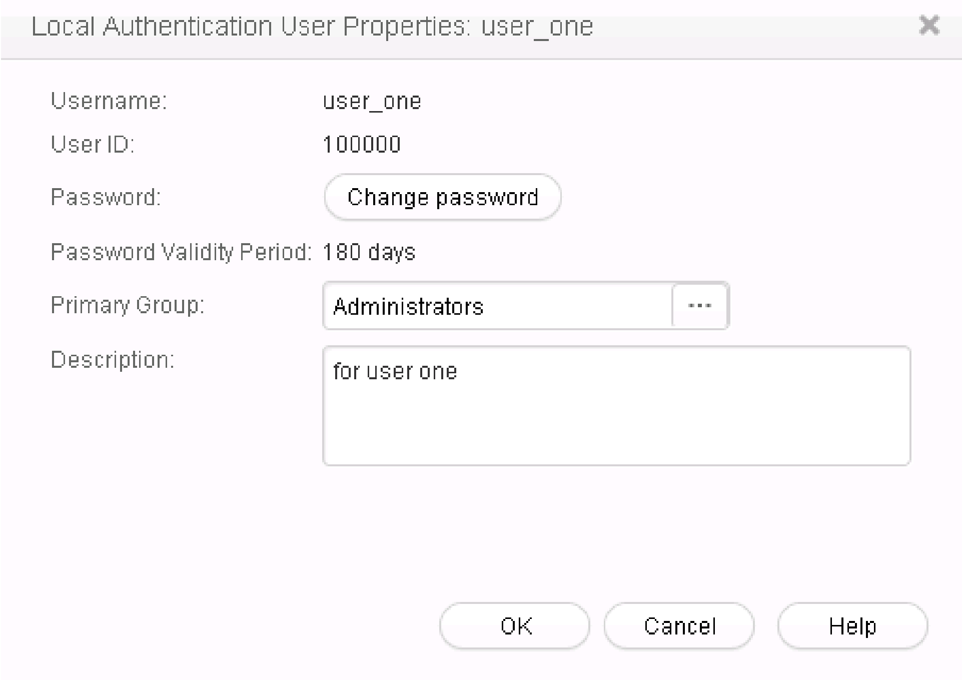
Step 1 Log in to DeviceManager.

Step 2 Choose **Provisioning** > **User Authentication**.

Step 3 Select the local authentication user whose properties you want to change.

Step 4 Click **Properties**.

The **Local Authentication User Properties** dialog box is displayed.



Local Authentication User Properties: user_one

Username: user_one

User ID: 100000

Password: Change password

Password Validity Period: 180 days

Primary Group: Administrators

Description: for user one

Step 5 Change the password of the local authentication user.

1. Click **Change password**.
2. In **New Password**, enter a new password.

   The system default password requirements are:

   - Contain 8 to 16 characters.
   - Contain special characters. Special characters include: !"#$%&'()*+,-./:;<=>?@[\]^`{_|}~ and space.
   - Contain any two types of the uppercase letters, lowercase letters, and digits.
   - Cannot contain three consecutive same characters.
   - Be different from the user name or the user name typed backwards.

   You can modify password security policy in **Set Security Policies**.
3. In **Confirm Password**, enter the new password again.

Step 6 Modify the primary group.

1. Click the **Primary Group** the local authentication user belongs to.

   The **Select Primary Group** dialog box is displayed.
2. In the user group list, select a new user group and click **OK**.
   The system goes back to **Local Authentication User Properties** dialog box.

Step 7 Modify the description of the local authentication user.

1. Enter the description of this local authentication user in **Description**.

Step 8 Click **OK**.
The **Success** dialog box is displayed.

Step 9 Click **OK** to finish modifying the properties of the local authentication user.

----End

5.10.8 Modifying the Secondary Group of a Local Authentication User

This operation enables you to modify the secondary group of a local authentication user.

Context

The change of the local authentication user or domain user (including the user is disabled or deleted, user password is changed or expires, and the owning group of the user is changed) that access a CIFS/FTP/NFS share takes effect after the user is authenticated again. You can mount the share again to trigger the authentication.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Provisioning** > **User Authentication**.

Step 3 Select the local authentication user whose secondary group you want to change.

Step 4 Click **More** > **Change Secondary Group**.

The **Change Secondary Group** dialog box is displayed.

Step 5 Change the secondary group of a local user.

1. To add a new user group, click **Add**.

   The **Select User Group** dialog box is displayed.

2. Select one user group or multiple user groups that you want to add and click **OK**.

   To remove a user group, select it and click **Remove**.

3. Click **OK**.
   The **Success** dialog box is displayed indicating that the operation succeeded.

4. Click **OK** to finish modifying the secondary group of a local authentication user.

----End

5.10.9 Modifying the Properties of Local Authentication User Group

This operation enables you to modify the description of a local authentication user group.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Provisioning** > **User Authentication** > **Local Authentication User Group**.

Step 3 Select the local user group you want to modify.

Step 4 Click **Properties**.

The **Local Authentication User Group Properties** is displayed.

Step 5 Modify the description of local authentication user group.

1. Enter new description of the local authentication user group in **Description**.
2. Click **OK**.

   The **Success** dialog box is displayed.

Step 6 Click **OK** to finish modifying the description.

----End

5.10.10 Adding/Removing a User to a Local Authentication User Group

This operation enables you to add/remove local authentication users, domain users or domain user groups from a local authentication user group.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Provisioning** > **User Authentication** > **Local Authentication User Group**.

Step 3 Select the local authentication user group that you want to modify.

Step 4 Add a local authentication user for the local authentication user group.

1. Click the **Local Authentication User** tab.
2. Click **Add**.

   The **Add User** dialog box is displayed.
3. Select the user or users that you want to add and click **OK**.

   The **Execution Result** dialog box is displayed.
4. Click **Close** to finish adding a local authentication user to the local authentication user group.

   NOTE

   If the primary group of the user to be added is the same as the user group to which the user is added, the primary group and secondary group of the user remain unchanged.

   If the primary group of the user to be added is different from the user group to which the user is added, the user group to which the user is added becomes the secondary group of the user.

Step 5 Remove a local authentication user from the local authentication user group.

1. Click the **Local Authentication User** tab.
2. Select the local authentication user that you want to remove.
3. Click **Remove**.

   The security alert dialog box is displayed.
4. Confirm the information in the dialog box and select **I have read and understand the consequences associated with performing this operation**. Then click **OK**.

The **Success** dialog box is displayed.

5. Click **OK** to finish removing a local authentication user from the local authentication user group.

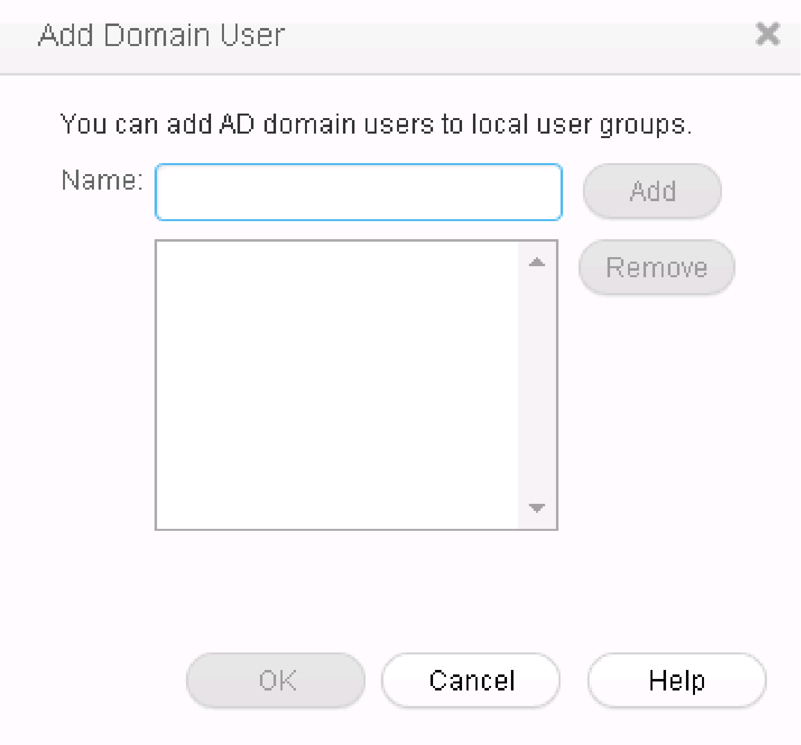
   NOTE

   The local authentication user cannot be removed from its primary group.

Step 6 Add a domain user for the local authentication user group.

1. Click the **Domain User** tab.
2. Click **Add**.

   The **Add Domain User** dialog box is displayed.



Add Domain User

You can add AD domain users to local user groups.

Name:

3. In **Name**, enter the domain user name, and click **Add**.

   NOTE

   The name format is **domain name\domain user name**.

4. Click **OK**.

   The **Execution Result** dialog box is displayed.

5. Click **Close** to add domain user to local authentication user group.

Step 7 Remove a domain user from the local authentication user group.

1. Click the **Domain User** tab.
2. Select the domain user that you want to remove.
3. Click **Remove**.

   The security alert dialog box is displayed.

4. Confirm the information in the dialog box and select **I have read and understand the consequences associated with performing this operation**. Then click **OK**.

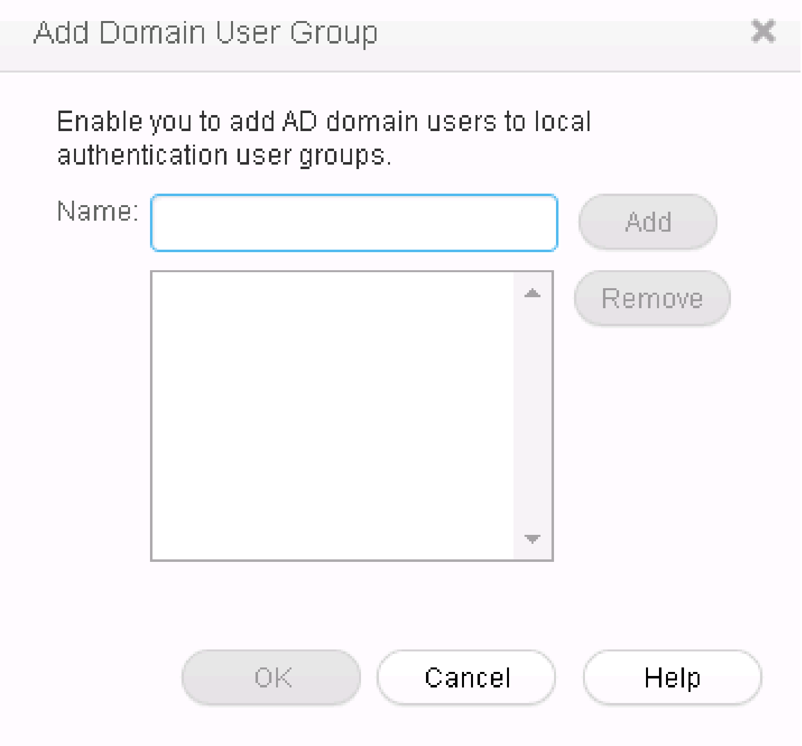
   The **Success** dialog box is displayed.

5. Click **OK** to remove a domain user from the local authentication user group.

Step 8 Add a domain user group for the local authentication user group.

1. Click the **Domain User Group** tab.
2. Click **Add**.

   The **Add Domain User Group** dialog box is displayed.



Add Domain User Group

Enable you to add AD domain users to local authentication user groups.

3. In **Name**, enter the domain user group name, and click **Add**.

   NOTE
   The name format is **domain name\domain user group name**.

4. Click **OK**.

   The **Execution Result** dialog box is displayed.

5. Click **Close** to add domain user group to local authentication user group.

Step 9 Remove a domain user group from the local authentication user group.

1. Click the **Domain User Group** tab.
2. Select the domain user group that you want to remove.
3. Click **Remove**.

   The security alert dialog box is displayed.

4. Confirm the information in the dialog box and select **I have read and understand the consequences associated with performing this operation**. Then click **OK**.

   The **Success** dialog box is displayed.

5. Click **OK** to remove a domain user group from the local authentication user group.

----End

5.10.11 Configuring Security Policy for Local Authentication User

Security policies include the password policy and login policy. Security policies are used to protect the system security.

Procedure

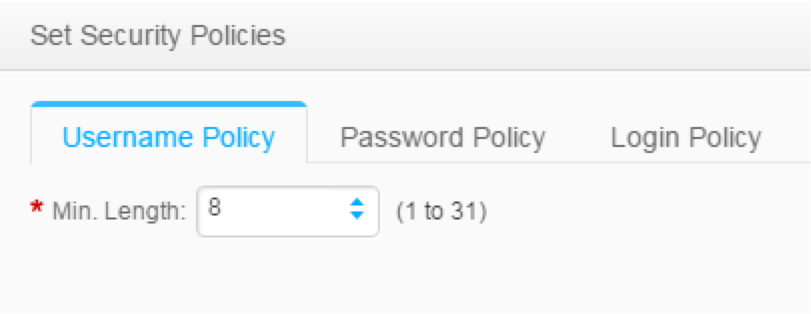
Step 1 Log in to DeviceManager.

Step 2 Choose **Provisioning** > **User Authentication**.

Step 3 Select **More** > **Set Security Policies**.

The **Set Security Policies** dialog box is displayed.

Step 4 Select **Username Policy** tab to configure local authentication user name policy. **Table 5-46** describes the related parameter.



Set Security Policies

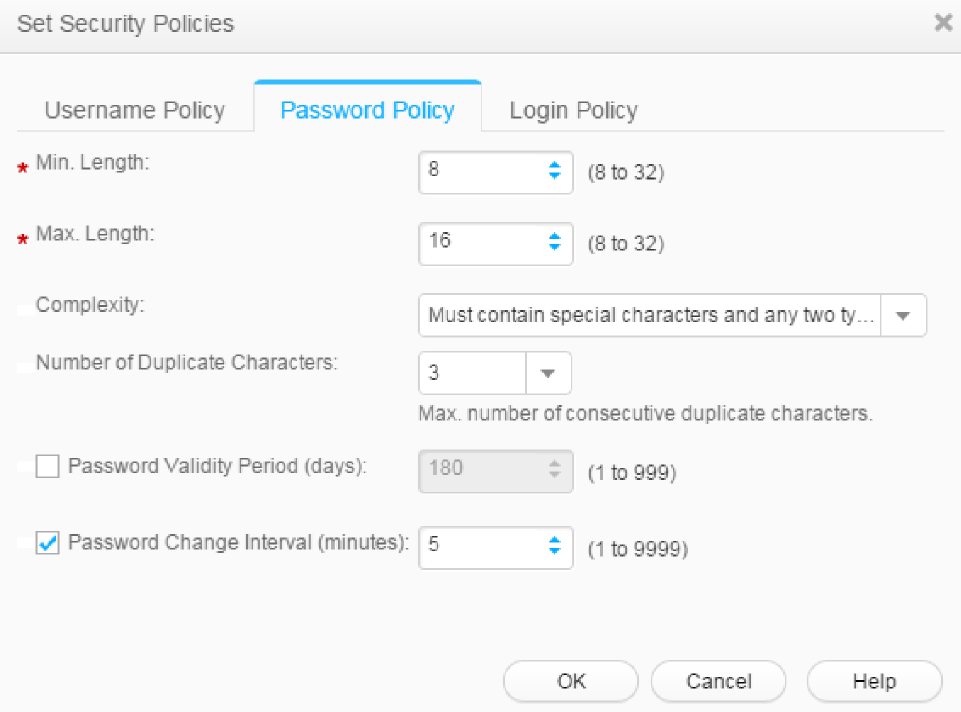
Username Policy | Password Policy | Login Policy

* Min. Length: 8 (1 to 31)

Table 5-46 Username Policy

Parameter	Description	Value
Min.Length	Minimum length of the user name. This parameter prevents user name being too short.	[Value range] Its value is an integer ranging from 1 to 31. [Default value] 8

Step 5 Select **Password Policy** tab to configure password policy for local authentication user. **Table 5-47** describes related parameters.



* Min. Length: 8 (8 to 32)

* Max. Length: 16 (8 to 32)

Complexity: Must contain special characters and any two ty...

Number of Duplicate Characters: 3

Max. number of consecutive duplicate characters.

□ Password Validity Period (days): 180 (1 to 999)

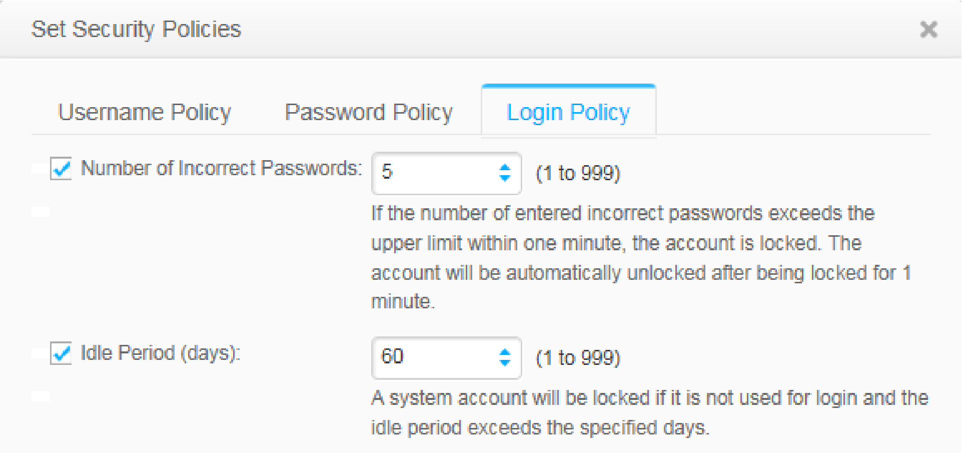
☑ Password Change Interval (minutes): 5 (1 to 9999)

Table 5-47 Password Policy

Parameter	Description	Value
Min. Length	Minimum length of the user password. This parameter prevents password being too short.	[Value range] Its value is an integer ranging from 8 to 32. [Default value] 8
Max. Length	Maximum length of the user password. This parameter prevents password being lengthy.	[Value range] Its value is an integer ranging from 8 to 32. [Default value] 16
Complexity	Complexity of the user password. This parameter prevents password being too simple. The complexity types include: ● Must contain special characters and any two types of uppercase letters, lowercase letters and digits ● Must contain special characters, uppercase letters, lowercase letters and digits	[Default value] **Contains special characters and any two types of uppercase letters, lowercase letters and digits**.

Parameter	Description	Value
Number of Duplicate Characters	Maximum number of consecutive duplicate characters.	[Value range] Its value is **Unlimited** or an integer ranging from 1 to 9. [Default value] 3
Password Validity Period (days)	Setting of the password's validity period. You are advised to enable **Password Validity Period (days)**. After **Password Validity Period (days)** is enabled, you need to set the password validity days. After the validity period of a password expires, the system prompts you to change the password in a timely manner. NOTE If this parameter is not selected, the password will never expire. To ensure storage system security, you are advised to select and set this parameter.	[Value range] Its value is an integer ranging from 1 to 999. [Default value] 180
Password Change Interval (minutes)	Change interval of a password.	[Value range] Its value is an integer ranging from 1 to 9999. [Default value] 5

Step 6 Select **Login Policy** tab to configure password policy for local authentication user. **Table 5-48** describe related parameters.



☑ Number of Incorrect Passwords: 5 (1 to 999)

If the number of entered incorrect passwords exceeds the upper limit within one minute, the account is locked. The account will be automatically unlocked after being locked for 1 minute.

☑ Idle Period (days): 60 (1 to 999)

A system account will be locked if it is not used for login and the idle period exceeds the specified days.

Table 5-48 Login Policy

Parameter	Description	Value
Number of Incorrect Passwords	Times allowed for consecutively entering incorrect passwords. After it has been enabled, within one minute, when incorrect passwords are input exceeds the **Number of Incorrect Passwords** times, the user account is automatically locked. The user account will be automatically unlocked after being locked for 1 minute.	[Value range] Its value is an integer ranging from 1 to 999. [Default value] 5
Idle Period (Days)	A local authentication user account will be locked if it is not used for login and the idle period exceeds the specified days.	[Value range] Its value is an integer ranging from 1 to 999. [Default value] 60

Step 7 Click **OK**.

The **Success** dialog box is displayed.

Step 8 Click **OK** to finish configuring security policies.

----End

5.11 User Mapping Management

User mappings enable you to access shares across different operating systems by using the mappings created locally or in the IDMU domain. This chapter describes how to manage user mappings.

5.11.1 Viewing User Mappings

This operation enables you to view the created user mappings.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Provisioning** > **User Authentication** > **User Mapping**.

Step 3 Browse the user mapping information. **Table 5-49** explains the related parameters.

Table 5-49 User mapping parameters

Parameter Name	Description
ID	A user mapping ID.

Parameter Name	Description
Mapping Type	A user mapping type related to the operating system, including: ● Windows to Unix: When accessing Unix shares using Windows, a Windows user has all the permissions granted to the target user. ● Unix to Windows: When accessing Windows shares using Unix, a Unix user has all the permissions granted to the target user.
Source User	The original user in a mapping.
Target User	The target user in a mapping.
Priority	When multiple mappings share the same original user, the system uses the mapping with the highest priority. **NOTE** Priority: A smaller number indicates a higher priority.

----End

5.11.2 Modifying a User Mapping

This operation enables you to modify the mapping type, original user, target user, mapping priority of a mapping. The modified mapping can be used to access shares.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Provisioning** > **User Authentication** > **User Mapping**.

Step 3 Select a user mapping that you want to modify and click **Properties**.

Step 4 Modify the parameters of the user mapping by referring to **Table 5-50**.

Table 5-50 User mapping parameters

Parameter Name	Description	Value
Mapping Type	A user mapping type related to the operating system, including: ● Windows to Unix: When accessing Unix shares using Windows, a Windows user has all the permissions granted to the target user. ● Unix to Windows: When accessing Windows shares using Unix, a Unix user has all the permissions granted to the target user.	[Example] Windows to Unix
Source User	The original user in a mapping.	[Example] sourceuser
Target User	The target user in a mapping. NOTE Click **Test** to check whether the target user exists.	[Example] targetuser
Priority	When multiple mappings share the same original user, the system uses the mapping with the highest priority. NOTE A smaller number indicates a higher priority.	[Example] 32

Step 5 Click **OK**.

Step 6 Click **Close**.

----End

5.11.3 Deleting a User Mapping

This section introduces how to delete a user mapping. After the deletion, the original user cannot be mapped to the specific target user and access shares across different systems.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Provisioning** > **User Authentication** > **User Mapping**.

Step 3 Select a user mapping that you want to delete and click **Delete**.

The security alert dialog box is displayed.

Step 4 Confirm the information in the dialog box and select **I have read and understand the consequences associated with performing this operation.**. Then click **OK**.

The **Execution Result** dialog box is displayed.

Step 5 Click **Close** to complete deleting the user mapping.

----End

5.12 Operations

The following operations enable you to manage Ethernet ports, VLANs, FC port, FCoE port, port group, bond port and logical ports.

5.12.1 Viewing Bit Error Statistics

You can learn about the data transmission quality of a storage device port by checking its bit error statistics. The access performance of application servers deteriorates upon a high bit error rate.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **System**.

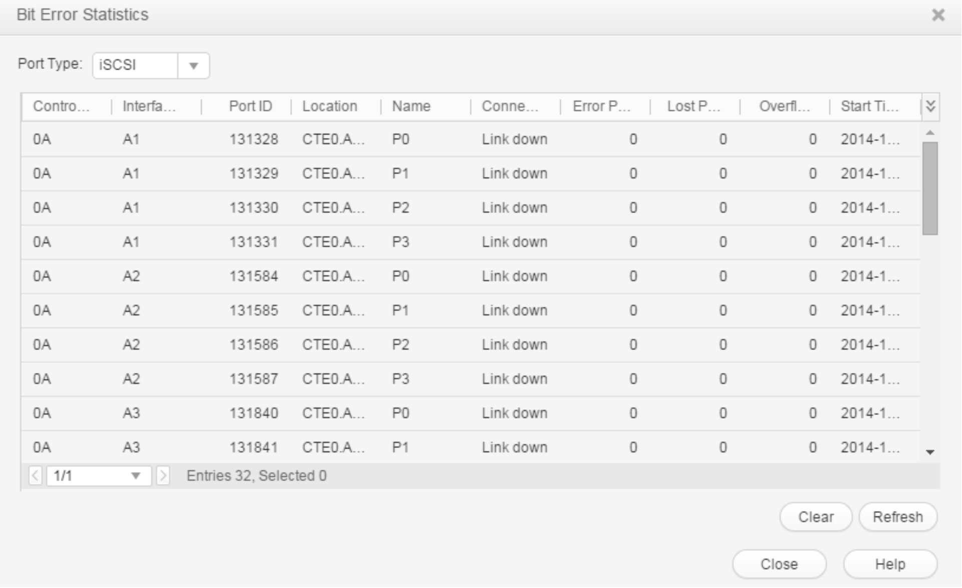
Step 3 Click the controller enclosure where the bonded Ethernet ports reside.

Step 4 Click to switch to the rear view.

Step 5 Click the Ethernet port you want to view.

Step 6 In the lower function pane, click **Bit Error Statistics**.

The **Bit Error Statistics** dialog box is displayed.



Bit Error Statistics

Port Type: iSCSI

Contro...	Interfa...	Port ID	Location	Name	Conne...	Error P...	Lost P...	Overfl...	Start Ti...
0A	A1	131328	CTE0.A...	P0	Link down	0	0	0	2014-1...
0A	A1	131329	CTE0.A...	P1	Link down	0	0	0	2014-1...
0A	A1	131330	CTE0.A...	P2	Link down	0	0	0	2014-1...
0A	A1	131331	CTE0.A...	P3	Link down	0	0	0	2014-1...
0A	A2	131584	CTE0.A...	P0	Link down	0	0	0	2014-1...
0A	A2	131585	CTE0.A...	P1	Link down	0	0	0	2014-1...
0A	A2	131586	CTE0.A...	P2	Link down	0	0	0	2014-1...
0A	A2	131587	CTE0.A...	P3	Link down	0	0	0	2014-1...
0A	A3	131840	CTE0.A...	P0	Link down	0	0	0	2014-1...
0A	A3	131841	CTE0.A...	P1	Link down	0	0	0	2014-1...

1/1 Entries 32, Selected 0

Step 7 View bit error information about the Ethernet port.

1. Select **iSCSI** from **Port Type**.
2. From the port list, select the port and view bit error statistics.

   NOTE

   To clear bit error statistics, click **Clear**.

----End

5.12.2 Managing Routes

If cross-segment data transmission is required in an iSCSI network, this operation guides you to configure routes, enabling cross-segment data transmission.

Prerequisites

The IP address of an Ethernet port has been configured.

NOTE

On redundant links, you must configure IP addresses and route for multiple Ethernet ports.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **System**.

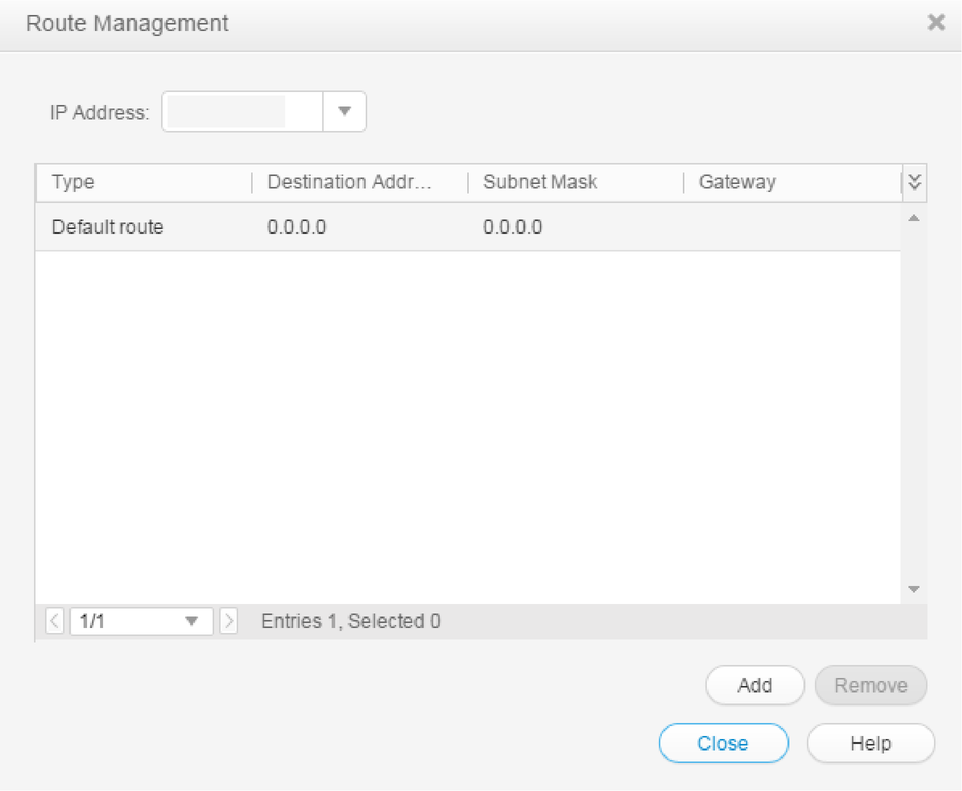
Step 3 Select the controller enclosure where the Ethernet ports reside.

Step 4 Click to switch to the rear view.

Step 5 Click the Ethernet port that you want to configure.

Step 6 Click **Route Management**.

The **Route Management** dialog box is displayed.



Type	Destination Addr...	Subnet Mask	Gateway
Default route	0.0.0.0	0.0.0.0	

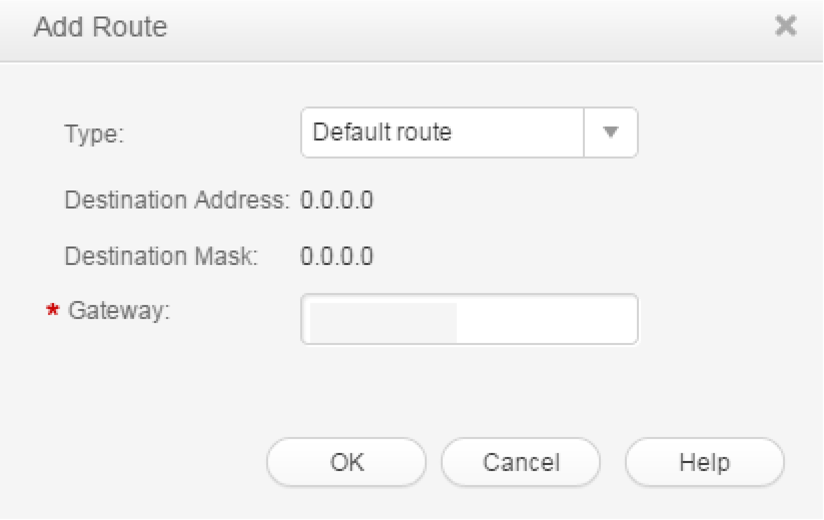
Step 7 Set route information for the Ethernet port.

NOTICE

- The default internal heartbeat IP addresses of a dual-controller storage system are **127.127.127.10** and **127.127.127.11**, and those of a four-controller storage system are **127.127.127.10**, **127.127.127.11**, **127.127.127.12**, and **127.127.127.13**. Therefore, the IP address of the router cannot fall within the 127.127.127.XXX segment. Additionally, the IP address of the gateway cannot be **127.127.127.10**, **127.127.127.11**, **127.127.127.12**, or **127.127.127.13**. Otherwise, routing will fail.
- Internal heartbeat links are established between controllers for the controllers to detect each other's working status. Heartbeat links do not require separate cable connections. In addition, internal heartbeat IP addresses have been assigned before delivery and cannot be changed.

1. In **IP Address**, select the IP address of the Ethernet port.
2. Click **Add**.

   The **Add Route** dialog box is displayed.



Type: Default route

Destination Address: 0.0.0.0

Destination Mask: 0.0.0.0

* Gateway:

3. In the text box of **Type**, select the type of the route to be added and the route parameters. **Table 5-51** describes related parameters.

Table 5-51 Route parameters

Parameter	Description
Type	There are three route options: – **Default route** The route through which data is forwarded by default if no preferred route is available. The destination address field and the destination mask field (IPv4) or prefix (IPv6) of the default route are automatically set to 0. To use this option, simply add a gateway. – **Host route** A route to an individual host. The destination mask (IPv4) or prefix (IPv6) of the host route is automatically set to 255.255.255.255 or 128. To use this option, add the destination address and a gateway. – **Network segment route** The route to a network segment. To use this option, add the destination address, the destination address mask (IPv4) or prefix (IPv6), and gateway.
Destination address	IPv4\IPv6 address or network segment of the storage device's Ethernet port or the application server's service network port that connects to the storage device's Ethernet port.

Parameter	Description
Destination mask/Prefix	Subnet mask of the IPv4 address or the prefix of the IPv6 address for the storage device's Ethernet port or the application server's service network port that connects to the storage device's Ethernet port.
Gateway	Gateway where the IP address of the Ethernet port on the local storage system resides.

Step 8 Confirm the route management operation.

1. Click **OK**. The route information is added to the route list.

   The security alert dialog box is displayed.

2. Confirm the information in the dialog box and select **I have read the previous information and understand subsequences of the operation.**.

3. Click **OK**.

   The **Success** dialog box is displayed, indicating that the operation succeeded.

   NOTE

   To delete a route, select the route and click **Remove**.

4. Click **Close**.

----End

5.12.3 Viewing Ethernet Port Details

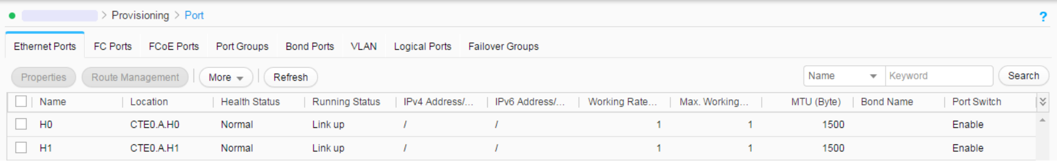
This operation enables you to view the operating status and health status of an Ethernet port.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Provisioning** > **Port** > **Ethernet Ports**.

Step 3 View details about an Ethernet port. The related parameters are described in **Table 5-52**.



□	Name	Location	Health Status	Running Status	IPv4 Address/...	IPv6 Address/...	Working Rate...	Max. Working...	MTU (Byte)	Bond Name	Port Switch
□	H0	CTE0.A.H0	Normal	Link up	/	/	1	1	1500		Enable
□	H1	CTE0.A.H1	Normal	Link up	/	/	1	1	1500		Enable

Table 5-52 Ethernet port parameters

Parameter	Description	Value
Name	Name of an Ethernet port.	[Example] P0
Location	Location of an Ethernet port.	[Example] CTE0.A.IOM0.P0
Health Status	Health status of an Ethernet port.	[Example] Normal
Running Status	Running status of an Ethernet port.	[Example] Link up
MAC Address	MAC address of an Ethernet port.	[Example] 04:f9:38:95:88:f1
IPv4 Address/Mask	IPv4 address and mask of an Ethernet port.	[Example] 192.168.100.11/255.255.255.0
IPv6 Address/Prefix	IPv6 address and prefix of an Ethernet port.	[Example] fc::1234/64
Working Rate (Gbit/s)	Transfer rate of an Ethernet port.	[Example] 1
Max. Working Rate (Gbit/s)	Maximum transfer rate of an Ethernet port.	[Example] 1
MTU (Byte)	Maximum transmission unit (MTU) of an Ethernet port.	[Example] 1500
Bond Name	Name of the bond port.	[Example] as
Port Switch	Isolation status of an Ethernet port. Possible values are **Enable** and **Disable**. When **Port Switch** is set to **Disable**, the port cannot be used.	[Example] Enable
ID	ID of an Ethernet port.	[Example] 139267

Step 4 **Optional:** Select a port and the details about the initiator to which the port belongs will be displayed in the **Initiator** area, as shown in **Table 5-53**.

Table 5-53 Initiator parameter

Parameter	Description
Type	Type of an initiator.
Alias	Alias of an initiator.
WWPN/IQN	The unique identifier of an initiator.
Status	Status of an initiator.
Idle or Not	Whether initiator is idle or not.

Step 5 **Optional:** Associate an initiator with a host.

1. Select an initiator that you want to associate with a host.
2. Click **Associate Host**.

   The **Associate Host** dialog box is displayed.
3. Select a host with which you want to associate the initiator and click **OK**.

   The system associates the host with the initiator.

Step 6 **Optional:** Select an initiator and click **Create Host** to create a new host and associate it with the selected initiator. **Table 5-54** describes the related parameters.

Table 5-54 Host parameters

Parameter	Description	Value
Name	Name of a host. Name a host in accordance with the following rules so that the host is available to host applications. ● The name must be unique. ● The name can contain only letters, digits, periods (.), underscores (_), and hyphens (-). ● The name contains 1 to 31 characters.	[Example] Host002
Description	Description of a host.	[Example] -

Parameter	Description	Value
OS	Operating system used by a host.	[Value range] Possible values are **Linux**, **Windows**, **Solaris**, **HP-UX**, **AIX**, **XenServer**, **Mac OS**, **VMware ESX**, **Windows Server 2012**, **Oracle VM** and **OpenVMS**. NOTE Use **Windows Server 2012** operating system only when the host needs to access the thin LUN and use the space reclaiming function. [Example] Windows
IP Address	IP address of a host.	[Example] 192.168.1.100
Device Location	Location of a host.	[Example] Chengdu

----End

5.12.4 Modifying the Properties of an Ethernet Port

When the network changes, modify the Ethernet port parameters to ensure that the storage system can communicate correctly with the application servers.

Context

Note the following when modifying the properties of an Ethernet port:

- Changing the IP address of the Ethernet port will interrupt the ongoing services. Check whether a redundant path exists between the storage system and host. If there is no redundant path, stop the services on the application server. Do not change the IP address of the Ethernet port unless necessary.
- The IP addresses of the Ethernet port and internal heartbeat must be on different network segments. The default IP addresses of the internal heartbeat on the dual-controller storage system are **127.127.127.10** and **127.127.127.11**, and the default IP addresses of the internal heartbeat on the four-controller storage system are **127.127.127.10**, **127.127.127.11**, **127.127.127.12**, and **127.127.127.13**. (Internal heartbeat links are established between controllers for these controllers to detect each other's working status. You do not need to separately connect cables. In addition, internal heartbeat IP addresses have been assigned before delivery, and you cannot change these IP addresses).
- The IP addresses of the Ethernet port and management network port must be on different network segments.
- The IP addresses of the Ethernet port and maintenance network port must be on different network segments.

- The IP address of the Ethernet port must be on the same network segment as that of its connected service network port on the application server or that of its connected Ethernet port on another storage system. If the network segment has insufficient available IP addresses, add a route.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Provisioning** > **Port** > **Ethernet Ports**.

Step 3 Select an Ethernet port and click **Properties**.

The **Properties of Port** dialog box is displayed.

1. Click **General** tab.
2. In the **IPv4 Address** or **IPv6 Address** text box, enter an IP address for the Ethernet port.
3. In the **Subnet Mask** or **Prefix** area, enter the subnet mask or prefix of the Ethernet port.
4. In the **MTU (Byte)** text box, enter the maximum size of a data packet that can be transferred between the Ethernet port and the application server.
5. **Optional:** Click **Owning Port Group** tab, view the owning port group information of Ethernet port.
6. **Optional:** Click **VLAN** tab, view the VLAN information of Ethernet port.
7. **Optional:** Click **Logical Ports** tab, view the logical ports information of Ethernet port.

Step 4 Confirm that you want to modify the properties of the Ethernet port.

1. Click **OK**.

   The security alert dialog box is displayed.
2. Confirm the information of the dialog box and select **I have read and understand the consequences associated with performing this operation.**.
3. Click **OK**.

   The **Execution Result** dialog box is displayed indicating that the operation succeeded.
4. Click **OK**.

----End

5.12.5 Viewing VLAN Details

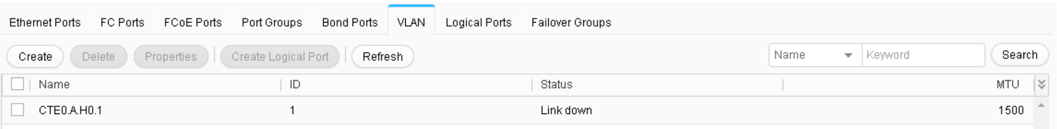
This operation enables you to view the name, ID, status, and maximum transmission unit (MTU) of a virtual local area network (VLAN).

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Provisioning** > **Port** > **VLAN**.

Step 3 View details about a VLAN. The related parameters are described in **Table 5-55**.



□	Name	ID	Status	MTU
□	CTE0.A.H0.1	1	Link down	1500

Table 5-55 VLAN parameters

Parameter	Description	Value
Name	VLAN name.	[Example] CTE0.A.IOM0.P1.2
ID	VLAN ID.	[Example] 2
Status	VLAN connection status.	[Example] Link down
MTU	VLAN maximum transmission unit (MTU).	[Example] 1500

----End

5.12.6 Modifying VLAN Properties

This operation enables you to change the maximum transmission unit (MTU) of a VLAN to meet the transfer rate requirements.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Provisioning** > **Port** > **VLAN**.

Step 3 Select the VLAN whose properties you want to modify and click **Properties**.

The **VLAN Properties** dialog box is displayed and listing the selected port.

Step 4 In **MTU**, enter the allowed maximum MTU.

NOTE

The size of a packet transferred between a port and a host cannot exceed the MTU of the Ethernet port.

Step 5 Click **OK**.

The **Success** dialog box is displayed indicating that the operation succeeded.

Step 6 Click **OK**.

----End

5.12.7 Deleting a VLAN

This operation enables you to delete a virtual local area network (VLAN), and deleting a VLAN may interrupt services running on the VLAN.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Provisioning** > **Port** > **VLAN**.

Step 3 In the middle function pane, select a VLAN and click **Delete**.

The security alert dialog box is displayed.

Step 4 Confirm the information of the dialog box and select **I have read and understand the consequences associated with performing this operation.**.

Step 5 Click **OK**.

The **Execution Result** dialog box is displayed.

Step 6 Click **Close**.

----End

5.12.8 Viewing Logical Port Details

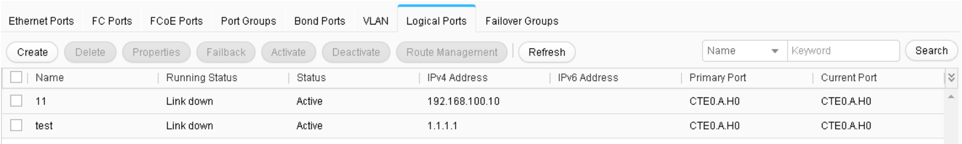
This operation enables you to view the information such as ID, name, running status, status, IPv4 address, IPv6 address, and current port of a logical port.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Provisioning** > **Port** > **Logical Ports**.

Step 3 View logical port information. The related parameters are described in **Table 5-56**.



□	Name	Running Status	Status	IPv4 Address	IPv6 Address	Primary Port	Current Port
□	11	Link down	Active	192.168.100.10		CTE0.A.H0	CTE0.A.H0
□	test	Link down	Active	1.1.1.1		CTE0.A.H0	CTE0.A.H0

Table 5-56 Logical port parameters

Parameter	Description	Value
ID	ID of the logical port.	[Example] 4278321152

Parameter	Description	Value
Name	Name of the logical port. The name must meet the following requirements so that the logical port is available to compatible applications: ● The name must be unique. ● The name can contain only letters, digits, underscores (_), periods (.), and hyphens (-). ● The name contains 1 to 31 characters.	[Example] Lif01
Running Status	Operating status of the logical port to which the logical port belongs.	[Example] Link up
Status	Operating status of the logical port.	[Example] Active
IPv4 Address	IPv4 address of the logical port.	[Example] 192.168.100.11
IPv6 Address	IPv6 address of the logical port.	[Example] None
Primary Port	The primary port to which the logical port belongs.	[Example] CTE0.A.H0
Current Port	The current port to which the logical port belongs.	[Example] CTE0.A.H0

Parameter	Description	Value
Role	Roles of logical ports include the following: ● Management: The port is used by a super administrator to log in to the system for management. ● Service: The port is used by a super administrator to access services such as file system CIFS shares. ● Management+Service: The port is used by a super administrator to log in to the system to manage the system and access services.	[Example] Service
Dynamic DNS	When the dynamic DNS is enabled, the DNS service will automatically and periodically update the IP address configured for the logical port.	[Example] Enable
Data Protocol	Network protocol used for accessing data via the logical port.	[Example] NFS+CIFS
Manage Access Mode	Management mode for the logical port.	[Example] WEB+REST API
DNS Zone	Name of the DNS zone. **NOTE** ● If the value is blank, the logical port is not used for DNS-based load balancing. ● This parameter is only supported in V300R006C10 and later versions.	[Example] None

Parameter	Description	Value
Listen DNS Query Request	After this function is enabled, external NEs can access the DNS service provided by the storage system by using the IP address of this logical port. **NOTE** This parameter is only supported in V300R006C10 and later versions.	[Example] Enable
vStore Name	Name of the owning vStore of the logical port.	[Example] vStore000
vStore ID	ID of the owning vStore of the logical port.	[Example] 1

----End

5.12.9 Modifying the Properties of a Logical Port

This operation enables you to modify the properties of a logical port.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Provisioning** > **Port** > **Logical Ports**.

Step 3 Modify the basic information of a logical port.

1. Select a logical port and click **Properties**.

   The **Logical Port Properties** page is displayed.

2. In the **Logical Port Properties** dialog box, configure related parameters.

   The related parameters are described in **Table 5-57**.

Table 5-57 Logical port parameters

Parameter	Description	Value
Name	Name of the logical port. The name must meet the following requirements so that the logical port is available to compatible applications: – The name must be unique. – The name can contain only letters, digits, underscores (_), periods (.), and hyphens (-). – The name contains 1 to 31 characters.	[Example] Lif01
IP Address Type	IP address type of the logical port, IPv4 address or IPv6 address.	[Example] IPv4 address
IPv4 Address	IPv4 address of the logical port.	[Example] 192.168.100.11
Subnet Mask	IPv4 subnet mask of the logical port.	[Example] 255.255.255.0
IPv4 Gateway	IPv4 gateway of the logical port.	[Example] 192.168.100.1
IPv6 Address	IPv6 address of the logical port.	[Example] fc00::1234
Prefix	IPv6 prefix length of the logical port.	[Example] 64
IPv6 Gateway	IPv6 gateway of the logical port.	[Example] fc00::1
Status	The status of a logical port.	[Example] Inactive
Primary Port	Port to which the logical port belongs, including the Ethernet port, Bond port, and VLAN.	[Example] None

Parameter	Description	Value
Failover Group	Failover group name. **NOTE** – If a failover group is specified, services on the failed primary port will be taken over by a port in the specified failover group. – If no failover group is specified, services on the failed primary port will be taken over by a port in the default failover group.	[Example] None
IP Address Failover	After IP address failover is enabled, services are failed over to other normal ports within the failover group if the primary port fails. However, the IP address used by services remains unchanged. **NOTE** Shares of file systems do not support the multipathing mode. IP address failover is used to improve reliability of links.	[Example] Enable

Parameter	Description	Value
Failback Mode	Mode in which services fail back to the primary port after the primary port is recovered. The mode can be manual or automatic. **NOTE** – If **Failback Mode** is **Manual**, ensure that the link to the primary port is normal before the failback. Services will manually fail back to the primary port only when the link to the primary port keeps normal for over five minutes. – If **Failback Mode** is **Automatic**, ensure that the link to the primary port is normal before the failback. Services will auto fail back to the primary port only when the link to the primary port keeps normal for over five minutes.	[Example] Automatic
Role	Roles of logical ports include the following: – Management: The port is used by a super administrator to log in to the system for management. – Service: The port is used by a super administrator to access services such as file system CIFS shares. – Management+Service: The port is used by a super administrator to log in to the system to manage the system and access services.	[Example] Service

Parameter	Description	Value
Dynamic DNS	When the dynamic DNS is enabled, the DNS service will automatically and periodically update the IP address configured for the logical port.	[Example] Enable
Listen DNS Query Request	After this function is enabled, external NEs can access the DNS service provided by the storage system by using the IP address of this logical port.	[Example] Enable
DNS Zone	Name of the DNS zone. **NOTE** The value of DNS zone is blank. The logical port is not used for DNS-based load balancing.	[Example] None
Data Protocol	Network protocol used for accessing data via the logical port.	[Example] NFS+CIFS
Manage Access Mode	Management mode for the logical port.	[Example] WEB+REST API
vStore Name	Name of the owning vStore of the logical port.	[Example] vStore000

Step 4 Click **OK**.

The security alert dialog box is displayed.

Step 5 Confirm the information of the dialog box and select **I have read and understand the consequences associated with performing this operation.**.

Step 6 Click **OK**.

----End

5.12.10 Activating a Logical Port

This operation enables you to activate a logical port for managing and accessing NAS.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Provisioning** > **Port** > **Logical Ports**.

Step 3 In the middle function pane, select a logical port and click **Activate**.

The security alert dialog box is displayed.

Step 4 Confirm the information of the dialog box and select **I have read and understand the consequences associated with performing this operation.**, click **OK**.

The **Execution Result** dialog box is displayed.

Step 5 Click **Close**.

----End

5.12.11 Deactivating a Logical Port

This operation enables you to deactivate a logical port.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Provisioning** > **Port** > **Logical Ports**.

Step 3 Select a logical port and click **Deactivate**.

The security alert dialog box is displayed.

Step 4 Confirm the information of the dialog box and select **I have read and understand the consequences associated with performing this operation.**.

Step 5 Click **OK**.

The **Execution Result** dialog box is displayed.

Step 6 Click **Close**.

----End

5.12.12 Deleting a Logical Port

This operation enables you to delete a logical port.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Provisioning** > **Port** > **Logical Ports**.

Step 3 In the middle function pane, select a logical port and click **Delete**.

The security alert dialog box is displayed.

Step 4 Confirm the information of the dialog box and select **I have read and understand the consequences associated with performing this operation.**.

Step 5 Click **OK**.

The **Execution Result** dialog box is displayed.

Step 6 Click **Close**.

----End

5.12.13 (Optional) Creating a Bond Port

This section describes how to bond Ethernet ports on a same controller.

Prerequisites

Ethernet ports that have IP addresses cannot be bound. The IP addresses of the bonded host ports need to be cleared before bonding.

Context

- Port bonding provides more bandwidth and redundancy for links. Although ports are bonded, each host still transmits data through a single port and the total bandwidth can be increased only when there are multiple hosts. Determine whether to bond ports based on site requirements.
- The port bond mode of a storage system has the following restrictions:
  - On the same controller, a bond port is formed by a maximum of eight Ethernet ports.
  - Only the interface modules with the same port rate (GE or 10GE) can be bonded.
  - The port cannot be bonded across controllers. Non-Ethernet network ports cannot be bonded.
  - SmartIO interface modules cannot be bonded if they work in cluster or FC mode or run FCoE service in FCoE/iSCSI mode.
  - Read-only users are unable to bind Ethernet ports.
  - Each port only allows to be added to one bonded port. It cannot be added to multiple bonded ports.
  - Ports are bonded to create a bond port that cannot be added to the port group.
- After Ethernet ports are bonded, **MTU** changes to the default value and you must set the link aggregation mode for the ports. For example, on Huawei switches, you must set the ports to the static LACP mode.

  NOTE

  The detailed link aggregation mode varies with the switches' manufacturer.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Provisioning** > **Port** > **Bond Ports**.

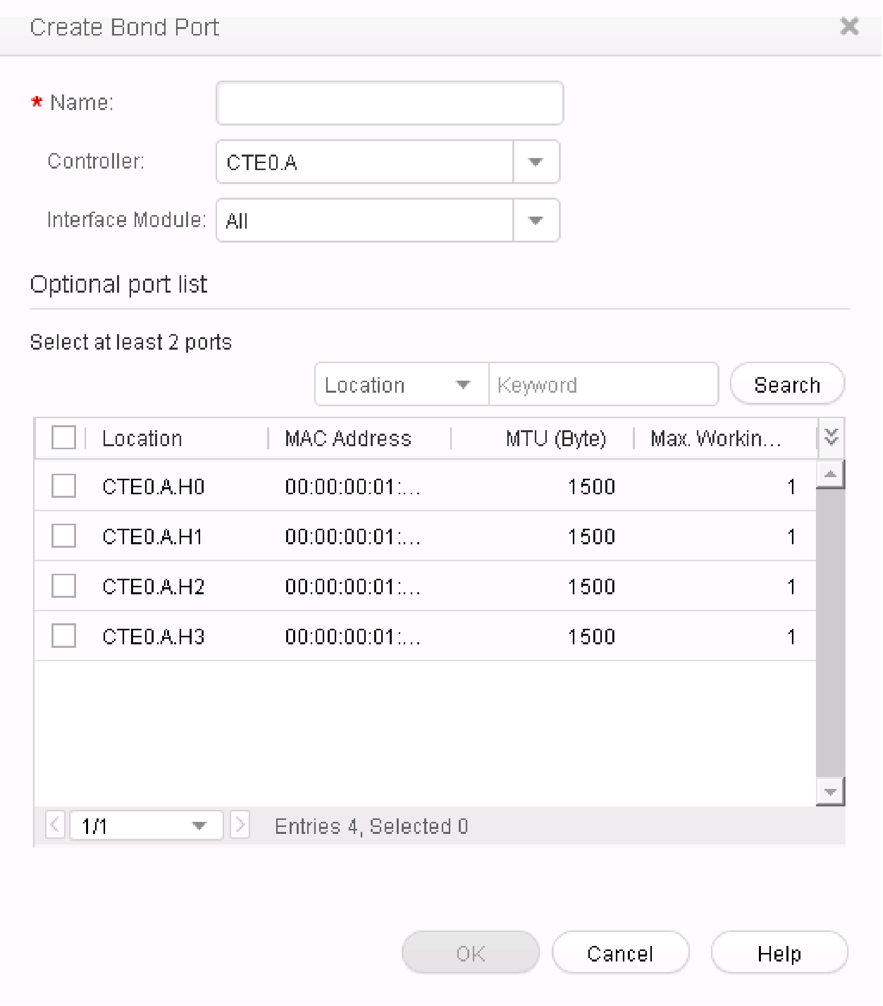
Step 3 Click **Create**.

The **Create Bond Port** dialog box is displayed.

NOTE

The port name format is **controller enclosure ID.interface module ID.port ID**.

Step 4 Set the name, interface module, and optional ports that can be bonded with the current Ethernet port.



Create Bond Port

* Name:

Controller: CTE0.A

Interface Module: All

Optional port list

Select at least 2 ports

□	Location	MAC Address	MTU (Byte)	Max. Workin...
□	CTE0.A.H0	00:00:00:01:...	1500	1
□	CTE0.A.H1	00:00:00:01:...	1500	1
□	CTE0.A.H2	00:00:00:01:...	1500	1
□	CTE0.A.H3	00:00:00:01:...	1500	1

1/1 Entries 4, Selected 0

1. In **Name**, enter a name for the bond port.

   The name:

   - Contains only letters, digits, underscores (_), periods (.), and hyphens (-).
   - Contains 1 to 31 characters.
2. From the **Controller**, select the controller the Ethernet ports own to.
3. Select the **Interface Module**.
4. From the **Optional port list**, select the Ethernet ports you want to bond.

   NOTE

   Select at least two ports.
5. Click **OK**.

   The security alert dialog box is displayed.

Step 5 Confirm that you want to bond these Ethernet ports.

1. Confirm the information of the dialog box and select **I have read and understand the consequences associated with performing this operation.**.
2. Click **OK**.

   The **Success** dialog box is displayed indicating that the operation succeeded.

3. Click **OK**.

----End

5.12.14 View Bonding Port

This section describes how to view the id, name, maximum transmission unit (MTU) and the number of ports bonded to the bond port.

Prerequisites

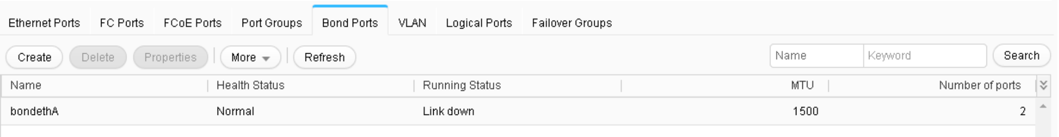
A bond port has been created.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Provisioning** > **Port** > **Bond Ports**.

Step 3 View bond port information. The related parameters are described in **Table 5-58**.



Name	Health Status	Running Status	MTU	Number of ports
bondethA	Normal	Link down	1500	2

Table 5-58 Bond port parameters

Parameter	Description
ID	ID of the bond port.
Name	Name of the bond port.
Health status	Health status of the bond port.
Running status	Running status of the bond port.
MTU	MTU of the bond port.
Number of ports	Number of Ethernet ports bonded into the bond port.

----End

5.12.15 Modifying the Properties of a Bonding Port

This section describes how to change the maximum transmission unit (MTU) of a bond port.

Prerequisites

- A bond port has been created.
- When the default value of MTU is changed, the changed MTU value takes effect only when it is the same as that on the peer switch and network adapter.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Provisioning** > **Port** > **Bond Ports**.

Step 3 Select the bond port whose properties you want to modify and click **Properties**.

Step 4 Modify **MTU**.

Step 5 Click **OK**.

The security alert dialog box is displayed.

Step 6 Confirm the information of the dialog box and select **I have read and understand the consequences associated with performing this operation.**.

Step 7 Click **OK**.

----End

5.12.16 Selecting a Primary Port

This section describes how to set or modify the primary port of a logical port.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Provisioning** > **Port** > **Logical Ports**.

Step 3 Click **Create**.

The **Create Logical Port** dialog box is displayed.

Step 4 On the **Primary Port** page, click **Browse**.

The **Select Primary Port** dialog box is displayed.

Step 5 In **Port Type**, select the primary port type.

The primary port types include Ethernet port, Bond port, and VLAN.

Step 6 In the port list, select the port.

Step 7 Click **OK**.

----End

6 FAQ

About This Chapter

This chapter describes FAQs related to the basic storage service configuration guide. You can also refer to this chapter when encountering faults during configurations or maintenance.

6.1 In a directory of a file system, why cannot I copy a file that has the same size as the directory to the directory?

Question

In a directory of a file system, why cannot I copy a file that has the same size as the directory to the directory?

Answer

When the Windows copy program copies local files to a file system, the file block size of the CIFS client is 4 KB, whereas the default file system block size of the storage system is 64 KB. If you copy a file smaller than 64 KB, the file occupies 64 KB space, wasting space. Therefore, you are advised to adjust the file system block size to ensure the full use of storage space.

6.2 What is a quota tree?

Question

What is a quota tree?

Answer

A quota tree is the root directory of a file system. File quantity and storage space under a quota tree can be managed.

6.3 What is a logical port?

Question

What is a logical port?

Answer

Its primary port will be floated to the peer controller.

Logical ports, used for file system service operation, are created based on Ethernet ports, bond ports, or VLANs. If a logical port carrying host services malfunctions, its primary port will be floated to the peer controller, imposing impact on system performance. If the controller malfunctions, the owning controller of the file system changes to and host services are switched to the peer controller, exerting an adverse impact on system performance.

6.4 What is the IP address floating policy?

Question

What is the IP address floating policy?

Answer

When a storage system is initialized, it automatically adds all Ethernet ports and bond ports to the default floating group. The priority of controllers for IP address floating is given to a port (at the same location) on the peer controller, then to a port (at another location) on the peer controller, and finally to a port on the current controller in the cluster. IP addresses can float between various interface modules. The port for the IP address floating policy is determined by the port location instead of the port rate.

6.5 Why is the allocated capacity of a newly created thin or thick file system 20%?

Question

Why is the allocated capacity of a newly created thin or thick file system 20%?

Answer

By default, 20% of storage system capacity is reserved for snapshots. You can change the value in the **Advanced** property of the file system.

6.6 After multiple Ethernet ports are bound, can I create a logical port based on one of the Ethernet ports?

Question

After multiple Ethernet ports are bound, can I create a logical port based on one of the Ethernet ports?

Answer

No.

6.7 What Is the Priority of Share Authentication When a Client Is Included in Multiple Share Permissions?

Question

When a client is included in multiple share permissions, what is the priority of its share authentication?

For example, if an NFS share of a file system is exported and two NFS share permissions are configured:

1. Use network group **my_netgroup:rw** (read-write) to configure. This network group contains the client whose IP address is A.A.A.A.
2. Use IP network **A.A.0.0:ro** (read-only) to configure.

When a client with IP address A.A.A.A mounts the NFS share, what is its permission?

Answer

Its permission is allocated based on the following priority from high to low: host name > IP address > IP network > wildcard > network group > * (anonymous). In the previous example, the share permission of the client matches that of IP network **A.A.0.0:ro** which is read-only. Therefore, the client has the read-only permission. In addition, if multiple permissions of the same priority are matched, use the latest permission that is configured.

6.8 How can I perform configuration and verification on the host after Access Based Enumeration (ABE) is enabled when the storage system creates a CIFS share?

Question

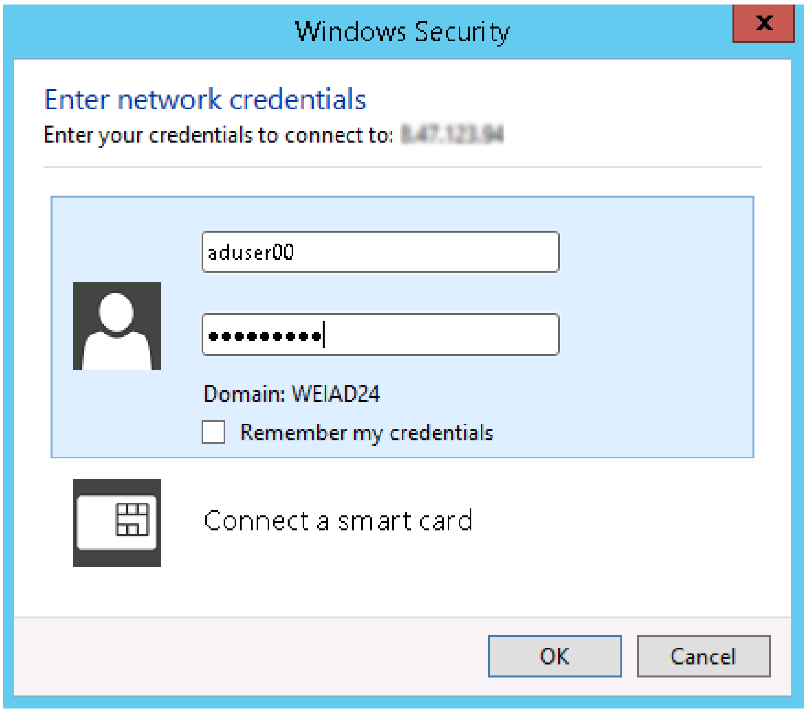
How can I perform configuration and verification on the host after ABE is enabled when the storage system creates a CIFS share?

Answer

After ABE is enabled, the share directory does not display files or file folders on which the user has no access permission. The following shows accessing a CIFS share on the host in the domain environment (also applicable to local authentication users).

1. The host accesses the CIFS share created by the storage system successfully. **Figure 6-1** shows share access by domain user **aduser00**.

Figure 6-1 The host accesses the CIFS share created by the storage system



Windows Security

Enter network credentials

Enter your credentials to connect to: [redacted]

aduser00

●●●●●●●●●

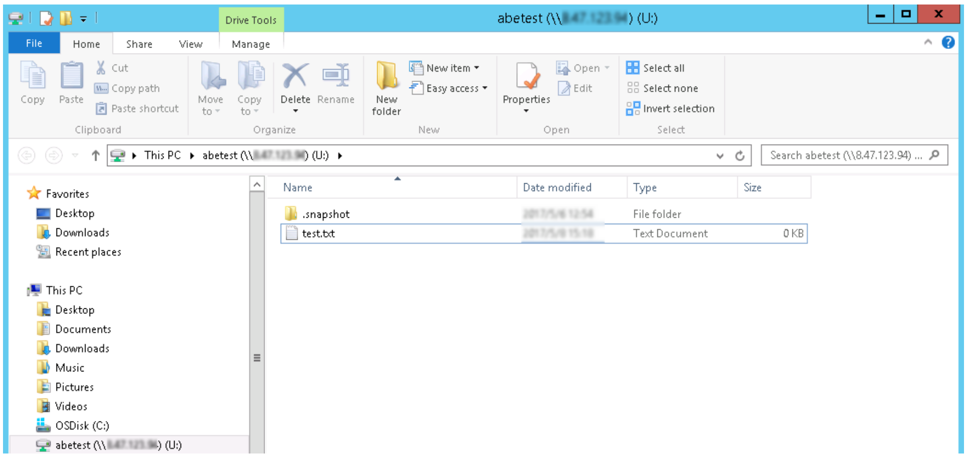
Domain: WEIAD24

□ Remember my credentials

Connect a smart card

2. Create file **test.txt** under the share path.**Figure 6-2** shows the result.

Figure 6-2 Create file under the share path



abetest (\\[redacted]) (U:)

This PC ▸ abetest (\\[redacted]) (U:) ▸

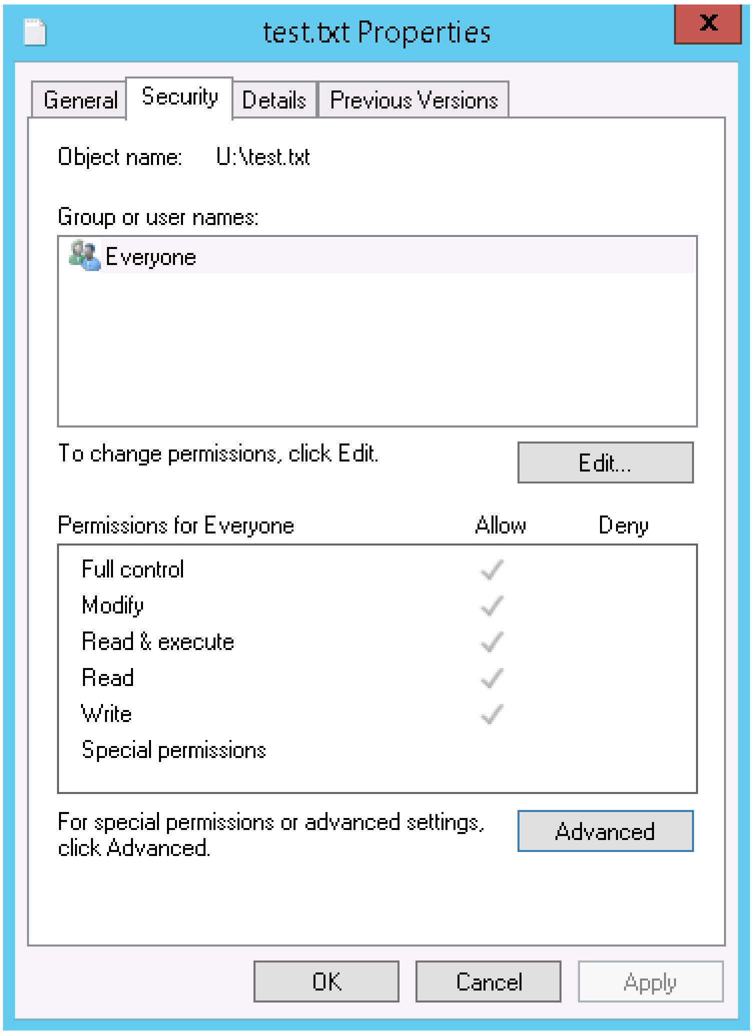
Search abetest (\\8.47.123.94) ...

Name	Date modified	Type	Size
.snapshot	[redacted]	File folder	
test.txt	[redacted]	Text Document	0 KB

3. Add permissions to domain users **aduser01** and **24aduser1** and remove the default permission of **Everyone**. If the default permission of **Everyone** is not removed, all users have full control over the file and can still view the file.

   Figure 6-3 shows how to modify the advanced settings of **test.txt**.

Figure 6-3 Modify the advanced settings



Object name: U:\test.txt

Group or user names:

Everyone

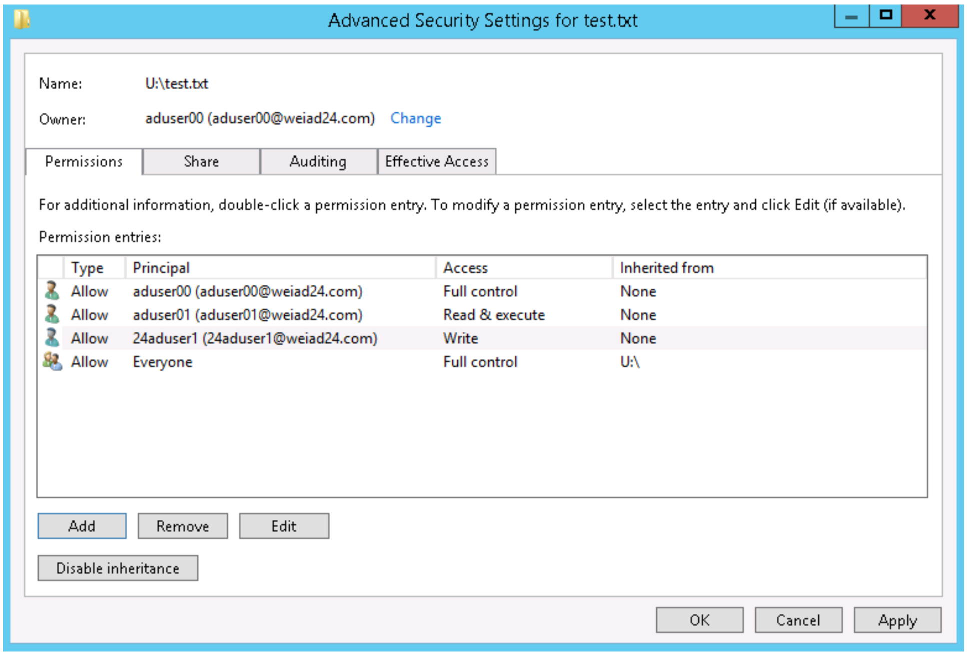
To change permissions, click Edit.

Permissions for Everyone	Allow	Deny
Full control	✓	
Modify	✓	
Read & execute	✓	
Read	✓	
Write	✓	
Special permissions		

For special permissions or advanced settings, click Advanced.

Figure 6-4 shows the advanced security settings before the default permission of **Everyone** is removed.

Figure 6-4 Before the default permission of Everyone is removed



Advanced Security Settings for test.txt

Name: U:\test.txt

Owner: aduser00 (aduser00@weiad24.com) Change

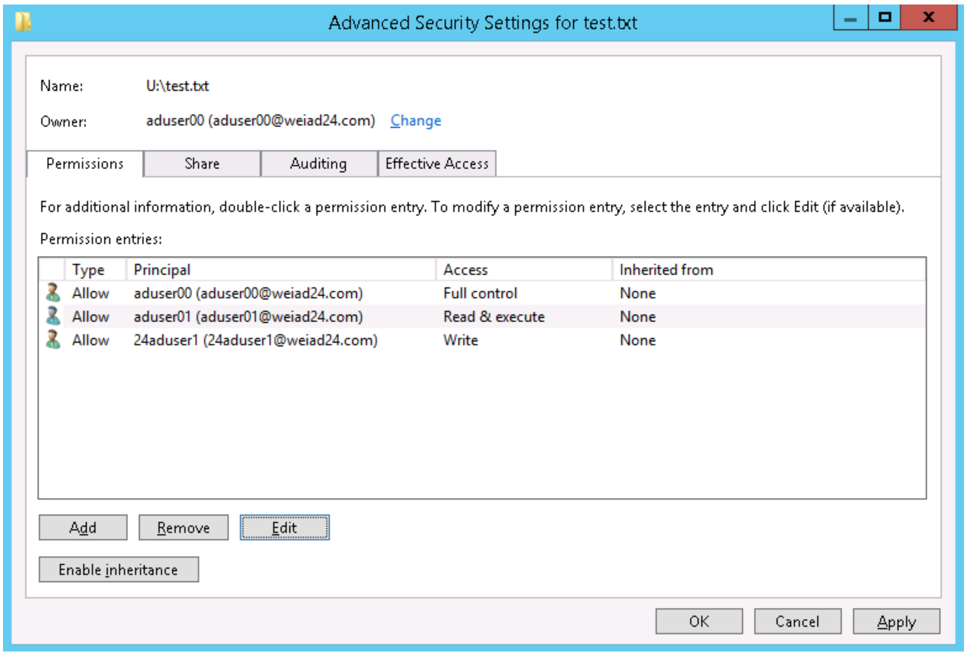
For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).

Permission entries:

Type	Principal	Access	Inherited from
Allow	aduser00 (aduser00@weiad24.com)	Full control	None
Allow	aduser01 (aduser01@weiad24.com)	Read & execute	None
Allow	24aduser1 (24aduser1@weiad24.com)	Write	None
Allow	Everyone	Full control	U:\

Figure 6-5 shows the advanced security settings after the default permission of **Everyone** is removed.

Figure 6-5 After the default permission of Everyone is removed



Advanced Security Settings for test.txt

Name: U:\test.txt

Owner: aduser00 (aduser00@weiad24.com) Change

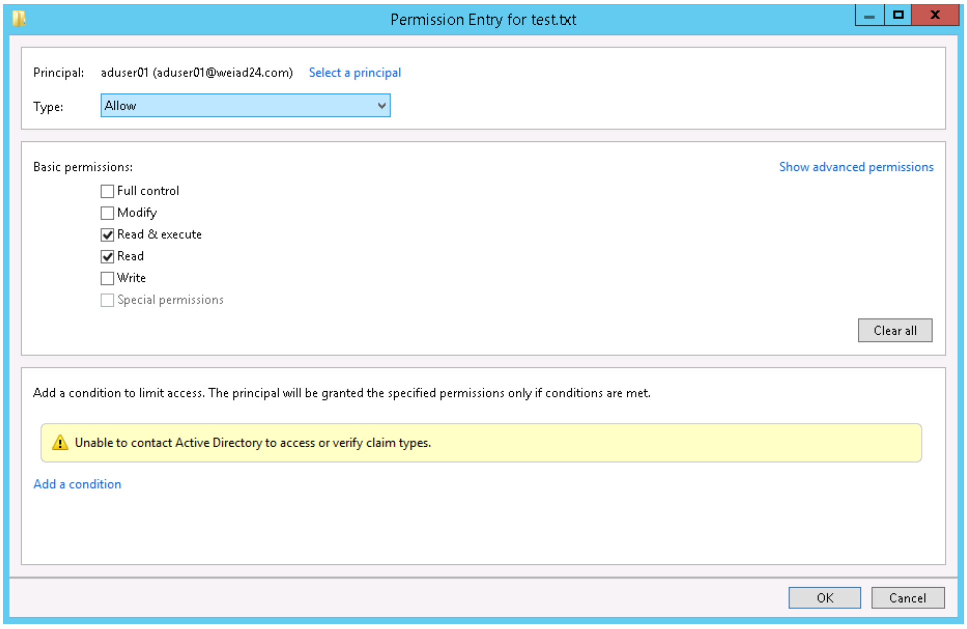
For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).

Permission entries:

Type	Principal	Access	Inherited from
Allow	aduser00 (aduser00@weiad24.com)	Full control	None
Allow	aduser01 (aduser01@weiad24.com)	Read & execute	None
Allow	24aduser1 (24aduser1@weiad24.com)	Write	None

Figure 6-6 shows the permission settings for domain user **aduser01**.

Figure 6-6 Permission settings for domain user aduser01


Permission Entry for test.txt

Principal: aduser01 (aduser01@weiad24.com) Select a principal

Type: Allow

Basic permissions: Show advanced permissions

- □ Full control
- □ Modify
- ☑ Read & execute
- ☑ Read
- □ Write
- □ Special permissions

Clear all

Add a condition to limit access. The principal will be granted the specified permissions only if conditions are met.

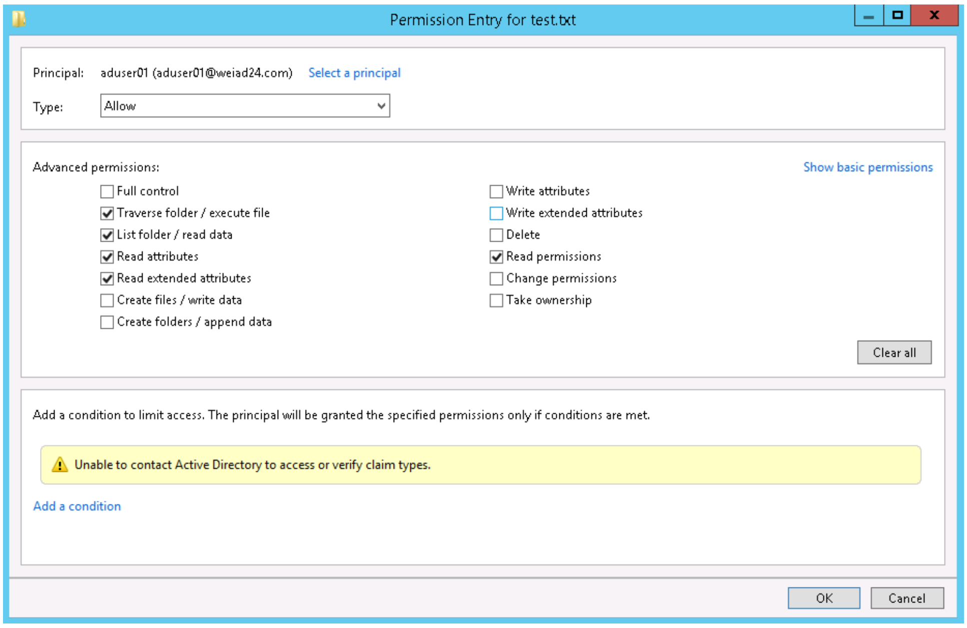
⚠ Unable to contact Active Directory to access or verify claim types.

Add a condition

OK Cancel

Figure 6-7 shows how to select **read data**, **read attributes**, **read extended attributes**, and **read permissions** to gain full read permissions.

Figure 6-7 Full read permissions


Permission Entry for test.txt

Principal: aduser01 (aduser01@weiad24.com) Select a principal

Type: Allow

Advanced permissions: Show basic permissions

- □ Full control
- ☑ Traverse folder / execute file
- ☑ List folder / read data
- ☑ Read attributes
- ☑ Read extended attributes
- □ Create files / write data
- □ Create folders / append data
- □ Write attributes
- □ Write extended attributes
- □ Delete
- ☑ Read permissions
- □ Change permissions
- □ Take ownership

Clear all

Add a condition to limit access. The principal will be granted the specified permissions only if conditions are met.

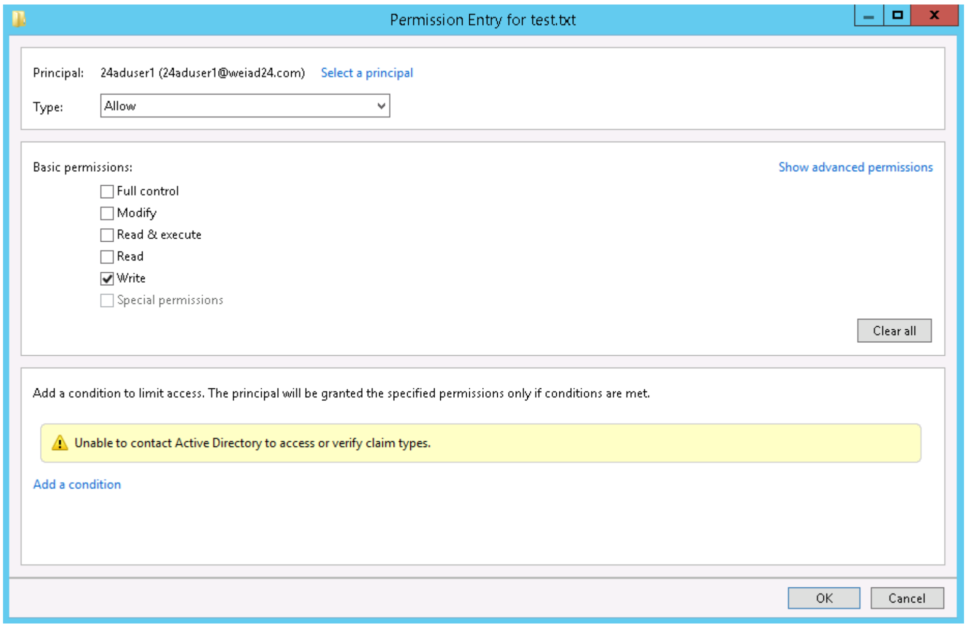
⚠ Unable to contact Active Directory to access or verify claim types.

Add a condition

OK Cancel

Figure 6-8 shows the permission settings for domain user **24aduser1**.

Figure 6-8 Permission settings for domain user 24aduser1


Permission Entry for test.txt

Principal: 24aduser1 (24aduser1@weiad24.com) Select a principal

Type: Allow

Basic permissions:

- □ Full control
- □ Modify
- □ Read & execute
- □ Read
- ☑ Write
- □ Special permissions

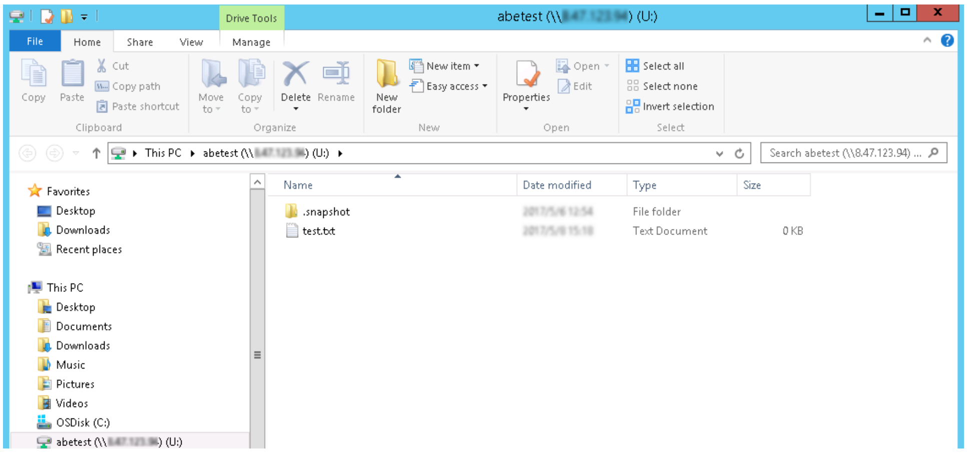
Add a condition to limit access. The principal will be granted the specified permissions only if conditions are met.

Unable to contact Active Directory to access or verify claim types.

4. View and check the files in the share path as domain users **aduser01** and **24aduser1**. The verification results are as follows:

   Figure 6-9 shows the verification results for domain user **aduser01**.

Figure 6-9 Verification results for domain user aduser01


abetest (\\[redacted]) (U:)

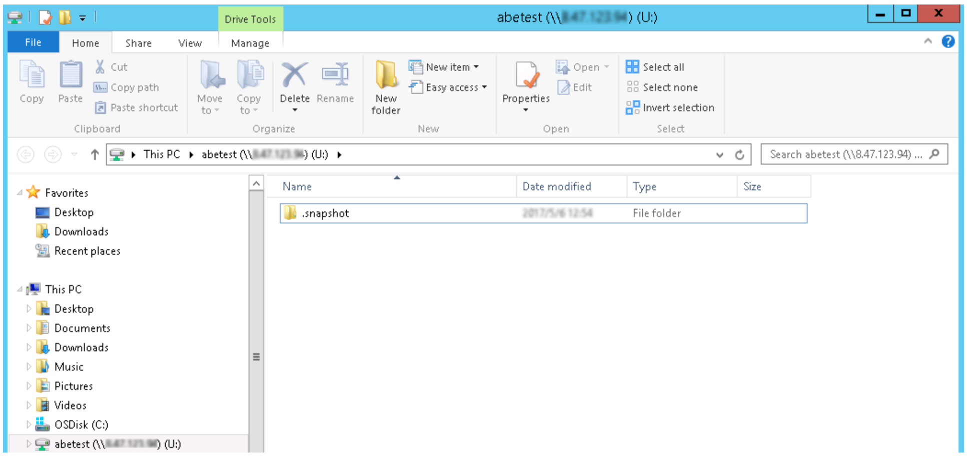
This PC ▸ abetest (\\[redacted]) (U:) ▸

Search abetest (\\8.47.123.94) ...

Name	Date modified	Type	Size
.snapshot	[redacted]	File folder	
test.txt	[redacted]	Text Document	0 KB

Figure 6-10 shows the verification results for domain user **24aduser1**.

Figure 6-10 Verification results for domain user 24aduser1



6.9 Restrictions on Mounting a CIFS Share in a Linux/MAC Environment

Question

What are the restrictions on mounting a CIFS share in a Linux/MAC environment?

Answer

In a Linux/MAC environment, you can run the **mount -cifs** command to mount a CIFS share. However, soft and hard links are not supported when you access files at a mount point.

- Hard link is the same file using multiple aliases (they have in common inode), it can be created by using **link** or **ln**.
- Soft link is a regular file, but the content of the file is the path name to point to another file, it can be created by using **ln** with arguments of *s*.

6.10 Restrictions on CIFS Share Mounting in Windows

Question

What are the restrictions on mounting a CIFS share (Homedire share) by mapping a network drive in Windows?

Answer

The restrictions on mounting a CIFS share in Windows are as follows:

- When CIFS shares with the same IP address (domain name or host name) are mounted in Windows, one or more CIFS shares can be mounted to one user. However, the same or different CIFS shares cannot be mounted to different users.
- When Homedire shares with the same IP address (domain name or host name) are mounted in Windows, multiple shares cannot be mounted to multiple users.

6.11 Permission for CIFS Shares

Question

If a user belongs to different user groups and the user and user groups have different permissions for a CIFS share, what are the user' new permissions for the CIFS share?

Answer

A user's permission on a CIFS share is the permission with the highest priority of the user or the user group. Priorities in the descending order are **Forbidden**, **Full control**, **Read and write** , and **Read-only**.

6.12 Precautions for Mounting CIFS Shares in Windows

Question

What are precautions for mounting common Internet file system (CIFS) shares in Windows?

Answer

- Before mounting CIFS shares, restart the operating system to prevent impacts of residual information.
- After uninstalling CIFS shares, run the **net -use** command to delete mounting information.
- When a domain client loads a CIFS share, the domain name can be the full domain name (domain name with a suffix, for example, **domain.com**) or short domain name (domain name without a suffix, for example, **domain**). Ensure that the domain account entered in the storage system is the same as that entered in the domain client.

6.13 Why Is an Error Displayed When You Copy a Folder Within a CIFS Share

Question

Why is an error displayed when you rename a folder and copy it in a CIFS share?

Answer

The folder is renamed after it is started by a client or application. It is not completely closed when you copy it. Therefore, an error is displayed. To solve this problem, completely close the folder started by the client or application and then copy it.

6.14 Can NFS Sharing Employ User Names and Passwords for Authentication?

Question

Can NFS sharing employ user names and passwords for authentication?

Answer

NFS sharing employs client identifiers (IP addresses and network groups) to restrict clients and cannot use user names and passwords for authentication.

6.15 After an NFS Share Is Mounted in Linux, Why Cannot I Create New Files on the Mount Point?

Question

After an NFS share is mounted in Linux, why cannot I create new files on the mount point?

Answer

Because the user mounts the NFS share after entering the mount point directory, the current directory remains a local directory although the mounting is successful. For this reason, files are created locally. In this situation, you need to enter the mount point and create files.

6.16 After the Storage System Is upgraded to the Version Supporting the GNS Feature, Why Cannot the File System Be Used as the Share Path for Creating a CIFS Share on MMC? (Applicable to V300R006C10 and Later Versions)

Question

After the storage system is upgraded to the version supporting the GNS feature, why cannot the file system be used as the share path for creating a CIFS share on MMC?

Answer

When upgrading the storage system to the version supporting the GNS feature, check whether a CIFS share whose **Share Name** is **c$** has been created. If yes, share **c$** will not be created again after the upgrade. You need to manually delete the share whose **Share Name** is **c$** and then a new share **c$** will be automatically created in the system. After the **c$** share is created, you can choose a file system as the share path when creating shares on MMC and do not need to manually enter the share path.

6.17 When the Versions of Primary and Secondary Storage Systems in the HyperMetro Pair Are Different, Why Does the Secondary Storage System Have No c$ Share? (Applicable to V300R006C10 and Later Versions)

Question

When the versions of primary and secondary storage systems in the HyperMetro pair are different, why does the secondary storage system have no c$ share?

Answer

For example, if the HyperMetro primary storage system is the new version that supports the GNS feature and the secondary storage system does not support the GNS feature, the c$ share at the primary end will not be synchronized to the secondary end. If share c$ needs to be used on the secondary end, upgrade the secondary storage system to the new version that supports the GNS feature.

A Permission Matrix for Self-defined Roles

Functional Module	Function	Function Description	Role Group
pool	disk_domain	Creates, deletes, modifies, and queries disk domains.	System group[a]
	disk_domain_readonly	Queries information about disk domains.	System group
	storage_pool	Creates, deletes, modifies, and queries storage pools.	System group
	storage_pool_readonly	Queries information about storage pools.	System group, vStore group[b]
	disk_readonly	Queries information about disks.	System group
	enclosure_readonly	Queries information about engines or disk enclosures.	System group
vstore	vstore	Creates, deletes, modifies, and queries vStores.	System group
	vstore_readonly	Querying information about vStores.	System group
lun	lun	Creates, modifies, deletes, and queries LUNs.	System group, vStore group
	lun_readonly	Queries information about LUNs.	System group, vStore group
	remote_resource	Manages the query of remote resources (file systems and LUNs).	System group, vStore group
	remote_resource_readonly	Queries remote resources (file systems and LUNs).	System group, vStore group
mapping_view	initiator	Creates, deletes, modifies, and queries initiators.	System group
	initiator_readonly	Query information about initiators.	System group

Functional Module	Function	Function Description	Role Group
	target	Creates, deletes, modifies, and queries targets.	System group
	target_readonly	Queries information about targets.	System group
	isns	Configures, deletes, and queries the IP address of an iSNS server.	System group
	isns_readonly	Queries the IP address of an iSNS server	System group
	mapping_view	Creates, deletes, modifies, and queries mapping views.	System group
	mapping_view_readonly	Queries information about mapping views.	System group
	lun_group	Creates, deletes, modifies, and queries LUN groups, as well as adds objects (LUNs and snapshots) to and removes objects from LUN groups.	System group
	lun_group_readonly	Queries information about LUN groups.	System group
	host_group	Creates, deletes, modifies, and queries host groups, as well adds hosts to or removes hosts from host groups.	System group
	host_group_readonly	Queries information about host groups.	System group
	host	Creates, deletes, modifies, and queries hosts, as well adds initiators to or removes initiators from hosts.	System group
	host_readonly	Queries information about hosts.	System group
	port_group	Creates, deletes, modifies, and queries port groups.	System group
	port_group_readonly	Queries information about port groups.	System group
file_system	file_system	Creates, deletes, modifies, and queries file systems.	System group, vStore group
	file_system_readonly	Query information about file systems.	System group, vStore group
quota	quota_tree	Creates, deletes, modifies, and queries quota trees in file systems.	System group, vStore group

Functional Module	Function	Function Description	Role Group
	quota_tree_readonly	Queries quota trees in file systems.	System group, vStore group
	quota	Creates, deletes, modifies, and queries quota in file systems.	System group, vStore group
	quota_readonly	Queries quota in file systems.	System group, vStore group
share	share	Creates, deletes, modifies, and queries shared services.	System group, vStore group
	share_readonly	Queries information about shared services.	System group, vStore group
file_storage_service	nfs_service	Configures and queries NFS service information.	System group, vStore group
	nfs_service_readonly	Queries NFS service information.	System group, vStore group
	cifs_service	Configures and queries CIFS service information.	System group, vStore group
	cifs_service_readonly	Queries CIFS service information.	System group, vStore group
	http_service	Configures and queries HTTP service information.	System group
	http_service_readonly	Queries HTTP service information.	System group
	ftp_service	Configures and queries FTP service information.	System group
	ftp_service_readonly	Queries FTP service information.	System group
resource_user	domain	Configures and queries domain authentication information.	System group, vStore group
	domain_readonly	Queries domain authentication information.	System group, vStore group
	resource_user	Creates, deletes, modifies, and queries authenticated users.	System group, vStore group
	resource_user_readonly	Queries information about authenticated users.	System group, vStore group
network	port	Adds, deletes, modifies, and queries ports.	System group

Functional Module	Function	Function Description	Role Group
	port_readonly	Queries information about ports.	System group, vStore group
	logical_port	Creates, deletes, modifies, and queries logical ports, as well as adds routes to or deletes routes from logical ports.	System group
	logical_port_readonly	Queries information about logical ports.	System group, vStore group
	vlan	Creates, deletes, modifies, and queries VLANs.	System group
	vlan_readonly	Queries information about VLANs.	System group, vStore group
	failover_group	Creates, modifies, deletes, and queries failover groups, as well as adds members to or removes members from failover groups.	System group
	failover_group_readonly	Queries information about failover groups.	System group, vStore group
	controller_readonly	Queries information about controllers.	System group
	interface_module_readonly	Queries information about interface modules.	System group
	dns_zone[d]	Creates, deletes, modifies, and queries DNS Zone.	System group
	dns_zone_readonly[d]	Queries information about DNS Zone.	System group, vStore group
local_data_protection	remote_device	Creates, deletes, modifies, and queries remote devices, as well as adds links to or deletes links from remote devices.	System group
	remote_device_readonly	Queries information about remote devices.	System group, vStore group
	remote_resource	Manages the query of remote resources (file systems and LUNs).	System group
	remote_resource_readonly	Queries remote resources (file systems and LUNs).	System group, vStore group

Functional Module	Function	Function Description	Role Group
	mirror_lun	Creates, deletes, modifies, and queries mirror LUNs, as well as adds mirror copies to or removes mirror copies from mirror LUNs.	System group
	mirror_lun_readonly	Queries information about mirror LUNs.	System group
	lun_snapshot	Creates, deletes, modifies, queries, activates, recreates, rolls back, cancels the rollback of, and creates copies for LUN snapshots.	System group
	lun_snapshot_readonly	Queries information about LUN snapshots.	System group
	lun_clone	Creates, deletes, modifies, queries, consistently splits, synchronizes, and reversely synchronizes clones, as well as adds pairs to or removes pairs from clones.	System group
	lun_clone_readonly	Queries information about clones.	System group
	fs_snapshot	Creates, deletes, modifies, queries, rolls back, and cancels the rollback of file system snapshots.	System group, vStore group
	fs_snapshot_readonly	Query information about file system snapshots.	System group, vStore group
	lun_copy	Creates, deletes, modifies, queries, suspends, continues, and stops LUN copy.	System group
	lun_copy_readonly	Queries information about LUN copy.	System group
remote_data_protection	remote_device	Creates, deletes, modifies, and queries remote devices, as well as adds links to or deletes links from remote devices.	System group
	remote_device_readonly	Queries information about remote devices.	System group, vStore group
	remote_resource	Manages the query of remote resources (file systems and LUNs).	System group
	remote_resource_readonly	Queries remote resources (file systems and LUNs).	System group, vStore group

Functional Module	Function	Function Description	Role Group
	hyper_vault	Creates, deletes, modifies, and queries HyperVault.	System group, vStore group
	hyper_vault_read only	Queries information about HyperVault.	System group, vStore group
	remote_replicatio n	Deletes, modifies, queries, synchronizes, and splits remote replication pairs, as well as switches primary/secondary resources and enables or cancels secondary resource protection for remote replication pairs.	System group, vStore group
	remote_replicatio n_readonly	Queries information about remote replication.	System group, vStore group
	ndmp_service	Modifies and queries NDMP service configuration.	System group, vStore group
	ndmp_service_re adonly	Queries NDMP service configuration.	System group, vStore group
	lun_group	Creates, deletes, modifies, and queries LUN groups, as well as adds objects (LUNs and snapshots) to and removes objects from LUN groups.	System group
	lun_group_reado nly	Queries information about LUN groups.	System group
	consistency_grou p	Creates, deletes, modifies, queries, synchronizes, and verifies consistency groups.	System group
	consistency_grou p_readonly	Queries information about consistency groups.	System group
	remote_replicatio n_vstore_pair[d]	Deletes, modifies, queries, synchronizes, and splits remote replication vStore pairs, as well as switches primary/secondary resources and enables or cancels secondary resource protection for remote replication vStore pairs.	System group
	remote_replicatio n_vstore_pair_rea donly[d]	Queries information about remote replication vStore pairs.	System group, vStore group

Functional Module	Function	Function Description	Role Group
hyper_metro	remote_device	Creates, deletes, modifies, and queries remote devices, as well as adds links to or deletes links from remote devices.	System group
	remote_device_readonly	Queries information about remote devices.	System group, vStore group
	remote_resource	Manages the query of remote resources (file systems and LUNs).	System group
	remote_resource_readonly	Queries remote resources (file systems and LUNs).	System group, vStore group
	hyper_metro_consistency_group	Creates, deletes, modifies, queries, starts, and stops HyperMetro consistency groups.	System group
	hyper_metro_consistency_group_readonly	Queries information about HyperMetro consistency groups.	System group, vStore group
	hyper_metro_domain	Creates, deletes, modifies, and queries HyperMetro domains, as well as adds quorum servers to or removes quorum servers from HyperMetro domains.	System group
	hyper_metro_domain_readonly	Queries information about HyperMetro domains.	System group, vStore group
	hyper_metro_pair	Creates, deletes, modifies, and queries HyperMetro pairs, as well as configures consistency check for HyperMetro pairs.	System group, vStore group
	hyper_metro_pair_readonly	Queries information about HyperMetro pairs.	System group, vStore group
	hyper_metro_vstore_pair	Creates, deletes, modifies, and queries HyperMetro vStore pairs, as well as configures consistency check for HyperMetro vStore pairs.	System group
	hyper_metro_vstore_pair_readonly	Queries information about HyperMetro vStore pairs.	System group, vStore group
	quorum_server	Creates, deletes, modifies, and queries quorum servers, as well as adds links to or removes links from quorum servers.	System group

Functional Module	Function	Function Description	Role Group
	quorum_server_readonly	Queries information about quorum servers.	System group, vStore group
resource_performance_tuning	smart_qos	Creates, modifies, deletes, and queries SmartQos policies, as well as adds objects (LUNs and file systems) to or removes objects from SmartQoS policies.	System group
	smart_qos_readonly	Queries information about SmartQoS policies.	System group
	smart_tier[c]	Configures and queries SmartTier polices (data migration policies or I/O monitoring policies).	System group
	smart_tier_readonly[c]	Queries information about SmartTier policies.	System group
	smart_partition	Creates, modifies, deletes, and queries smart partitions, as well as adds objects (LUNs and file systems) to or removes objects from smart partitions.	System group
	smart_partition_readonly	Queries information about smart partitions.	System group
	disk_readonly	Queries information about disks.	System group
	enclosure_readonly	Queries information about engines or disk enclosures.	System group
	smart_cache[c]	Creates, modifies, deletes, and queries SmartCaches, as well as adds objects (LUNs and file systems) to or removes objects from SmartCache.	System group
	smart_cache_readonly[c]	Queries information about SmartCache.	System group
	smart_migration	Creates, deletes, modifies, queries, consistently splits, and splits LUN migration.	System group
	smart_migration_readonly	Queries information about LUN migration.	System group
smart_virtualization	remote_resource	Manages the query of remote resources (file systems and LUNs).	System group, vStore group
	remote_resource_readonly	Queries remote resources (file systems and LUNs).	System group, vStore group

Functional Module	Function	Function Description	Role Group
	remote_device	Creates, deletes, modifies, and queries remote devices, as well as adds links to or deletes links from remote devices.	System group
	remote_device_readonly	Queries information about remote devices.	System group, vStore group
	port	Adds, deletes, modifies, and queries ports.	System group
	port_readonly	Queries information about ports.	System group
performance	performance	Configures and queries performance statistics policies.	System group
	performance_readonly	Queries information about performance statistics policies.	System group
	cifs_service_readonly	Queries CIFS service information.	System group
	nfs_service_readonly	Queries NFS service information.	System group
	lun_copy_readonly	Queries information about LUN copy.	System group
	share_readonly	Queries information about shared services.	System group
	controller_readonly	Queries information about controllers.	System group
	smart_qos_readonly	Queries information about SmartQoS policies.	System group
	disk_domain_readonly	Queries information about disk domains.	System group
	storage_pool_readonly	Queries information about storage pools.	System group
	smart_partition_readonly	Queries information about smart partitions.	System group
	host_readonly	Queries information about hosts.	System group
	remote_device_readonly	Queries information about remote devices.	System group
	remote_replication_readonly	Queries information about remote replication.	System group

Functional Module	Function	Function Description	Role Group
	file_system_readonly	Query information about file systems.	System group
	lun_readonly	Queries information about LUNs.	System group
	port_readonly	Queries information about ports.	System group
	lun_snapshot_readonly	Queries information about LUN snapshots.	System group
	disk_readonly	Queries information about disks.	System group
	enclosure_readonly	Queries information about engines or disk enclosures.	System group
a: Permissions that can only be configured for system roles b: Permissions that can be configured for both system and vStore roles c: Function is not supported by 2000F, 5000F, 6000F, 18000F series storage systems. d: Function is supported by V300R006C10 storage systems.			

B Obtaining and Configuring Manila Driver

Manila Driver is a plug-in that is deployed on the OpenStack Manila module. The plug-in can be used to provide functions such as the sharing configuration for virtual machines (VMs) in OpenStack.

Obtaining Manila Driver

You can obtain OpenStack Manila Driver by using either of the following methods:

- Obtain Manila Driver from the OpenStack community warehouse: Since the Kilo version, Huawei has contributed all of its storage drivers to the OpenStack community. OpenStack integrates Huawei's storage drivers. Users can download OpenStack drivers contributed to the OpenStack community. After OpenStack of the specified version is installed, you can find Manila Driver in **/manila/manila/share/drivers/huawei**.

  NOTE

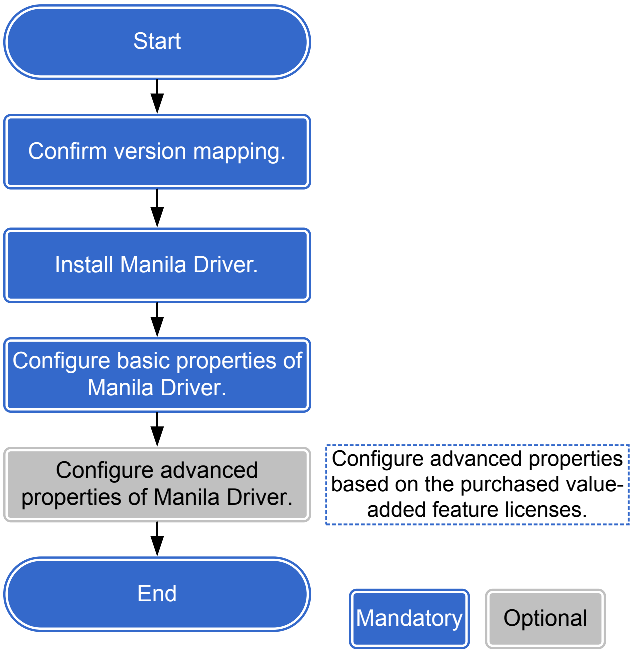
  If you cannot find the installation file after installation, you can download the specified Manila Driver from the OpenStack official website.

- Obtain Manila Driver from Huawei's OpenStack driver warehouse: Go to **https://github.com/huaweistorage/OpenStack_Driver**. Then you can download Manila Driver that matches the OpenStack version.

Configuration Roadmap

Figure B-1 shows the configuration roadmap of Manila Driver.

Figure B-1 Manila Driver configuration roadmap


Start
Confirm version mapping.
Install Manila Driver.
Configure basic properties of Manila Driver.
Configure advanced properties of Manila Driver.
Configure advanced properties based on the purchased value-added feature licenses.
End
Mandatory
Optional

For the specific steps of configuring Manila Driver, see the configuration guide released with Manila Driver.

C How to Obtain Help

If a tough or critical problem persists in routine maintenance or troubleshooting, contact Huawei for technical support.

C.1 Preparations for Contacting Huawei

To better solve the problem, you need to collect troubleshooting information and make debugging preparations before contacting Huawei.

C.1.1 Collecting Troubleshooting Information

You need to collect troubleshooting information before troubleshooting.

You need to collect the following information:

- Name and address of the customer
- Contact person and telephone number
- Time when the fault occurred
- Description of the fault phenomena
- Device type and software version

- Measures taken after the fault occurs and the related results
- Troubleshooting level and required solution deadline

C.1.2 Making Debugging Preparations

When you contact Huawei for help, the technical support engineer of Huawei might assist you to do certain operations to collect information about the fault or rectify the fault directly.

Before contacting Huawei for help, you need to prepare the boards, port modules, screwdrivers, screws, cables for serial ports, network cables, and other required materials.

C.2 How to Use the Document

Huawei provides guide documents shipped with the device. The guide documents can be used to handle the common problems occurring in daily maintenance or troubleshooting.

To better solve the problems, use the documents before you contact Huawei for technical support.

C.3 How to Obtain Help from Website

Huawei provides users with timely and efficient technical support through the regional offices, secondary technical support system, telephone technical support, remote technical support, and onsite technical support.

Contents of the Huawei technical support system are as follows:

- Huawei headquarters technical support department
- Regional office technical support center
- Customer service center
- Technical support website: **http://support.huawei.com/enterprise/**

You can query how to contact the regional offices at **http://support.huawei.com/enterprise/**.

C.4 Ways to Contact Huawei

Huawei Technologies Co., Ltd. provides customers with comprehensive technical support and service. For any assistance, contact our local office or company headquarters.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base Bantian, Longgang Shenzhen 518129 People's Republic of China

Website: **http://enterprise.huawei.com/**

D Glossary

If you want to obtain information about glossaries, visit **http://support.huawei.com/enterprise/**. In the search field, enter a product model, and select a path from the paths that are automatically displayed to go to the document page of the product. Browse or download the *OceanStor V3 Series V300R006 Glossary*.

E Abbreviation

A	
AD	Active Directory
C	
CIFS	Common Internet File System
CLI	Command Line Interface
D	
DNS	Domain Name Server
F	
FTP	File Transfer Protocol
G	
GUI	Graphical User Interface
H	
HTTP	Hypertext Transfer Protocol
I	
IP	Internet Protocol
ISM	Integrate Storage Manager

J	
JRE	Java Runtime Environment
L	
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
N	
NAS	Network Attached Storage
NFS	Network File System
NTFS	New Technology File System
NTLM	NT LAN Manager
NTP	Network Time Protocol
S	
SMB	Server Message Block
SSH	Secure Shell