About This Document

Purpose

This document describes the implementation principles and application scenarios of the NAS feature. Also, it explains how to configure and manage NAS.

Intended Audience

This document is intended for:

l Technical support engineers

l 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.
⚠ 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.

Symbol	Description
📖 **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 06 (2017-03-27)

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

Added description of cross-protocol share access.

Issue 05 (2016-11-20)

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

l Added descriptions about the FTPS protocol.

l Updated the list of reserved system users.

l Optimized descriptions about some operation steps.

Issue 04 (2016-07-25)

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

l Added description of CIFS share permissions.

l Added the Configuration of the NFSv4 service in a Non-Domain Environment.

Issue 03 (2016-04-30)

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

l Added configuring CIFS-NFS cross-protocol share access.

l Added NFS lock policy.

l Added restrictions of bond ports.

Issue 02 (2015-12-10)

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

Clarified route adding principles in **Configuring a Network**.

Revised some ambiguous descriptions.

Contents

1 File Access Protocols

About This Chapter

File access protocols are protocols used by clients for accessing file systems. mRAID16 supports NFS, CIFS , FTP and HTTP file
access protocols.

mRAID16 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.

1.1 Introduction
Common file access protocols include Network File System (NFS), common Internet file system (CIFS), File Transfer Protocol (FTP) and Hypertext Transfer Protocol (HTTP). This section describes the differences between them.

1.2 Authentication Specifications for File Access
This section describes the authentication modes employed by mRAID16 for file access in terms of authentication specifications and process.

1.1 Introduction

Common file access protocols include Network File System (NFS), common Internet file system (CIFS), File Transfer Protocol (FTP) and Hypertext Transfer Protocol (HTTP). This section describes the differences between them.

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

Type	Application Scenario	Transmission Protocol	Working Principle
CIFS	l Windows environments, including the non-domain environment and active directory (AD)^c domain environment. lLinux 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.			

1.2 Authentication Specifications for File Access

This section describes the authentication modes employed by mRAID16 for file access in terms of authentication specifications and process.

Table 1-2 describes the authentication specifications supported by themRAID16 .

Table 1-2 Authentication specifications

Authentication Mode	Kerberos^a	NTLM^b	User/User Group Management	Network Group
Local authentication	×^{c}	√^{c}	√	×

Authentication Mode	Kerberos[a]	NTLM[b]	User/User Group Management	Network Group
AD domain server authentication	lAccess 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

l   mRAID16 storage system can be added into an AD domain, LDAP domain, or NIS domain. However, each domain can have only one such storage system.

l   NFS shares support LDAP/NIS domain authentication but do not support Kerberosauthentication.

l   For FTP shares and HTTP shares, the storage system employs **User/User Group Management** for local authentication.

2 NFS-based File System Access

About This Chapter

This chapter describes the functions, planning, configuration, and management of the NFS protocol.

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

Planning an NFS share helps facilitate the follow-up service configuration. The following items need to be planned: networks, domains, permissions, and clients.

mRAID16 supports the NFS share mode. After configuring an NFS share, you can set different access permissions for clients.

This section uses an example to explain how to configure 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.

2.1 NFS Feature

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

2.1.1 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.

mRAID16 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.

📖**NOTE**

> During online upgrade, NFS v4 cannot ensure service continuity due to the limitation of its own protocol mechanism, but NFS v3 can ensure service continuity.

NFS highlights:

l High concurrency

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

l Data integrity

All users can read the same group of files.

l 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.

l 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.

l 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.

l 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.

l 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 2-1**.

Table 2-1 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

2.1.2 Availability

This section describes the license and version required by the NFS feature. Understanding the feature availability helps obtain this feature and facilitates the follow-up service configuration.

License Requirement

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

Applicable Versions

Product	Version
mRAID16	V300R003

2.1.3 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. log in to **IETF website** to obtain the standard protocol document.

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

📖**NOTE**

l   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.

l   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 2-2 describes the relationship between the NFS feature and other features.

Table 2-2 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	l 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. l 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.

2.1.4 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 2-1** 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 2-1 NFS share in a non-domain environment
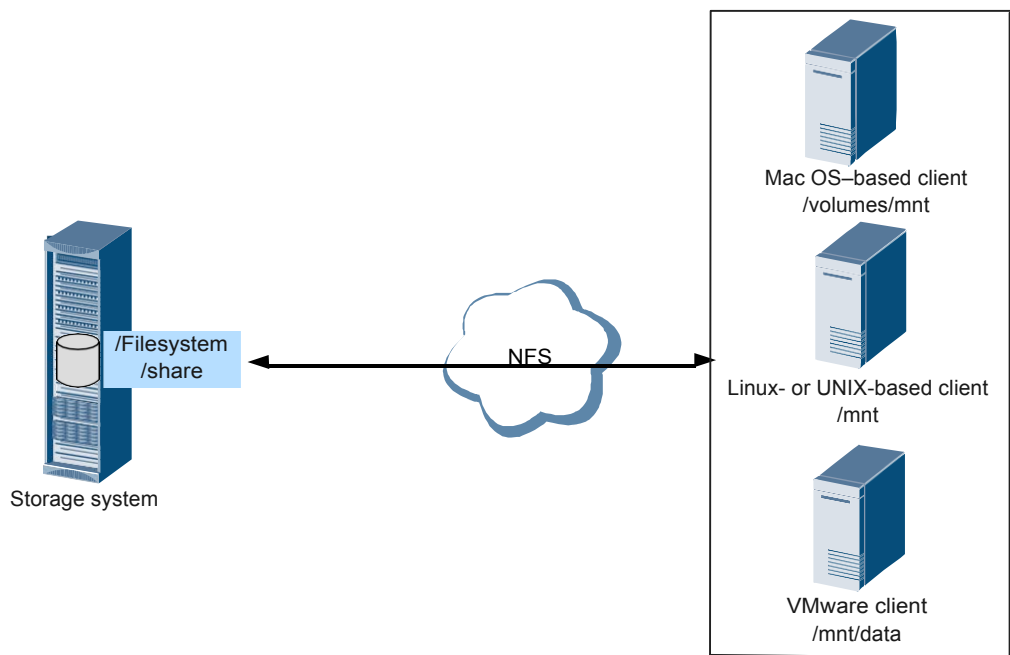
NFS Share in a Domain Environment

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 2-2**, 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 2-2 NFS share in a domain environment
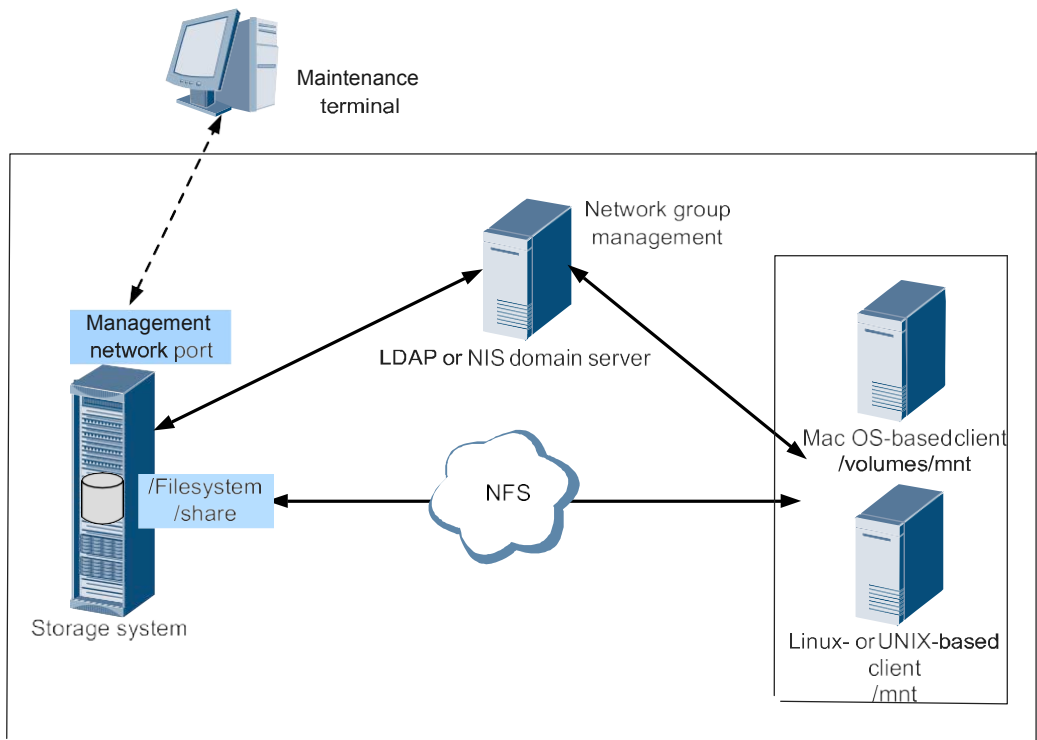
📖**NOTE**

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

2.2 Planning an NFS Share

Planning an NFS share helps facilitate the follow-up service configuration. The following items need to be planned: networks, domains, permissions, and clients.

Table 2-3 lists the required preparation items.

Table 2-3 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
Permission	-	Set users' permissions for accessing a file system. lWhen NFS v3 is used, the storage system supports UGO permissions but not ACL permissions. UGO permissions include **Execute**, **Read**, and **Write**. l 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
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.

2.3 Configuring an NFS Share

mRAID16 supports the NFS share mode. After configuring an NFS share, you can set different access permissions for clients.

2.3.1 Configuration Process

This section describes the NFS share configuration process.

Figure 2-3 shows the NFS share configuration process.

Figure 2-3 NFS share configuration process
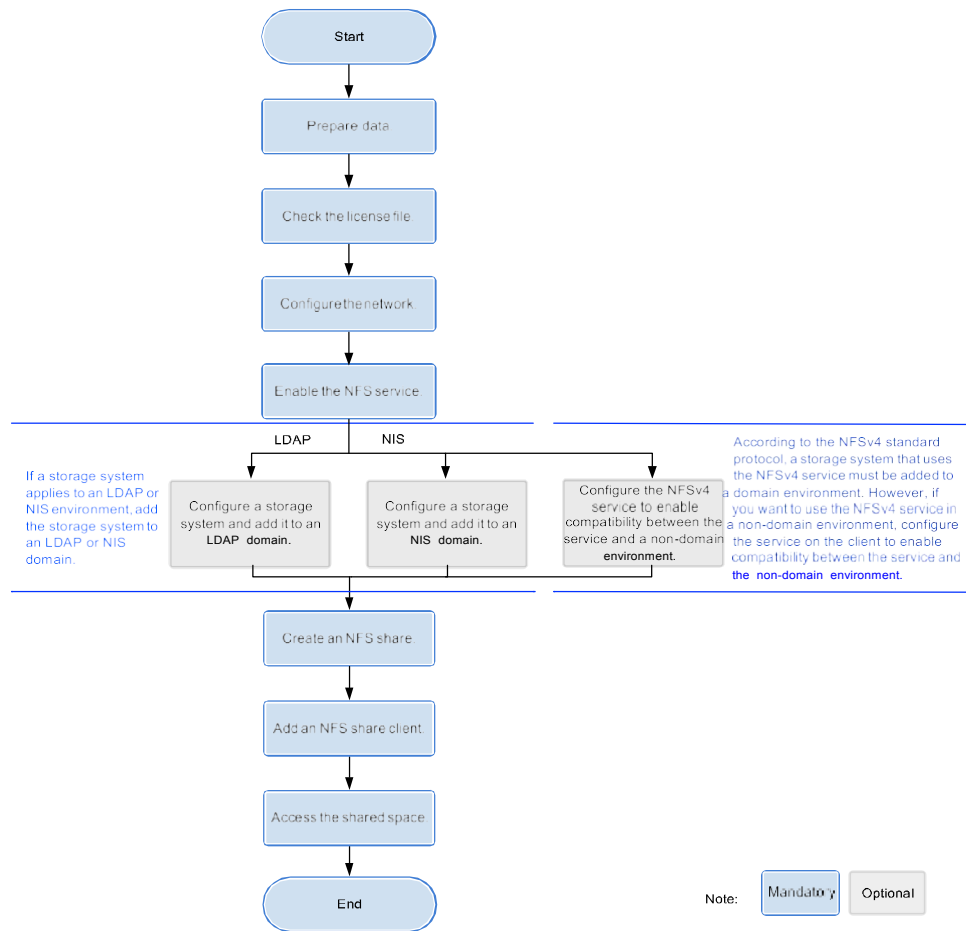
2.3.2 Preparing Data

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

Table 2-4 describes data to be planned and collected.

Table 2-4 Preparations required for configuring a NFS share

Item	Description	Example
Logical IP address *Indicates a logical IP address used by a storage system to provide shared space for a client.*	-	172.16.128.10
File system *File system used to create an NFS share.*	mRAID16 allows you to configure a file system or its sub- directory as an NFS share.	FileSystem001
LDAP domain or NIS domain information	LDAP domain information includes: lIP address of the primary LDAP server l**Optional:** IP address of the standby LDAP server lPort number used by the LDAP protocol lType of the encryption protocol lPassword hash algorithm lBase distinguished name (DN) lBonded DN NIS domain information includes: lDomain name lIP address of the active server in the NIS domain l**Optional:** IP address of the standby server in the NIS domain	LDAP
Permission *NFS share permissions of a client.*	The permissions include read-only and read-write. lRead-only: Clients have the read-only permission for NFS shares. lRead-write: Clients have the read-write permission for NFS shares.	Read-only

NOTE

You can contact your network administrator to obtain desired data.

2.3.3 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.

Procedure

Step 1 Log in to ActiveManager.

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 file.

   ----End

Follow-up Procedure

If no license is available, purchase, import and activate one.

2.3.4 Configuring a Network

This section describes how to use ActiveManager to configure IP addresses for a storage system.

Procedure

Step 1 Log in to ActiveManager and choose 🔄**Provisioning** > **Port**.

The **Port** page is displayed.

Step 2 **Optional:** Create a bond port.

Bond ports can increase link bandwidth and redundancy. Create bond ports based on site requirements. After bonding, the mode of all switch ports connected to the Ethernet port must be configured to 802.3AD LACP.

📖**NOTE**

The port bond mode of a storage system has the following restrictions:

l Only the interface modules with the same port rate (GE or 10GE) can be bonded.

lInterface modules cannot be bonded across controllers. Non-Ethernet network ports cannot be bonded. TOE interface modules cannot be bonded across cards.

lSmartIO interface modules cannot be bonded if they work in cluster or FC mode or run FCoE service in FCoE/iSCSI mode.

l Each port only allows to be added to one bond port. It cannot be added to multiple bond ports.

1. In **Ethernet Ports**, select a Ethernet port and click **More** > **Bond Port**.

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

2. Enter bond port information. **Table 2-5** describes related parameters.

Table 2-5 Bond port parameters

Parameter	Description	Value
Bond Name	Name of the bond port.	[Example] bond01
Available Ports	Available ports for binding.	[Example] CTE0.A.IOM1.P0

3. Click **OK**.

   The **Danger** dialog box is displayed.

4. Select **I have read and understood the consequences associated with performing this operation.** And click **OK**.

Step 3 Create a logical port.

📖**NOTE**

A maximum of 64 logical ports can be created for one controller. If more than 64 logical ports are created for one controller, logical ports drift towards a few available ports when a large number of ports fail, which deteriorates service performance.

1. Select **Logical Ports** and click **Create**.

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

2. Enter logical port information. **Table 2-6** describes related parameters.

Table 2-6 Create Logical Port parameters

Parameter	Description	Value
Name	Name of the logical port.	[Example] logip
IP Address Type	Type of the IP address: **IPv4 Address** or **IPv6 Address**.	[Example] IPv4 Address
IPv4 Address (IPv6 Address)	IP address of the logical port.	[Example] 172.16.128.10
Subnet Mask (Prefix)	Subnet mask (Prefix) of the logical port.	[Example] 255.255.255.0
IPv4 Gateway (IPv6 Gateway)	Address of the gateway.	[Example] 172.16.128.1
Primary Port	Physical port preferred by the logical port.	[Example] CTE0.A.IOM0.P0

Parameter	Description	Value
IP Address Floating	Whether IP address floating is enabled. mRAID16 supports IP address floating. When the primary port is disabled, the IP address will be floated to another port that can be used. **NOTE** Shares of file systems do not support the multipathing mode. IP address floating is used to improve reliability of links.	[Example] Enable
Failback Mode	Failback mode of the IP address: **Automatic** and **Manual**. **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
Activate Now	Whether the logical port is activated immediately. After activated, the logical IP can be used to access the shared space.	[Example] Enable

3. Click **OK**.

   The **Success** dialog box is displayed.

4. Click **OK**.

Step 4 **Optional:** Managing a Route.

You need to configure a route when the NFS server and the storage system are not on the same network.

l 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.

l 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.

1. Select the locical port for which you want to add a route and click **Route Management**.

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

2. Configure the route information for the logical port.

    a. In **IP Address**, select the IP address of the logical port.

    b. 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).

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

        There are three route options:

        n   Default route

            Data is forwarded through this route by default if no preferred route is available. The target address field and the target mask field (IPv4) or prefix (IPv6) of the default route are automatically set to 0. To use this option, you only need to add a gateway.

        n   Host route

            The host route is the route to an individual host. The destination mask (IPv4) or prefix (IPv6) of the host route are automatically set respectively to 255.255.255.255 or 128. To use this option, you only need to add the target address and a gateway.

        n   Network segment route

            The network segment route is the route to a network segment. You need to add the target address, target mask (IPv4) or prefix (IPv6), and gateway. Such as the target address is 172.17.0.0, target mask is 255.255.0.0, and gateway is 172.16.0.1.

    d. Set **Destination Address**.

          n   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.

          n   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.

    e.   Set **Destination Mask** (IPv4) or **Prefix** (IPv6).

        n 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.

        n   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.

    f.   In **Gateway**, enter the gateway of the local storage system's logical port IP address.

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

    The **Danger** dialog box is displayed.

4.   Confirm the information of the dialog box and select **I have read and understood the consequences associated with performing this operation.**.

5.   Click **OK**.

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

    📖**NOTE**

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

6.   Click **Close**.

----End

2.3.5 Enabling 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 ActiveManager.

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.

l If the host needs to use NFSv3 to mount shares, select **Enable NFSv3**.

l 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 mountshare.

    – 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

2.3.6 (Optional) Configuring a Storage System to Add It to a Domain

This section describes how to add the storage system to a domain such as an LDAP or NIS domain.

2.3.6.1 Configuring a Storage System to Add It to an LDAP Domain

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

Prerequisites

l An LDAP domain has been set up.

l Associated configurations have been completed, and required data is ready.

📖**NOTE**

l mRAID16 storage system can be connected to the LDAP server through the management port or the service port (ethernet port or logical port). When using the management port to connect to the LDAP server, it requires all the controllers can communicate with the LDAP server. You are advised to use the service port to connect to the LDAP server.

lmRAID16 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 ActiveManager.

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 2-7** below.

★ Primary Server Address:	
Standby Server Address 1:	
Standby Server Address 2:	
★ Port:	389 (1-65535)
★ Protocol:	LDAP
	⚠ If you use the LDAP protocol, there may be security risks.
★ Base DN:	ou=ou
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 2-7 Parameters of the LDAP domain

Parameter	Description	Value
Primary Server Address	IP address of an LDAP domain server. **NOTE** 　Ensure that the IP address is reachable. Otherwise, user authentication commands and network commands will time out.	[Example] 192.168.1.10
Standby Server Address 1	IP address of standby LDAP server 1. **NOTE** 　Ensure that the IP address is reachable. Otherwise, user authentication commands and network commands will time out.	[Example] 192.168.1.11
Standby Server Address 2	IP address of standby LDAP server 2. **NOTE** 　Ensure that the IP address is reachable. Otherwise, user authentication commands and network commands will time out.	[Example] 192.168.1.12
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] 389

Parameter	Description	Value
Protocol	Protocol used by the system to communicate with the LDAP domain server. l **LDAP**: indicates that the system uses the standard LDAP protocol to communicate with the LDAP domain server. l **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] LDAP
Base DN	Distinguished Name (DN) that specifies LDAP for searching.	[Rule] A DN consists of Relative Distinguished Names (RDN), which are separated from each other using commas (,). For example: testDn=testDn,xxxDn=xxx. [Format] xxx=yyy, separated by commas (,). [Example] dc=admin,dc=com
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=ldapuser01,ou=user,dc=admin ,dc=com

Parameter	Description	Value
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=Groups,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 **Save**. The LDAP domain authentication configuration is completed.

NOTE

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

----End

2.3.6.2 Configuring a Storage System to Add It to an NIS Domain

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

l An NIS domain has been set up.

l Associated configurations have been completed, and required data is ready.

📖**NOTE**

l The storage system can be connected to the NIS server through the management port or the service port (Ethernet port or logical port). When using the management port to connect to the NIS server, it requires all the controllers can communicate with the NIS server. You are advised to use the service port to connect to the NIS server.

l 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 ActiveManager.
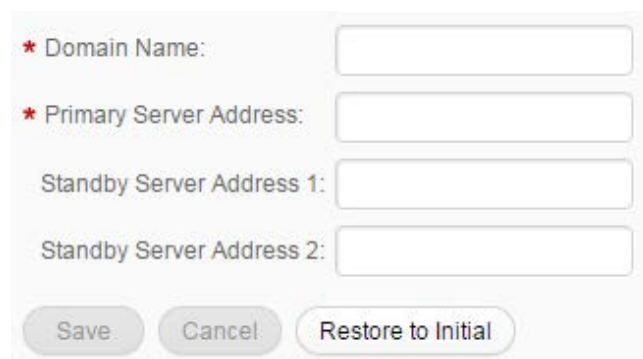
Step 2 Choose ⚙️ **Settings** > 🖥️ **Storage Settings** > **File Storage Service** > **Domain Authentication**.

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 2-8** below.

Table 2-8 Parameters of the NIS domain

Parameter	Description	Value
Domain Name	Domain name of a server.	[Rule] 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 (.). [Example] site
Primary Server Address	NIS domain server IP address. **NOTE** Ensure that the IP address is reachable. Otherwise, user authentication commands and network commands will time out.	[Example] 192.168.0.100
Standby Server Address 1	IP address of standby NIS server 1. **NOTE** Ensure that the IP address is reachable. Otherwise, user authentication commands and network commands will time out.	[Example] 192.168.0.101
Standby Server Address 2	IP address of standby NIS server 2. **NOTE** Ensure that the IP address is reachable. Otherwise, user authentication commands and network commands will time out.	[Example] 192.168.0.102

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

NOTE

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

----End

2.3.7 (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

l 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.

l 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.

l 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

2.3.8 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

l Associated configurations have been completed, and required data is ready.

l The NFS service has been enabled.

Procedure

Step 1 Log in to ActiveManager.

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 2-9 describes the related parameters.

Table 2-9 Parameters for creating an NFS share

Parameter	Description	Value
File System	File system for which you want to create an NFS share.	[Example] FileSystem001
Quota Tree	Level-1 directory under the root directory of the file system.	To share a quota tree, click [...] and select a quota tree you want to share. [Example] share **NOTE** The share path is **/Filesystem001/share**.

Parameter	Description	Value
Share Path	Name used by a user for accessing the shared resources.	-
Description	Description of the created NFS share.	[Value range] Contains 0 to 255 characters. [Example] Share for user 1.

Character Encoding	Clients communicate with the storage system using codes. These codes apply to names and metadata of shared files, but do not change the codes of file data. Codes include:
	lUTF-8
	    International code set
	lEUC-JP
	    euc-j*[ja] code set
	lJIS
	    JIS code set
	lS-JIS
	    cp932*[ja_jp. 932] code set
		[Default value]
		UTF-8

Step 5 Click **Next**.

The **Set Permissions** page is displayed.

Step 6 **Optional:** Assign the client the permission to the 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, please refer to **Adding an NFS Share Client**.

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

2.3.9 Adding an NFS Share Client

An NFS share client enables client users to access shared file systems using a network.

Prerequisites

l Associated configurations have been completed, and required data is ready.

l Create an available host name on the DNS in advance if you need to add a client of **Host** type.

l 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 ActiveManager.
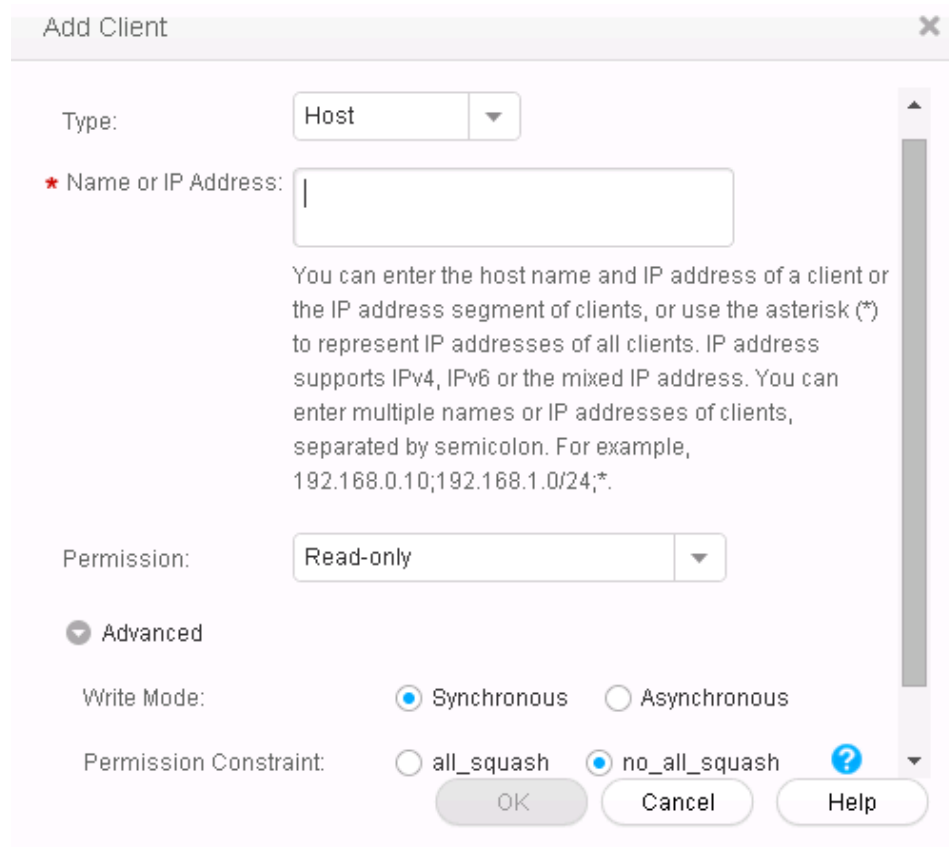
Step 2 Choose ![icon]**Provisioning** > ![icon] **Share** > **NFS (Linux/UNIX/MAC)**.

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 2-10** describes related parameters.

Table 2-10 NFS share client properties

Parameter	Description	Value

Type	Client type of the NFS share. Types include:
	
	 lHost
	    Applicable to the client in non-domain environment.
	
	 lNetwork 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]
		The name:
		lContains 1 to 255 characters, including letters, digits, hyphens (-), periods (.), and underscores (_).
		lThe value can begin with only a digit or letter and cannot end with a hyphen (-) or an underscore (_).
		l The value cannot contain consecutive periods (.), pure digits, or a period before or after an underscore, for example, "_." or "._".
		The IP address:
		lYou can enter the IP address of a client or the IP address segment of clients, or use asterisk (*) to represent IP addresses of all clients.
		lYou can enter IPv4, IPv6 or their mixed IP address.
		lThe mask of IPv4 ranges from 1 to 32. The mask of IPv6 ranges from 1 to 128.
		[Example]
		192.168.0.10
		192.168.0.10;192.168.1.0/24
		NOTE
		    You can enter multiple names or IP addresses of clients, separated by semicolon.

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: lContains 1 to 254 characters. l 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: lRead-only Only reading the files in the share is allowed. lRead-write Any operation is allowed.	[Default value] Read-only
Write Mode (Optional)	Write mode of the NFS share client. The modes include: lSynchronous: the data written to the share is written into the disk immediately. l 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. lall_squash: The user ID (UID) and group ID (GID) of a shared directory are mapped to user **nobody**, which are applicable to public directories. lno_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. l 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**. lno_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

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

2.3.10 Accessing NFS Share

This section describes how a client accesses an NFS shared file system. The operating systems that support the client in accessing NFS shared file systems include SUSE, Red Hat, HP-UX, SUN Solaris, IBM AIX, and Mac OS, etc.

Accessing an NFS Shared File System 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 followingcontents:

```
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 to restart thesystem.

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

Step 2 Run **showmount -e** *ipaddress* to view available NFS shared file systems of the storage system.

ipaddress represents the virtual 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 path of the NFS share created in the storage system.

Step 3 Run **mount -t nfs -o vers=n,proto=m,rsize=o,wsize=p,hard,intr,timeo=q**
ipaddress:*filesystem* /**mnt** to mount the NFS shared file system. **Table 2-11** describes the
related parameters.

```
#mount -t nfs -o vers=3,proto=tcp,rsize=1048576,wsize=1048576,hard,intr,timeo=600
172.16.128.10:/nfstest /mnt
```

Table 2-11 SUSE/Red Hat mount NFS shares parameters

Parameter	Description	Example
o	Option that nfs mount, including **ro**, **rw** and so on. lro: Mount a share that only be read. lrw: Mount a share that can be read and write.	The default value is **rw**.
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 a environment that requires high reliability, you are advised to use NFS v3.
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.	Recommended to use **1048576**, and recommended to use **16384** for Red Hat 7.
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 tenths of a second	Recommended to use **600**
filesystem	The path of the NFS share created in the storage system.	-

Step 4 Run **mount** to verify that the NFS shared file system 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)
```

When the previous output appears, the NFS shared file system 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 Shared File System 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 shared file systems of the storage system.

ipaddress represents the virtual 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 path of the NFS share created in the storage system.

Step 3 Run **mount** [**-F nfs**|**-f nfs**] **-o vers=n,proto=m** *ipaddress*:*filesystem* **/mnt** to mount the NFS shared file system. **Table 2-12** describes the related parameters.

```
#mount -f nfs -o vers=3,proto=tcp 172.16.128.10:/nfstest /mnt
```

Table 2-12 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 a environment that requires high reliability, you are advised to use NFS v3.
proto	The transfer protocol. The value can be **tcp** or **udp**.	tcp
filesystem	The path of the NFS share created in the storage system.	-

Step 4 Run **mount** to verify that the NFS shared file system 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)
```

When the previous output appears, the NFS shared file system 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 Shared File System 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 shared file systems of the storage system.

ipaddress represents the virtual 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 path of the NFS share created in the storage system.

Step 3 Run **mount** *ipaddress*:*filesystem* **/mnt** to mount the NFS shared file system.

📖**NOTE**

filesystem represents the path 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**

If the AIX client fails to mount the NFS shared file system 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 shared file system has been mounted to the local computer.

```
#mount
172.16.128.10:/nfstest on /mnt type nfs (rw,addr=172.16.128.10)
```

When the previous output appears, the NFS shared file system 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 Shared File System by a Mac OS Client

Step 1 Run **showmount -e** *ipaddress* to view available NFS shared file systems of the storage system.

ipaddress represents the virtual 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 path of the NFS share created in the storage system.

Step 2 Run **sudo /sbin/mount_nfs -P** *ipaddress*:*filesystem* **/Volumes/mount1** to mount the NFS
shared file system.

📖**NOTE**

filesystem represents the path of the NFS share created in the storage system.

```
Volumes root# sudo /sbin/mount_nfs -P 172.16.128.10:/nfstest /Volumes/mount1
```

Step 3 Run **mount** to verify that the NFS shared file system 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)
```

When the previous output appears, the NFS shared file system 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 Shared File System 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 2-13** describes related parameters.

Table 2-13 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	The path of the NFS share created in the storage system.	Example /nfstest
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

Postrequisite

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.

2.4 Configuration Example

This section uses an example to explain how to configure an NFS share.

2.4.1 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 2-4 shows the customer's network diagram.

Figure 2-4 Customer's network diagram
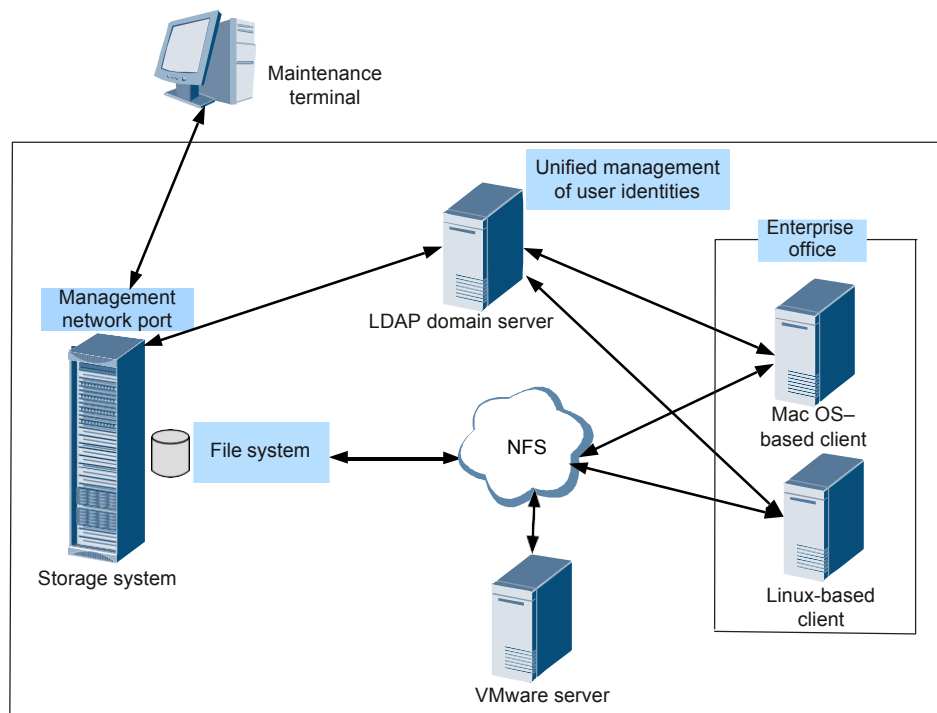
The status quo of the customer's live network can be concluded as follows:

l The enterprise office system runs Linux and Mac OS, which are connected to an LDAP domain server.

l Linux-based hosts belong to network group **ldapgrouplinux**, whereas Mac OS-based hosts belong to network group **ldapgroupmac**.

l 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:

l 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.

l The Mac network group and Linux network group can only access their own storage space.

2.4.2 Requirement Analysis

This section analyzes the customer's requirements and provides a solution.

The customer's requirements are analyzed as follows:

l All clients use the Linux operating system, so mRAID16 can employ NFS sharing to provide storage space for the two systems respectively.

l mRAID16 supports NFS share management in a non-domain and an LDAP domain environment.

Based on the previous analysis, a solution as follows is provided:

l Use mRAID16 as the storage system.

l Configure each service system as shown in **Table 2-14**.

Table 2-14 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

2.4.3 Configuration Process

The preceding solutions and the following configuration flowchart help you understand the subsequent configuration.

Figure 2-5 shows the configuration process.

Figure 2-5 Configuration process
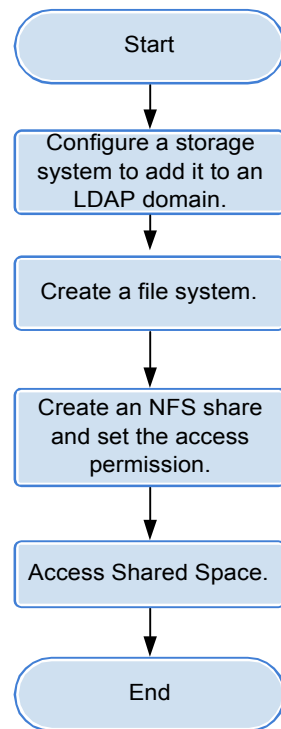
2.4.4 Creating an NFS Share

After requirement analysis and service planning, you need to configure an NFS share on ActiveManager.

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.
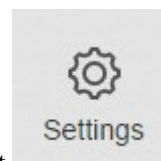
On the navigation bar of the ActiveManager, select   > **Storage Settings** > **File Storage Service** > **Domain Authentication**. Input the parameters of the LDAP domain in the **LDAP Domain Settings** area.

LDAP Domain Settings

Lightweight Directory Access Protocol (LDAP) is based on the X.500 model. It supports TCP/IP. The LDAP directory server is used for maintaining the directory information table of the current storage resources. The table contains the information about the obtained resources and access permission of each user or user group, and provides a mapping between logical file names and physical file locations. The LDAP directory server also offers higher-level directory services such as the resource attribute–based query function. How to configure an LDAP domain?

★ 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 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)

Save   Cancel   Restore to Initial

📖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.
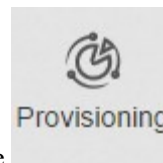
Provisioning

1. On the ActiveManager page, choose > **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 2-15** describes related parameters.

Table 2-15 Create File System parameters

Parameter	Planned Value
Name	FileSystem
Capacity	1 TB
Quantity	3
Owning Storage Pool	StoragePool000
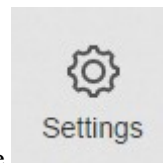
📖**NOTE**

> 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.

4.   Click **OK**.

Step 3 Create an NFS share and set the access permission. Such as share the **FileSystem001** with a Linux-based host.
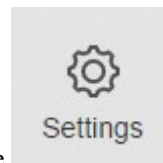
1.   On the ActiveManager page, choose ⬚ > **Share**. The **Share** page is displayed.

2.   Choose **NFS (Linux/UNIX/MAC)** > **Create**.

     The **Create NFS Share Wizard: Step 4-1** page is displayed.

3.   In **File System**, select file system **FileSystem0000**.

4.   Click **Next**.

     The **Create NFS Share Wizard: Step 4-2** page is displayed.

5.   Click **Add**.

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

6.   Set **Type** to **Network Group** and enter **ldapgrouplinux** in **Network Group Name**.

7.   Click **OK**.

     The **Create NFS Share Wizard: Step 4-2** page is displayed.

8.   Click **Next**.

     The **Create NFS Share Wizard: Step 4-3** page is displayed.

9.   Click **Finish**.

     The **Create NFS Share Wizard: Step 4-4** page is displayed.

10. 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 3.6**.

If **FileSystem0002** is shared with a VMware ESX-based host, enter **172.16.211.200** in **IP Address** in **Step 3.6**.

----End

2.4.5 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=600172.16.211.20:/ 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 shared file system 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 2-16** describes related parameters.

Table 2-16 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

2.5 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.

2.5.1 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 ActiveManager.

Step 2 Choose ![icon] **Provisioning** > ![icon] **Share** > **NFS (Linux/UNIX/MAC)**.

Step 3 In NFS share list, view the NFS share information. **Table 2-17** describes the related parameters.

Table 2-17 NFS share information

Parameter	Description
Share Path	Path of the NFS share.
ID	ID of the NFS share.
Description	Description of the NFS share.

Parameter	Description
Character Encoding	Clients communicate with the storage system using codes. These codes apply to names and metadata of shared files, but do not change the codes of file data. Codes include: lUTF-8 　　International code set lEUC-JP 　　euc-j*[ja] code set lJIS 　　JIS code set lS-JIS 　　cp932*[ja_jp.932] 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 2-18**.

Table 2-18 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: lHost 　　Applicable to the client in non-domain environment. lNetwork group 　　Applicable to client in LDAP or NIS domain.
Permission Level	The permission for client to access the NFS share. The permissions include: lRead-only 　　Only reading the files in the share is allowed. lRead-write 　　Any operation is allowed.
ID	Client ID of the NFS share.

----End

2.5.2 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 ActiveManager.

Step 2 Choose ![icon] **Provisioning** > ![icon] **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.

Table 2-19 describes the related parameters.

Table 2-19 Parameters for a NFS share

Parameter	Description	Value
Description	Description about the NFS share.	[Value range] Contains 0 to 255 characters. [Example] Share for user 1.

Character Encoding	Clients communicate with the storage system using codes. These codes apply to names and metadata of shared files, but do not change the codes of file data. Codes include:
	lUTF-8
	    International code set
	lEUC-JP
	    euc-j*[ja] code set
	lJIS
	    JIS code set
	lS-JIS
	    cp932*[ja_jp. 932] code set
		[Default value]
		UTF-8

Step 5 Confirm that you want to modify the properties of the NFS share.

1. Click **OK**.

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

2. Click **Close**.

----End

2.5.3 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 ActiveManager.
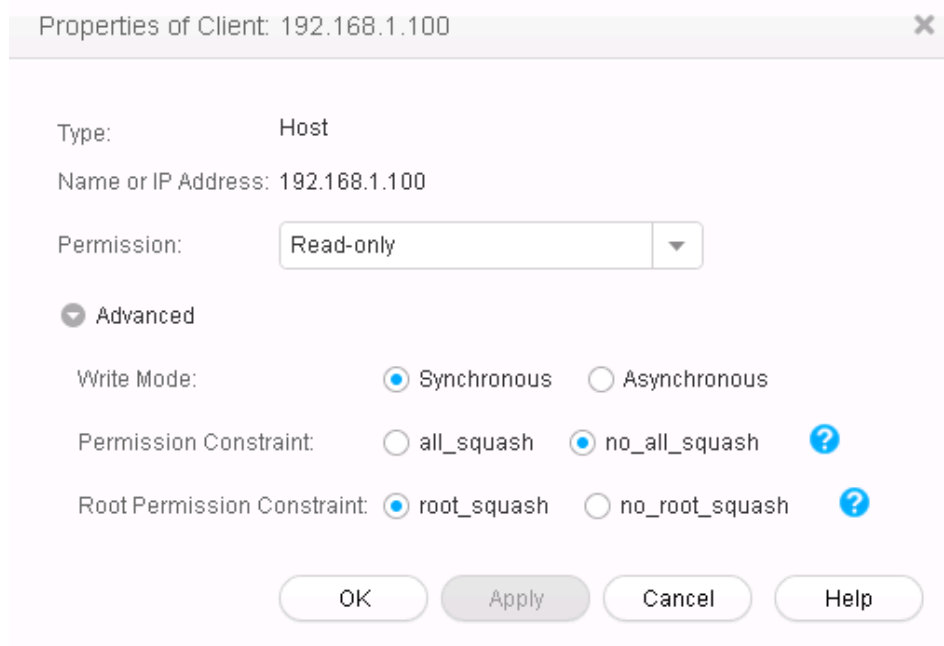
Step 2 Choose ![icon] **Provisioning** > ![icon] **Share** > **NFS (Linux/UNIX/MAC)**.

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 2-20** describes related parameters.

Table 2-20 NFS share client properties

Parameter	Description	Value

Permission	The permission for client to access the NFS share. The permissions include:
	
	lRead-only
	    Only reading the files in the share is allowed.
	
	lRead-write
	    Any operation is allowed.
		[Default value]
		Read-only

Write Mode (Optional)	Write mode of the NFS share client. The modes include: lSynchronous: the data written to the share is written into the disk immediately. l 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. lall_squash: The user ID (UID) and group ID (GID) of a shared directory are mapped to user **nobody**, which are applicable to public directories. lno_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. l 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**. lno_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

Step 6 Click **OK**.

----End

2.5.4 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 ActiveManager.

Step 2 Choose ![icon] **Provisioning** > ![icon] **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

2.5.5 Disabling the NFS Service

When the NFS service is abnormal, disable it to prevent file systems from being incorrectly accessed.

Procedure

Step 1 Log in to ActiveManager.

Step 2 Choose [icon] **Settings** > [icon] **Storage Settings** > **File Storage Service** > **NFS Service**.

Step 3 Disable the NFS service.

1. In the **NFSv3** area, deselect **Enable** to disable the NFSv3 service.

2. In the **NFSv4** area, deselect **Enable** to disable the NFSv4 service.

Step 4 Click **Save**.

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

Step 6 Click **OK**.

----End

2.5.6 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 ActiveManager.

Step 2 Choose [icon] **Provisioning** > [icon] **Share** > **NFS (Linux/UNIX/MAC)**.

Step 3 Select the NFS share and click **Delete**.

The security alert dialog box is displayed.

[icon]**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

3 CIFS-based File System Access

About This Chapter

This chapter describes the functions, management, and configuration of the CIFS protocol.

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

3.2 Planning a CIFS Share
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.

3.3 Configuring a CIFS Share
mRAID16 supports the CIFS share mode. By configuring a CIFS share, a user can access the shared directory.

3.4 Configuring a Homedir Share
mRAID16 supports the Homedir share mode. After the Homedir share service is enabled, a user can only access the shared directory with the same name as the user.

3.5 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.

3.6 Managing an CIFS Share
After an CIFS share is configured for a storage system, you need to manage and maintain the CIFS share. This section describes how to manage an CIFS share.

3.1 CIFS Feature

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

3.1.1 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). mRAID16 storage system supports SMB 1.0, SMB2 (SMB 2.0 and SMB 2.1) and SMB 3.0.

l If the client runs Windows Server 2003, Windows XP, Linux, or MAC OS, SMB 1.0 is used.

l If the client runs Windows Server 2008 or Windows Vista, SMB 2.0 is used.

l If the client runs Windows Server 2008 R2 or Windows 7, SMB 2.1 is used. l If

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

☐NOTE

Some file sharing protocols (such as SMB 1.0, SMB2 and NFS v4), limited by their own mechanisms, cannot ensure service continuity during online upgrade. SMB 3.0 and NFS v3 can ensure service continuity during online upgrade, but the **Failover** option needs to be manually enabled when using SMB 3.0.

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 mRAID16 storage system. With CIFS, clients can quickly read, write, and create files in mRAID16 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:

l 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.

l 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.

l 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.

l Robust security

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

l Wide application

Any client that supports the CIFS protocol can access the CIFS share space.

l 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**.

l **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.

l **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.

l **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.

l **Space Quota**: maximum capacity of quota tree in a file system

l **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**.

l **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.

l **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).

l **AntivirusGroup**: antivirus user group. The group members can use third-party antivirus software to scan for shared file systems. They have administrator permissions.

l **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.

3.1.2 Availability

This section describes the availability of the CIFS feature in terms of license and version requirements.

License Requirement

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

Applicable Versions

The storage system supports SMB 1.0, SMB2 (SMB 2.0 and SMB 2.1) and SMB 3.0 and is adaptive to the protocol version, making manual setting unnecessary.

l If the client runs Windows Server 2003, Windows XP, Linux, or MAC OS, SMB 1.0 is used.

l If the client runs Windows Server 2008 or Windows Vista, SMB 2.0 is used.

l If the client runs Windows Server 2008 R2 or Windows 7, SMB 2.1 is used. l If

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

3.1.3 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 3-1 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.
NFS/FTP/HTTP share	lFile 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. lIf 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. lThe software that are 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.

3.1.4 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 3-1**, 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 3-1 CIFS share in a non-domain environment
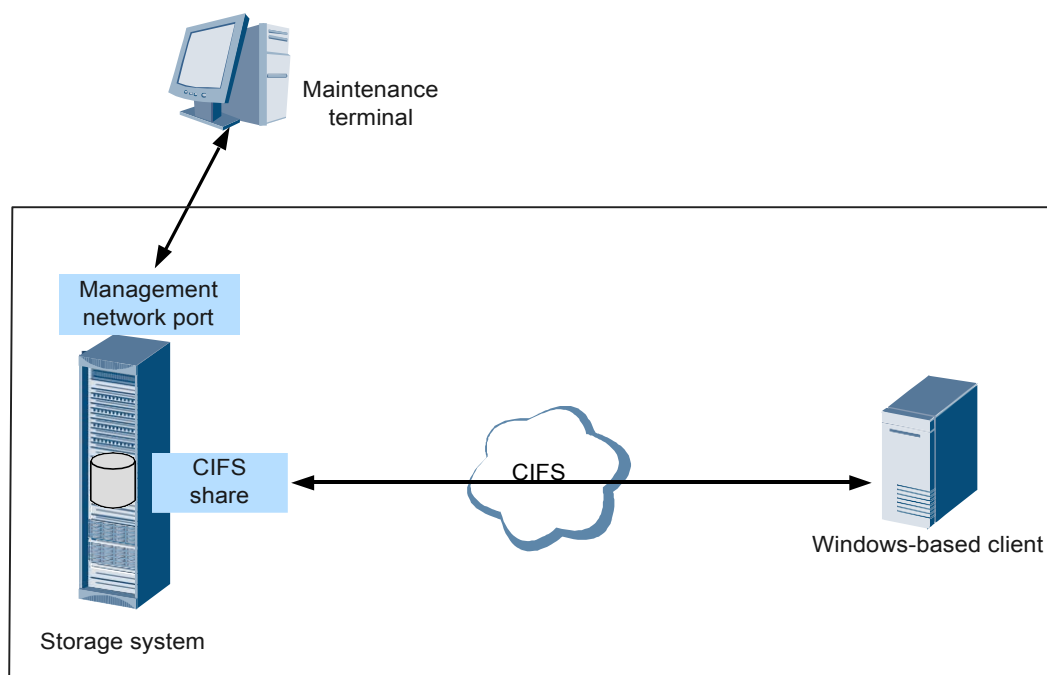
□**NOTE**

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 3-2**.

Figure 3-2 CIFS share in an AD domain environment
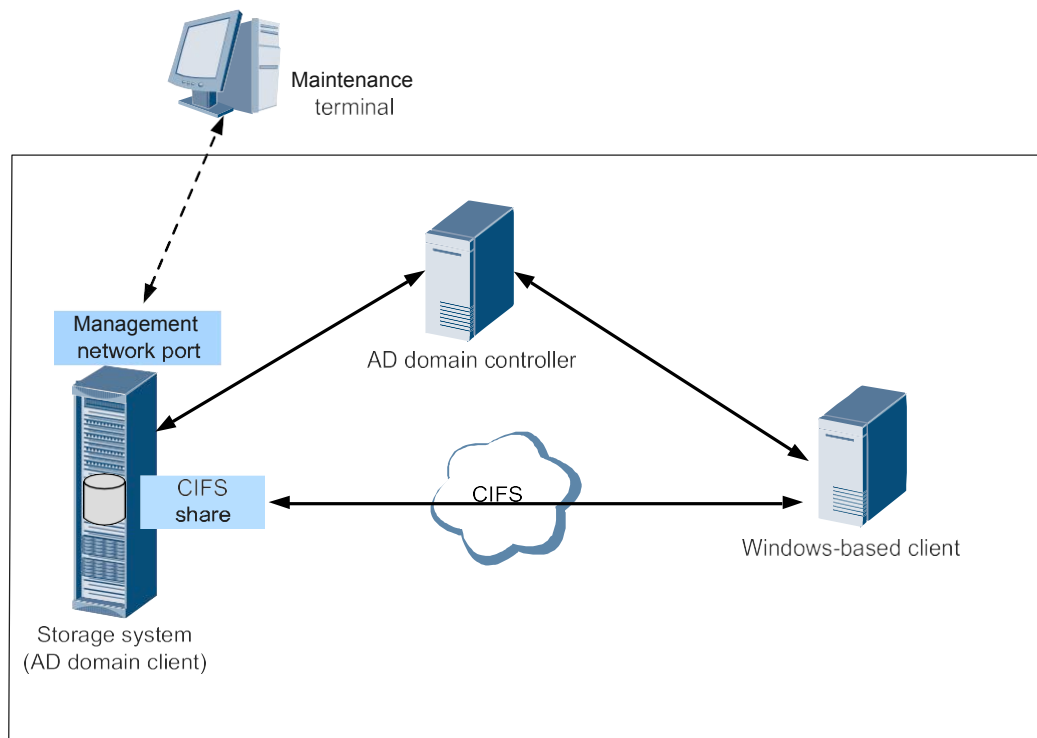
NOTE

l   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.

l   After Homedir is enabled, a user in the AD domain can only access the shared directorywith the same name as the user.

3.2 Planning a CIFS Share

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 3-2 lists the required preparation items.

Table 3-2 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
	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: l 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. l Non-domain: No domain environments need to be set up.	AD domain

Planned Item	Subitem	Requirement	Example
Authentication mode	Local, domain, or global authentication.	Configure an authentication mode based on the domain environment (AD domain or non-domain environment). lLocal authentication: Local user are used to validate the accounts identity. l Domain authentication: Domain servers are used to validate the user identity. l Global authentication: Local authentication is used first. If local authentication is not passed, domain authentication is used.	Global authentication
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: lRead-only: The user can only read the CIFS share. lRead-write: The user can read and write the CIFS share. lFull control: The user has full permission for the CIFS share. lForbidden: The user is forbidden to access the CIFS share.	Read-only

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. 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.

3.3 Configuring a CIFS Share

mRAID16 supports the CIFS share mode. By configuring a CIFS share, a user can access the shared directory.

3.3.1 Configuration Process

This section describes the CIFS share configuration process.

Figure 3-3 shows the CIFS share configuration process.

Figure 3-3 CIFS share configuration process
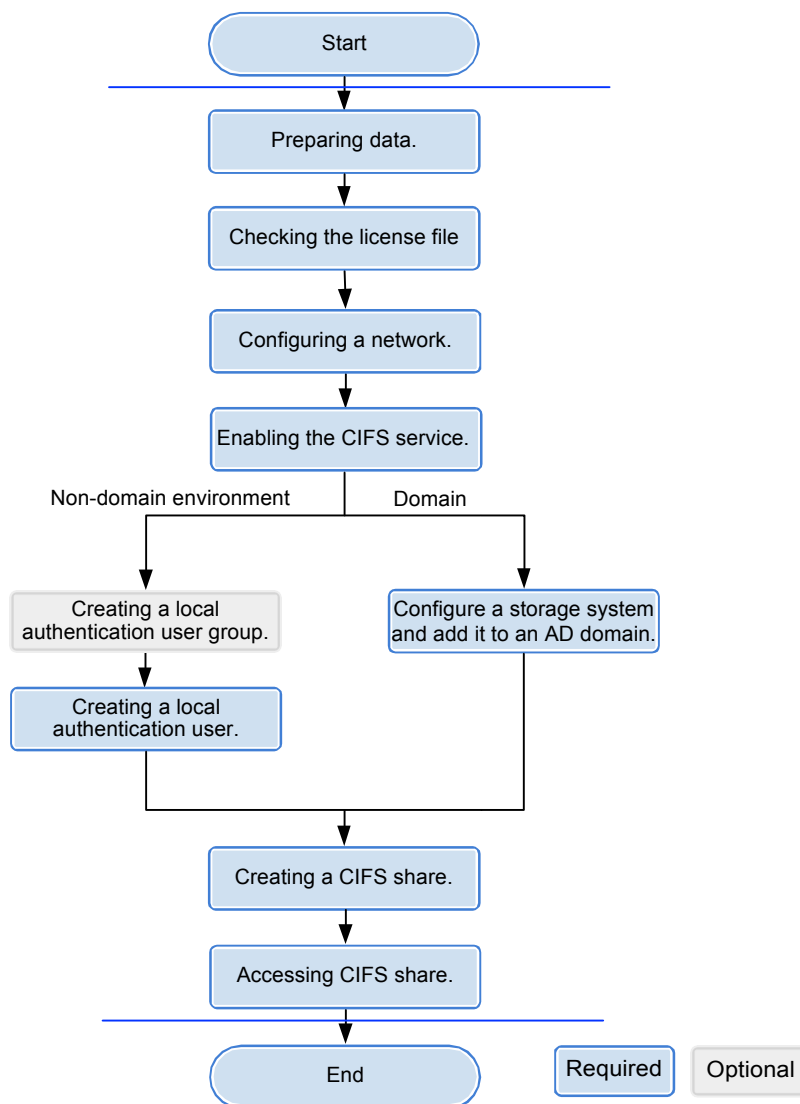
3.3.2 Preparing Data

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 3-3 describes preparations required for configuring a CIFS share.

Table 3-3 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.*	-	192.168.17.100
File system *Indicates the file system for which a CIFS share is configured.*	ThemRAID16 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: lMust contain 1 to 80 characters. l 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: lFull control: the user can full control the CIFS share. lRead-only: the user can only read the CIFS share. lRead and write: the user can read and write the CIFS share. lForbidden: the user can not access the CIFS share.	Read and write

Item	Description	Example
User *User that employs local authentication.*	The user name: lMust contain 8 to 32 characters by default. lCannot 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: l 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**. lUser accounts retained in Linux: **root**, **nogroup**, **nobody**, **ftp**, **anonymous**. lUser 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: lMust contain 1 to 32 characters. lCannot 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: l 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**. lUser accounts retained in Linux: **root**, **nogroup**, **nobody**, **ftp**, **anonymous**. lUser accounts retained in a storage system: **ibc_os_hs**.	default_group
AD domain information *AD domain information for domain authentication.*	AD domain information includes: lUser name of the domain administrator: The AD domain can provide an account that has the rights to add storage systems to the domain. lPassword: password of the user. lFull domain name: name of the AD domain lOrganization 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. lSystem name: name of a storage system that is added to the AD domain.	-
DNS *DNS information for domain authentication.*	IP address of DNS server.	-

Item	Description	Example
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.

3.3.3 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.

Procedure

Step 1 Log in to ActiveManager.

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 file.

----End

Follow-up Procedure

If no license is available, purchase, import and activate one.

3.3.4 Configuring a Network

This section describes how to use ActiveManager to configure IP addresses for a storage system.

Procedure

Step 1 Log in to ActiveManager and choose 🔄**Provisioning** > **Port**.

The **Port** page is displayed.

Step 2 **Optional:** Create a bond port.

Bond ports can increase link bandwidth and redundancy. Create bond ports based on site requirements. After bonding, the mode of all switch ports connected to the Ethernet port must be configured to 802.3AD LACP.

📖**NOTE**

The port bond mode of a storage system has the following restrictions:

l Only the interface modules with the same port rate (GE or 10GE) can be bonded.

lInterface modules cannot be bonded across controllers. Non-Ethernet network ports cannot be bonded. TOE interface modules cannot be bonded across cards.

lSmartIO interface modules cannot be bonded if they work in cluster or FC mode or run FCoE service in FCoE/iSCSI mode.

l Each port only allows to be added to one bond port. It cannot be added to multiple bond ports.

1.   In **Ethernet Ports**, select a Ethernet port and click **More** > **Bond Port**.

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

2.   Enter bond port information. **Table 3-4** describes related parameters.

Table 3-4 Bond port parameters

Parameter	Description	Value
Bond Name	Name of the bond port.	[Example] bond01
Available Ports	Ports that you select and ports to which you want to bond the selected ports.	[Example] CTE0.A.IOM1.P0

3.   Click **OK**.

The **Danger** dialog box is displayed.

4.   Select **I have read and understood the consequences associated with performing this operation.** And click **OK**.

Step 3   Create a logical port.

📖**NOTE**

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.

1.   Select **Logical Ports** and click **Create**.

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

2.   Enter logical port information. **Table 3-5** describes related parameters.

Table 3-5 Create Logical Port parameters

Parameter	Description	Value
Name	Name of the logical port.	[Example] logip
IP Address Type	Type of the IP address: **IPv4 Address** or **IPv6 Address**.	[Example] IPv4 Address
IPv4 Address (IPv6 Address)	IP address of the logical port.	[Example] 172.16.128.10

Parameter	Description	Value
Subnet Mask (Prefix)	Subnet mask (Prefix) of the logical port.	[Example] 255.255.255.0
IPv4 Gateway (IPv6 Gateway)	Address of the gateway.	[Example] 172.16.128.1
Primary Port	Physical port preferred by the logical port.	[Example] CTE0.A.IOM0.P0
IP Address Floating	Whether IP address floating is enabled. mRAID16 support IP address floating. When the primary port is disabled, the IP address will be floated to another port that can be used. NOTE Shares of file systems do not support the multipathing mode. IP address floating is used to improve reliability of links.	[Example] Enable
Failback Mode	Failback mode of the IP address: **Automatic** and **Manual**. 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
Activate Now	Whether the logical port is activated immediately. After activated, the logical IP can be used to access the shared space.	[Example] Enable

3. Click **OK**.

    The **Success** dialog box is displayed.

4. Click **OK**.

Step 4 **Optional:** Managing a Route.

You need to configure a route when the CIFS server and the storage system are not on the same network.

l 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.

l 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.

1. Select the locical port for which you want to add a route and click **Route Management**.

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

2. Configure the route information for the logical port.

    a. In **IP Address**, select the IP address of the logical port.

    b. 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).

---

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

        There are three route options:

        n   Default route

            Data is forwarded through this route by default if no preferred route is available. The target address field and the target mask field (IPv4) or prefix (IPv6) of the default route are automatically set to 0. To use this option, you only need to add a gateway.

        n   Host route

            The host route is the route to an individual host. The target mask (IPv4) or prefix (IPv6) of the host route are automatically set respectively to

255.255.255.255 or 128. To use this option, you only need to add the target address and a gateway.

- n   Network segment route

   The network segment route is the route to a network segment. You need to add the target address, target mask (IPv4) or prefix (IPv6), and gateway. Such as the target address is 172.17.0.0, target mask is 255.255.0.0, and gateway is 172.16.0.1.

d.   Set **Destination Address**.

- n   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.

- n   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.

- n   Set **Destination Mask** (IPv4) or **Prefix** (IPv6).

- n   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.

- n   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.

e.   In **Gateway**, enter the gateway of the local storage system's logical port IP address.

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

   The **Danger** dialog box is displayed.

4.   Confirm the information of the dialog box and select **I have read and understood the consequences associated with performing this operation.**.

5.   Click **OK**.

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

   📖**NOTE**

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

6.   Click **Close**.

----End

3.3.5 Enabling the CIFS Service

Before creating a CIFS share, check whether the CIFS service has been enabled and whether parameters are correct.

Procedure

Step 1 Log in to **ActiveManager**.

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. **Table 3-6** describes the related parameters.

Table 3-6 CIFS service parameters

Parameter	Description	Value
Authentication Mode	Authentication mode for accessing a CIFS share. – **Local authentication**: Applies to scenarios where a local 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.	[Example] Domain authentication

Parameter	Description	Value
Performance Settings	You can configure performance parameters to improve the CIFS share access efficiency. – Oplock: Opportunistic locking (Oplock) is a mechanism that improves client access efficiency. After this mechanism is enabled, files are cached locally before being sent to shared storage. This function is not recommended in the following scenarios: n 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. n 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 through automatic display refreshing.	None
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.	None

Parameter	Description	Value
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 ABSE. Otherwise, security risks may exist in all sharing including sharing without access permission.	[Example] ABSE
Signature Settings	You can set signatures to enhance CIFS share access security. – Signature: This item is available for a client that employs SMB (Server Message Block) 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 parameter is selected, clients are required to enable the signature function. If a client does not enable the signature function, the client is not allowed to access the system data. **NOTE** If the signature function is disabled, the storage system may encounter man-in-the-middle (MITM) attacks, resulting in security risks.	[Example] Signature enforcement

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

3.3.6 Configuring a Local Authentication User (Group)

In a non-domain environment, you must configure a local authentication user (group). mRAID16 enables you to allocate different CIFS share access permissions to different user (group).

3.3.6.1 (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.

l **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.

l **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.

l **AntivirusGroup**: antivirus user group. The group members can use third-party antivirus software to scan for shared file systems. They have administrator permissions.

l **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 ActiveManager.

Step 2 Choose ![icon] **Provisioning** > ![icon] **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**

l 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 (.).

l Contains 1 to 32 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

3.3.6.2 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 ActiveManager.

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:

l 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 (.).

l 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:

l Contain 8 to 16 characters.

l Contain special characters. Special characters include: !"#$%&'()*+,-./:;<=>? @[\]^`{_|}~ and space.

l Contain any two types of the uppercase letters, lowercase letters, and digits.

l Cannot contain three consecutive same characters.

l 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. For security purpose, you are advised to select **Password Validity Period (Days)**. After you select this item, your password will never expire. The default validity period is 180 days. After the password expires, the user cannot access shares. 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.

Step 9 Select the user group to which the user belongs to and click **OK**.

Step 10 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

3.3.7 Configuring a Storage System to Add It to an AD Domain

After mRAID16 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.

3.3.7.1 Connecting a Storage System to the 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.

Context

l A DNS server is used to resolve host names in a domain.

l 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 ActiveManager.

Step 2 Choose ⚙ **Settings** > 🔧 **Basic Information** > **DNS Service**.

Step 3 Set the DNS information.

1. Set **Active DNS IP Address**.

2. **Optional:** Set **Standby DNS IP Address 1**.

3. **Optional:** Set **Standby DNS IP Address 2**.

📖**NOTE**

   Please configure the standby DNS IP address 1 first and then the standby DNS IP address 2.

Step 4 Click **Save**.

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

Step 5 Click **OK**.

----End

3.3.7.2 Configuring a Storage System to AD Domain

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

l An AD domain has been set up.

l The storage system has been connected to the DNS server.

l AD domain server and DNS server must have time synchronization with storage system. The time difference must be no larger than 5 minutes.

📖**NOTE**

l mRAID16 storage system can be connected to the AD domain and DNS server through the management port or the service port (ethernet port or logical port). When using the management port to connect to the AD server, it requires all the controllers can communicate with the AD server. You are advised to use the service port to connect to the AD server.

l AD domain servers support the primary/secondary domain, parent/child domain, active/standby domain, or trust domain. One storage system can be connected to only one AD domain server.

Precautions

l 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.

l Simple password may cause security risk. Complicated password is recommended, for example, password contains uppercases, lowercases, digits and special characters.

l 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 ActiveManager.

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 3-7**.

Table 3-7 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
Password	Password of an administrator who logs in to the AD domain server.	[Rule] Contains 1 to 127 letters. [Example] !QAZ2wsx
Full Domain Name	Full domain name of the AD domain server	[Rule] Contains 1 to 127 characters. [Example] abc.com

Parameter	Description	Value
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
System Name	Name of a domain to which a client will be added. 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

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 ADdomain.

3.3.8 Creating a CIFS share

You may share the file system through CIFS, and user can access the shared storage space.

Prerequisites

l The CIFS service is enabled.

l If it is a non-domain environment, the CIFS authentication mode is configured as local authentication or global authentication.

l 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 ActiveManager.

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.
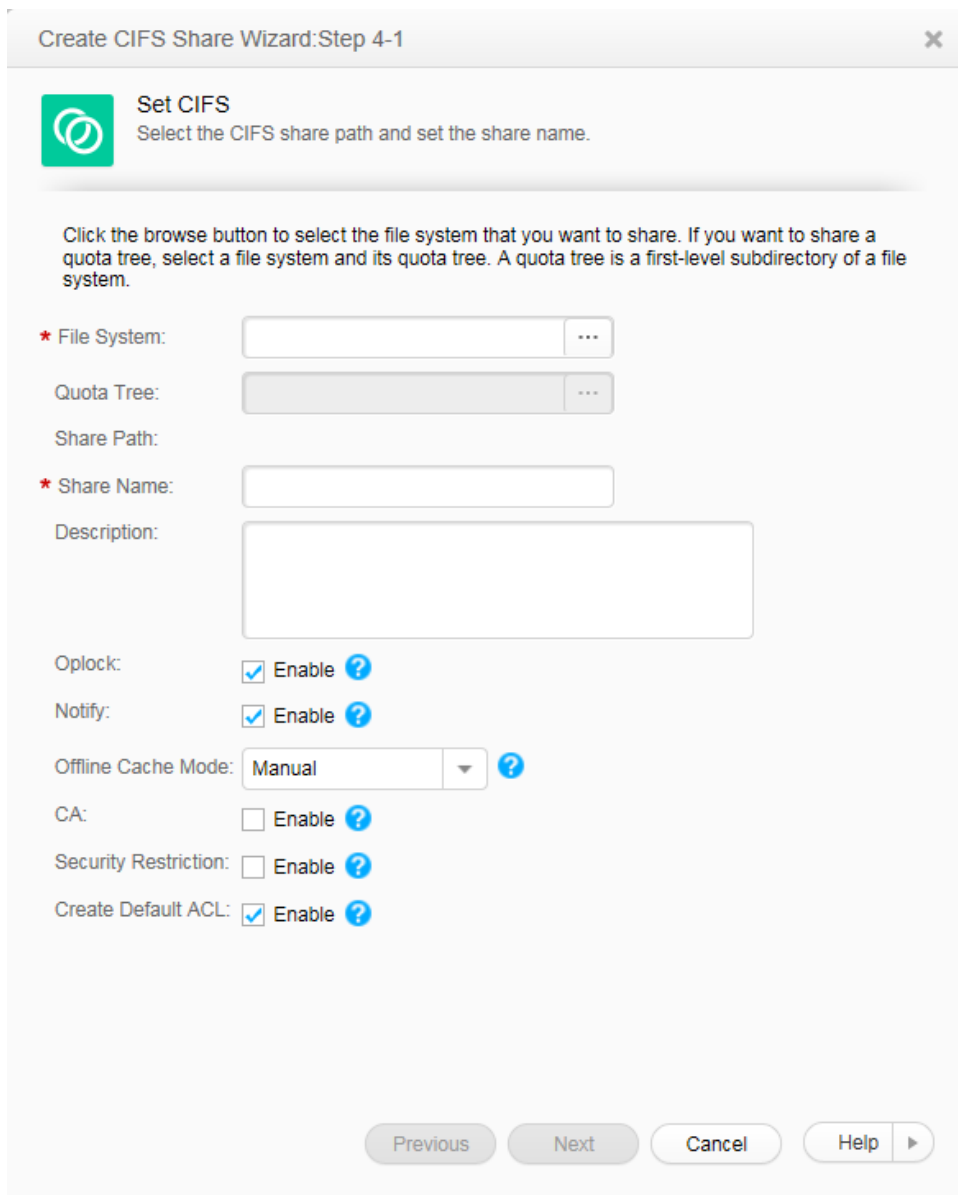
Table 3-8 describes the related parameters.

Table 3-8 Parameters for creating a CIFS share

Parameter	Description	Value
File System	File system for which you want to create a CIFS share.	[Example] Filesystem001

Parameter	Description	Value
Quota Tree	Level-1 directory under the root directory of the file system.	To share a quota tree, click [···] and select a quota tree you want to share. [Example] Share **NOTE** The share path is /**Filesystem001/Share**.
Share Name	Name used by a user for accessing the shared resources.	[Value range] – The share name can be in Chinese, English, or Japanese. – 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	[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 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

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.
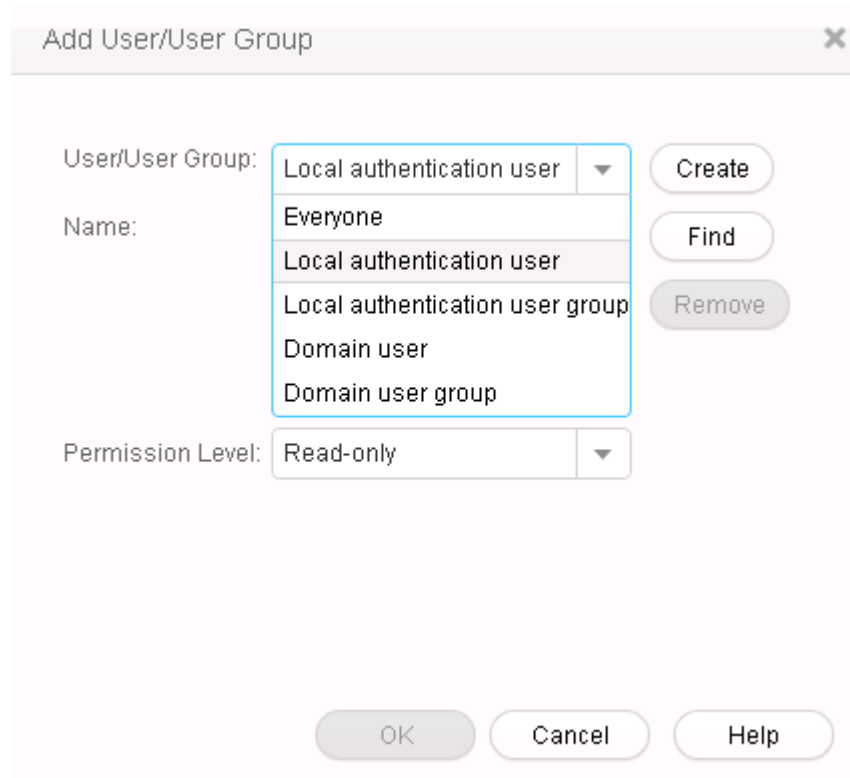
2. In **User/User Group**, select user type or user group type.

    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

        n **Everyone** means every user has the access permission.

        n 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 3-9 provides details about the permissions.

    Table 3-9 Description of CIFS share permissions

Permission	Forbidden	Read-Only	Read and Write	Full Control
Viewing files and subdirectories	X[a]	√[b]	√	√

Permission	Forbidden	Read-Only	Read and Write	Full Control
Viewing the contents of files	X	√	√	√
Running executable files	X	√	√	√
Adding files or subdirectories	X	-c	√	√
Modifying the contents of files	X	-	√	√
Deleting files and subdirectories	X	-	√	√
Renaming	X	-	√	√
Changing the ACL of files or directories	X	-	-	√
a: Users do not have the permission specified in the **Permission** column.				
b: Users have the permission specified in the **Permission** column.				
c: The permission specified in the **Permission** column is not involved.				

📖**NOTE**

The permission priority from high to low is **Forbidden** > **Full control** > **Read and write** > **Read-only**. The highest permission prevails. If a user adopts a higher permission than its original permission, the new permission takes effect immediately without re-authentication. For example, the access permission of a user is **Read-only**, and then the user is added to a user group whose access permission is **Full control**, therefore the access permission of the user is upgraded to **Full control**. Then you can access the CIFS share immediately without re-authentication.

4. Click **OK**.

The system adds the user or user group you select to the **Users/User Groups** list.

5. Click **Next**.

The **Security Restriction** page is displayed.

Step 6 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 notsupported.

        –   The IP rule can be:

          n   A single IPv4 or IPv6 address, for example, 192.168.1.100.

          n   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**.

       The **Summary** page is displayed.

Step 7   On the **Summary** page, check whether the CIFS information is correct. Click **Finish**.

Step 8 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

3.3.9 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 a logical port 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**.

    l 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**.

    l 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 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 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 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.)

3.3.10 Connecting MMC to the Storage System

mRAID16 enables the MMC console to manage CIFS shares (viewing a CIFS share and setting share permissions) and local authentication users and user groups (viewing a local user and a user group, adding a local authentication user to a local user group, and adding members to a local user group). This section describes how to connect MMC to the storage system.

Prerequisites

A user has been created on a Windows client and added to the administrator user group of the storage system.

> **NOTE**
>
> Because Windows has restrictions, the administrator users must be disabled on the client. Otherwise, Windows does not search for users or user groups in the storage system.

IP addresses have been configured for logical ports of the storage system.

To manage local authentication users and user groups of the storage system in MMC, you must add the storage system and client to the same AD domain.

Context

This section uses Windows 7 as an example to describe how to connect MMC to the storage system.

Procedure

Step 1 Right-click **Computer** and choose **Manage**.

The **Computer Management** dialog box is displayed.

Step 2 In the navigation tree, right-click **Computer Management** and choose **Connect to another computer (C)**.

The **Select Computer** dialog box is displayed.

Step 3 In **Another computer (A)**, enter the logical port IP address of the storage system.

Step 4   Click **OK**.

----End

3.4 Configuring a Homedir Share

mRAID16 supports the Homedir share mode. After the Homedir share service is enabled, a user can only access the shared directory with the same name as the user.

3.4.1 Configuration Process

Homedir shares are applicable to both an AD domain and a non-domain environment. This section describes the Homedir share configuration process.

Figure 3-4 shows the Homedir share configuration process.

Figure 3-4 Homedir share configuration process
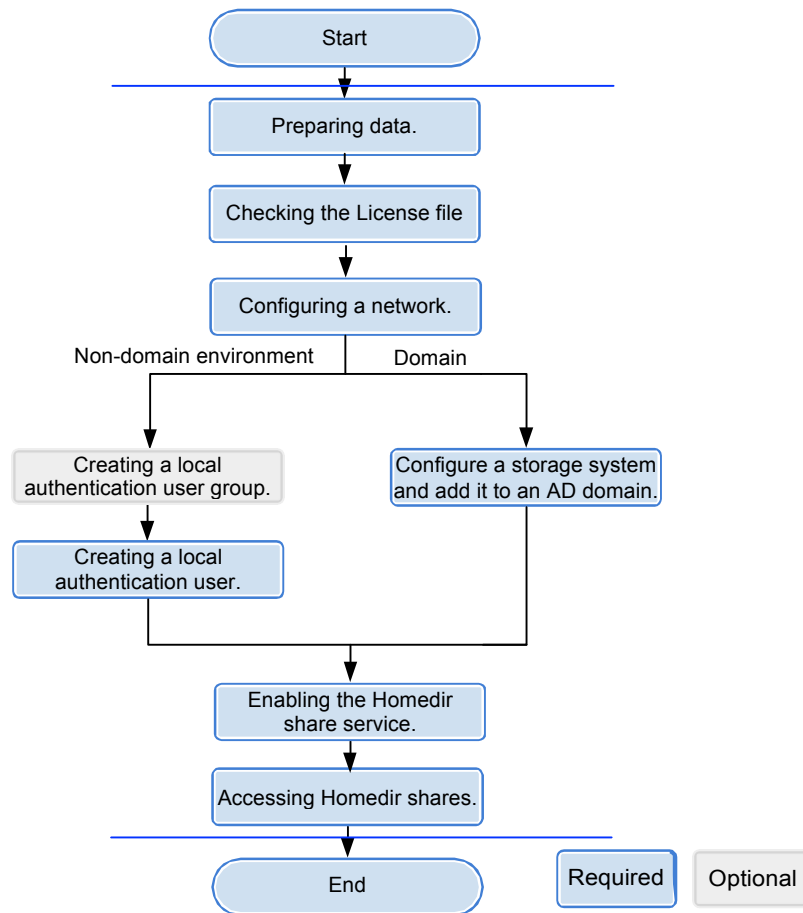
3.4.2 Preparing Data

Before configuring a Homedir share, obtain information about storage system IP address, file system, quota tree, local users in non-domain environment or AD server in AD domain environment to assist in the follow-up configuration.

Table 3-10 describes preparations required for configuring a Homedir share.

Table 3-10 Preparations required for configuring a Homedir 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 Homedir share is configured.*	mRAID16 enables you to configure a file system or its quota tree as a Homedir share.	FileSystem001
Quota Tree *Indicates the quota treefor which a Homedir share is configured.*	-	-

Item	Description	Example
User *User that employs local authentication.*	The user name: lMust contain 8 to 32 characters by default. lCannot 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: l 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**. lUser accounts retained in Linux: **root**, **nogroup**, **nobody**, **ftp**, **anonymous**. lUser 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: lMust contain 1 to 32 characters. lCannot 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: l 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**. lUser accounts retained in Linux: **root**, **nogroup**, **nobody**, **ftp**, **anonymous**. lUser accounts retained in a storage system: **ibc_os_hs**.	default_group
AD domain information *AD domain information for domain authentication.*	AD domain information includes: lUser name of the domain administrator: The AD domain can provide an account that has the rights to add storage systems to the domain. lPassword: password of the user. lFull domain name: name of the AD domain lOrganization 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. lSystem name: name of a storage system that is added to the AD domain	-
DNS *DNS information for domain authentication.*	IP address of DNS server.	-

📖**NOTE**

You can contact your network administrator to obtain desired data.

3.4.3 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.

Procedure

Step 1 Log in to ActiveManager.

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 file.

----End

Follow-up Procedure

If no license is available, purchase, import and activate one.

3.4.4 Configuring a Network

This section describes how to use ActiveManager to configure IP addresses for a storage system.

Procedure

Step 1 Log in to ActiveManager and choose 🔄**Provisioning** > **Port**.

The **Port** page is displayed.

Step 2 **Optional:** Create a bond port.

Bond ports can increase link bandwidth and redundancy. Create bond ports based on site requirements. After bonding, the mode of all switch ports connected to the Ethernet port must be configured to 802.3AD LACP.

📖**NOTE**

The port bond mode of a storage system has the following restrictions:

l Only the interface modules with the same port rate (GE or 10GE) can be bonded.

lInterface modules cannot be bonded across controllers. Non-Ethernet network ports cannot be bonded. TOE interface modules cannot be bonded across cards.

lSmartIO interface modules cannot be bonded if they work in cluster or FC mode or run FCoE service in FCoE/iSCSI mode.

l Each port only allows to be added to one bond port. It cannot be added to multiple bond ports.

1. In **Ethernet Ports**, select a Ethernet port and click **More** > **Bond Port**.

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

2. Enter bond port information. **Table 3-11** describes related parameters.

Table 3-11 Bond port parameters

Parameter	Description	Value
Bond Name	Name of the bond port.	[Example] bond01
Available Ports	Ports that you select and ports to which you want to bond the selected ports.	[Example] CTE0.A.IOM1.P0

3. Click **OK**.

    The **Danger** dialog box is displayed.

4. Select **I have read and understood the consequences associated with performing this operation.** And click **OK**.

Step 3 Create a logical port.

📖**NOTE**

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.

1. Select **Logical Ports** and click **Create**.

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

2. Enter logical port information. **Table 3-12** describes related parameters.

Table 3-12 Create Logical Port parameters

Parameter	Description	Value
Name	Name of the logical port.	[Example] logip
IP Address Type	Type of the IP address: **IPv4 Address** or **IPv6 Address**.	[Example] IPv4 Address
IPv4 Address (IPv6 Address)	IP address of the logical port.	[Example] 172.16.128.10
Subnet Mask (Prefix)	Subnet mask (Prefix) of the logical port.	[Example] 255.255.255.0
IPv4 Gateway (IPv6 Gateway)	Address of the gateway.	[Example] 172.16.128.1
Primary Port	Physical port preferred by the logical port.	[Example] CTE0.A.IOM0.P0

Parameter	Description	Value
IP Address Floating	Whether IP address floating is enabled. mRAID16 support IP address floating. When the primary port is disabled, the IP address will be floated to another port that can be used. **NOTE** Shares of file systems do not support the multipathing mode. IP address floating is used to improve reliability of links.	[Example] Enable
Failback Mode	Failback mode of the IP address: **Automatic** and **Manual**. **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
Activate Now	Whether the logical port is activated immediately. After activated, the logical IP can be used to access the shared space.	[Example] Enable

3. Click **OK**.

   The **Success** dialog box is displayed.

4. Click **OK**.

Step 4 **Optional:** Managing a Route.

   You need to configure a route when the CIFS server and the storage system are not on the same network.

l 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.

l 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.

1.   Select the locical port for which you want to add a route and click **Route Management**.

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

2.   Configure the route information for the logical port.

a.   In **IP Address**, select the IP address of the logical port.

b.   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).

---

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

There are three route options:

n   Default route

Data is forwarded through this route by default if no preferred route is
available. The target address field and the target mask field (IPv4) or prefix
(IPv6) of the default route are automatically set to 0. To use this option, you
only need to add a gateway.

n   Host route

The host route is the route to an individual host. The target mask (IPv4) or
prefix (IPv6) of the host route are automatically set respectively to
255.255.255.255 or 128. To use this option, you only need to add the target
address and a gateway.

n   Network segment route

The network segment route is the route to a network segment. You need to add
the target address, target mask (IPv4) or prefix (IPv6), and gateway. Such as
the target address is 172.17.0.0, target mask is 255.255.0.0, and gateway is
172.16.0.1.

d.   Set **Destination Address**.

n   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.

n   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.

n   Set **Destination Mask** (IPv4) or **Prefix** (IPv6).

n 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.

n   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.

e.   In **Gateway**, enter the gateway of the local storage system's logical port IP address.

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

The **Danger** dialog box is displayed.

4.   Confirm the information of the dialog box and select **I have read and understood the consequences associated with performing this operation.**.

5.   Click **OK**.

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

📖**NOTE**

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

6.   Click **Close**.

----End

3.4.5 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 in the mRAID16 , you can access Homedir shares as a local user.

3.4.5.1 (Optional) Creating a Local Authentication User Group

This section describes how to create a local authentication user group. Local authentication user groups can manage the 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.

l **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.

l **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.

l **AntivirusGroup**: antivirus user group. The group members can use third-party antivirus software to scan for shared file systems. They have administrator permissions.

      l **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 ActiveManager.

Step 2   Choose   **Provisioning** > **User Authentication** > **Local Authentication User Group**.

Step 3   Click **Create**.

      The **Local Authentication User Group** dialog box is displayed.

      Local Authentication User Group   ✕

        ★ User Group Name: [   ]

        Description: [   ]

          (OK)   (Cancel)   (Help)

Step 4   In **User Group Name**, enter a new user group name.

      NOTE

      l 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 (.).

      l Contains 1 to 32 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

3.4.5.2 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 ActiveManager.

Step 2 Choose ![icon]**Provisioning** > ![icon]**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:

l 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 (.).

l 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:

l Contain 8 to 16 characters.

l Contain special characters. Special characters include: !"#$%&'()*+,-./:;<=>?
@[\]^`{_|}~ and space.

l Contain any two types of the uppercase letters, lowercase letters, and digits.

l Cannot contain three consecutive same characters.

l 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. For security purpose, you are advised to select **Password Validity**
> **Period (Days)**. After you select this item, your password will never expire. The default validity period is
> 180 days. After the password expires, the user cannot access shares. 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.

Step 9 Select the user group to which the user belongs to and click **OK**.

Step 10 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

3.4.6 Configuring a Storage System to Add It to an AD Domain

In a domain, after the Homedir share service is enabled in the mRAID16 , you can
access Homedir shares as a domain user.

3.4.6.1 Connecting a Storage System to the 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.

Context

l A DNS server is used to resolve host names in a domain.

l 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 ActiveManager.

Step 2 Choose ⚙ **Settings** > 🔧 **Basic Information** > **DNS Service**.

Step 3 Set the DNS information.

Device Information	💡 View and configure the active or standby DNS server IP address.
Device Time	Active DNS IP Address:
DNS Service ▶	Standby DNS IP Address 1:
	Standby DNS IP Address 2:

1. Set **Active DNS IP Address**.
2. **Optional:** Set **Standby DNS IP Address 1**.
3. **Optional:** Set **Standby DNS IP Address 2**.

📖**NOTE**

Please configure the standby DNS IP address 1 first and then the standby DNS IP address 2.

Step 4 Click **Save**.

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

Step 5 Click **OK**.

----End

3.4.6.2 Configuring a Storage System to AD Domain

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

l An AD domain has been set up.

l The storage system has been connected to the DNS server.

l AD domain server and DNS server must have time synchronization with storage system. The time difference must be no larger than 5 minutes.

📖**NOTE**

l mRAID16 storage system can be connected to the AD domain and DNS server through the management port or the service port (ethernet port or logical port). When using the management port to connect to the AD server, it requires all the controllers can communicate with the AD server. You are advised to use the service port to connect to the AD server.

l AD domain servers support the primary/secondary domain, parent/child domain, active/standby domain, or trust domain. One storage system can be connected to only one AD domain server.

Precautions

l 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.

l Simple password may cause security risk. Complicated password is recommended, for example, password contains uppercases, lowercases, digits and special characters.

l 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 ActiveManager.

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 3-13**.

Table 3-13 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
Password	Password of an administrator who logs in to the AD domain server.	[Rule] Contains 1 to 127 letters. [Example] !QAZ2wsx
Full Domain Name	Full domain name of the AD domain server	[Rule] Contains 1 to 127 characters. [Example] abc.com
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
System Name	Name of a domain to which a client will be added. 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

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 ADdomain.

3.4.7 Enabling the Homedir Share Service

After the Homedir share service is enabled, mRAID16 supports Homedir shares.

Prerequisites

A file system whose Homedir share service must be enabled has been created.

Procedure

Step 1 Log in to **ActiveManager**.

Step 2 Choose **Settings** > **Storage Settings** > **File Storage Service** > **CIFS Service**.

Step 3 In **CIFS Service**, 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

3.4.8 Accessing Homedir Shares

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 a logical port IP address of the storage system, and *sharename* indicates the name of the Homedir share.

📖**NOTE**

> In a domain, enter the domain user name in the **~Domain name~Domain user name** format in *User Name*.

> In a non-domain environment, 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**.

l 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**.

l 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 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.)

3.5 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.

3.5.1 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 3-5](#) shows the customer's network.

Figure 3-5 Customer's network diagram
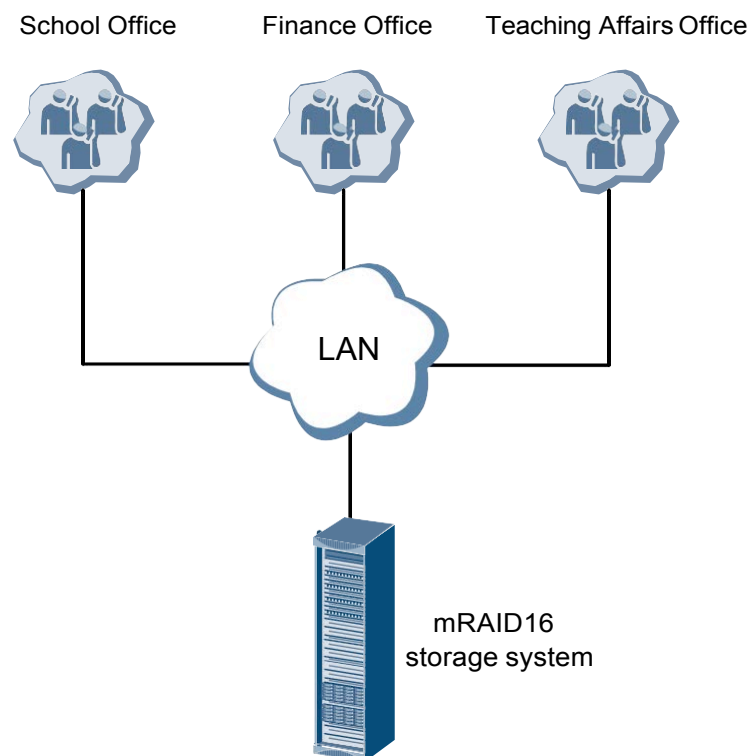
The status quo of the customer's live network can be concluded as follows:

l All clients use the Windows operating system.

l 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:

l Each of the three departments has 1 TB dedicated storage space.

l The three departments can write and read data in their respective 1 TB storage space.

l The School Office can access but cannot write or modify the storage space of the Teaching Affairs Office and the Finance Office.

l The Teaching Affairs Office can access but cannot write or modify the storage space of the Finance Office.

l The Finance Office can access but cannot write or modify the storage space of the Teaching Affairs Office.

l The Teaching Affairs Office and Finance Office cannot access the storage space of the School Office.

3.5.2 Requirement Analysis

This section analyzes the customer's requirements and provides a solution.

The customer's requirements are analyzed as follows:

l All clients use the Windows operating system, so themRAID16 storage system can use the CIFS share to provide storage space for the three departments respectively.

l mRAID16 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:

l **Table 3-14** describes the basic information of the three departments.

Table 3-14 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

l **Table 3-15** describes each local user group's permission to access the storage space of the School Office, Finance Office, and Teaching Affairs Office.

Table 3-15 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

3.5.3 Configuration Process

The preceding solutions and the following configuration flowchart help you understand the subsequent configuration.

Figure 3-6 shows the configuration process.

Figure 3-6 Configuration process
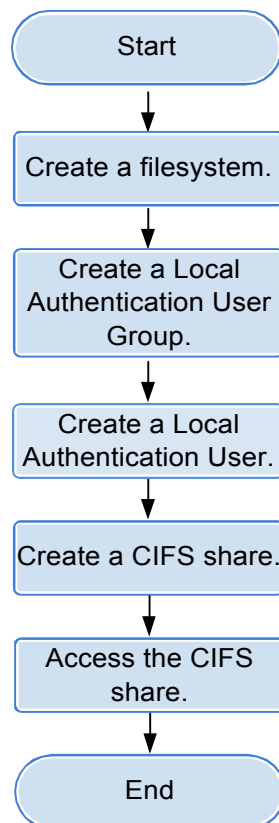
3.5.4 Configuration Operations

After requirement analysis and service planning, you need to configure a CIFS share on ActiveManager.

3.5.4.1 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.

Procedure

Step 1 On the ActiveManager 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 3-16** describes related parameters.

Table 3-16 Create File System parameters

Parameter	Planned Value
Name	FileSystem
Capacity	1 TB
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

3.5.4.2 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.

Procedure

Step 1 On the **ActiveManager** 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

3.5.4.3 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.

Procedure

Step 1 On the **ActiveManager** page, click ![icon] **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 3-17** describes related parameters.

Table 3-17 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

3.5.4.4 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.

Procedure

Step 1 On the ActiveManager page, choose ![icon] **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 **Summary** page is displayed.

5. Click **Finish**.

    The **Execution Result** page is displayed.

6. 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 3-18** lists planned access permissions.

Table 3-18 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

3.5.4.5 Accessing Shared Space

This section describes how the departments access 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.

Context

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.

Procedure

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

3.6 Managing an CIFS Share

After an CIFS share is configured for a storage system, you need to manage and maintain the CIFS share. This section describes how to manage an CIFS share.

3.6.1 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 ActiveManager.

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 3-19**.
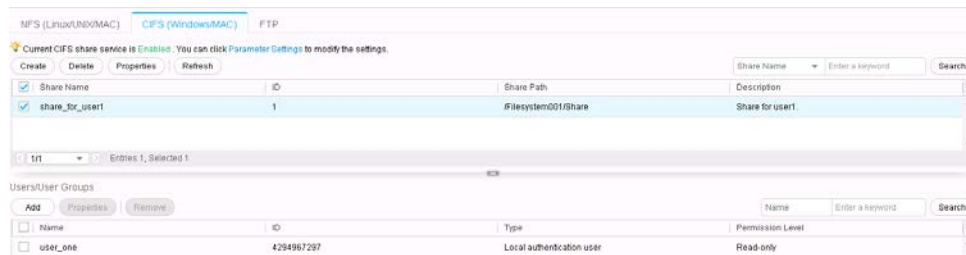
Table 3-19 CIFS Share Information

Parameter Name	Description
Share Name	The name of CIFS share.
Share Path	The directory of CIFS share.
ID	The ID of CIFS share.
Description	The description of CIFS share.

Step 4 In CIFS share list, select a CIFS share. In **Users/User Groups** list, check the permission of the user or user group of this CIFS share. The related parameters are shown in **Table 3-20**.

Table 3-20 User/User Group Information

Parameter Name	Description
Name	The name of a user or a user group.

Type	The type of a user or user group. The types include:
	lEveryone
	    Every user has the access permission.
	lLocal authentication user
	    The authentication user created in the storage system.
	lLocal authentication user group
	    The authentication user group created in the storage system.
	lDomain user
	    The user in AD domain server.
	lDomain user group
	    The user group in AD domain server.

Permission Level	The CIFS share access permission. The permissions include: l**Full control**: have all rights for CIFS share. l**Read-only**: only have read right for CIFS share. (Default value) l**Read and write**: have read and write right for CIFS share. l**Forbidden**: access is forbidden.

Parameter Name	Description
ID	The ID of share permission.

----End

3.6.2 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 ActiveManager.

Step 2 Choose ![icon] **Provisioning** > ![icon] **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

3.6.3 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 ActiveManager.

Step 2 Choose ![icon] **Provisioning** > ![icon] **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 Add user or user group for accessing the CIFS share.

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**.

3. If you select **Everyone**, click **Add**.

   The system add **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 access permission for the user or user group added.

   The CIFS access permission levels 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.

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.
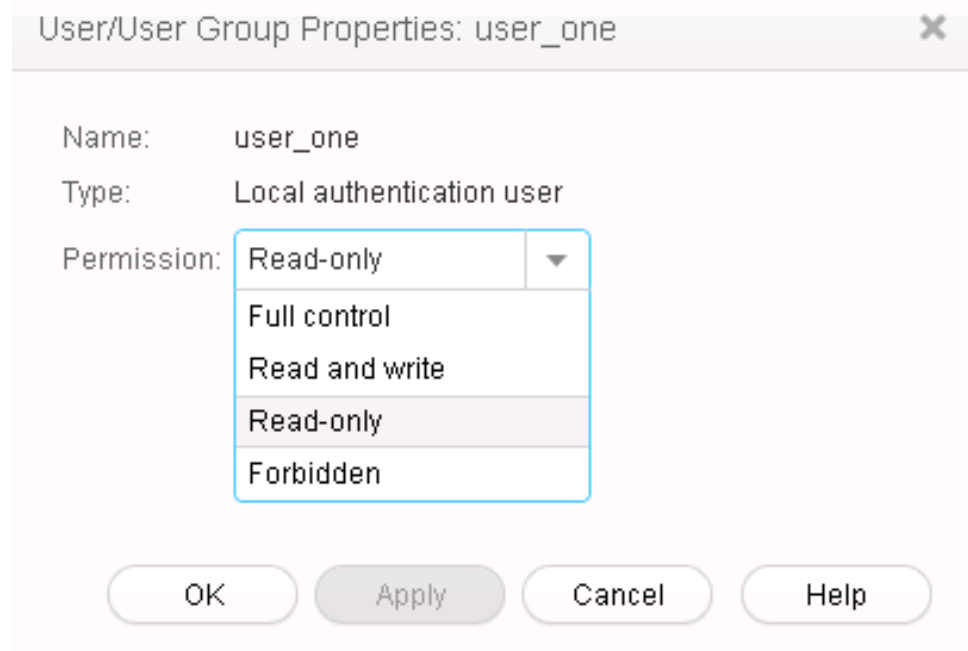
2. Select a new permission for the user or user group.

    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

3.6.4 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 ActiveManager.
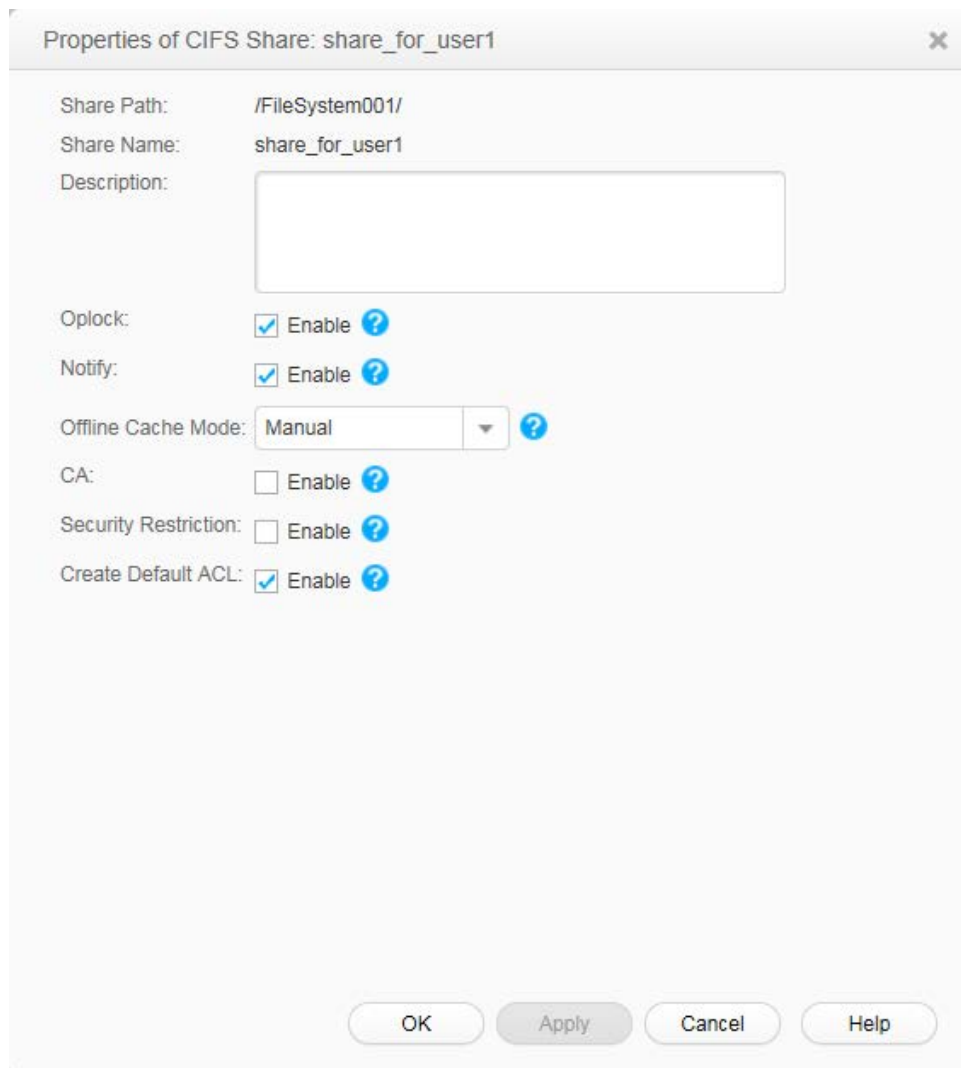
Step 2 Choose ![icon] **Provisioning** > ![icon] **Share** > **CIFS (Windows/MAC)**.

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.

The **Table 3-21** describes the related parameters.

Table 3-21 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.
Oplock	Opportunistic locking (Oplock) is a mechanism that improves client access efficiency. After this mechanism is enabled, files are cached locally before being sent to shared storage.	[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: lNone 　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. lManual 　Specified files and programs in the shared directory can be cached to local clients and operated offline. lDocuments 　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. lPrograms 　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

Step 6 Click **OK**.

The **Execution Result** dialog box is displayed.

Step 7 Click **Close** to finish modifying the CIFS properties.

----End

3.6.5 Modifying the 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 ActiveManager.

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 Add accessible IP addresses or IP address segments.

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 segmentsthat 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:

   n A single IPv4 or IPv6 address, for example, 192.168.1.100.

   n 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/ Address Segment** list.

Step 5 Modify an IP address or IP address segment.

1. In **Accessible IP Address/Address Segment**, select the IP address or IPaddress segment that you want to remove and click **Properties**.

   The **Accessible IP Address/Address Segment** dialog box is displayed.

2. In **IP Address/Address Segment**, specify the IP addresses or IP address segmentsthat 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:

   n A single IPv4 or IPv6 address, for example, 192.168.1.100.

   n 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/Address Segment**, select the IP address or IPaddress 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

3.6.6 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.

l **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.

l **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.

l **AntivirusGroup**: antivirus user group. The group members can use third-party antivirus software to scan for shared file systems. They have administrator permissions.

l **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 ActiveManager.

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**

l 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 (.).

l Contains 1 to 32 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

3.6.7 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 ActiveManager.

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:

l 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 (.).

l 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:

l Contain 8 to 16 characters.

l Contain special characters. Special characters include: !"#$%&'()*+,-./:;<=>?
   @[\]^`{_|}~ and space.

l Contain any two types of the uppercase letters, lowercase letters, and digits.

l Cannot contain three consecutive same characters.

l 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. For security purpose, you are advised to select **Password Validity
> Period (Days)**. After you select this item, your password will never expire. The default validity period is
> 180 days. After the password expires, the user cannot access shares. 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.

Step 9   Select the user group to which the user belongs to and click **OK**.

Step 10   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

3.6.8 Viewing Local Authentication User Group Information

View the information about a local authentication user group. The information include user group name, description and information of users in this group.

Procedure

Step 1   Log in to ActiveManager.

Step 2   Choose ![icon] **Provisioning** > ![icon] **User Authentication** > **Local Authentication User Group**.

Step 3 Check the local authentication user group information. The parameters are as shown in **Table 3-22**.

Table 3-22 Local Authentication User Group Information

Parameter	Description
Name	The name of a local authentication user group.
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 3-23**.

Table 3-23 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: lNormal: the user can access the share. lLock: 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 3-24**.

Table 3-24 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 3-25**.

Table 3-25 Domain User Group Information

Parameter	Description
Name	The name of a domain user group.
ID	The ID of a domain user group.

----End

3.6.9 Viewing Local Authentication User Information

View the information about a local authentication user. The information include name, status, primary group, secondary group, description and so on.

Procedure

Step 1 Log in to ActiveManager.

Step 2 Choose ![icon]**Provisioning** > ![icon]**User Authentication**.

Step 3 Check the local authentication user information. The parameters are shown as in **Table 3-26**.

Table 3-26 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: lNormal: the user can access the share. lLock: the user cannot access the share.
ID	The ID of a local authentication user.

Parameter	Description
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.

----End

3.6.10 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 ActiveManager.

Step 2 Choose ![icon] **Provisioning** > ![icon] **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

3.6.11 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 ActiveManager.

Step 2   Choose ![icon]**Provisioning** > ![icon]**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

3.6.12 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 ActiveManager.

Step 2   Choose ![icon]**Provisioning** > ![icon]**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

3.6.13 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 ActiveManager.

Step 2 Choose ![icon] **Provisioning** > ![icon] **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

3.6.14 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 ActiveManager.

Step 2 Choose ![icon] **Provisioning** > ![icon] **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.

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

3.6.15 Modifying the Owning Sub-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 ActiveManager.

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

3.6.16 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 ActiveManager.

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

3.6.17 Adding/Removing a User from 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 ActiveManager.

Step 2 Choose [icon] **Provisioning** > [icon] **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.

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.
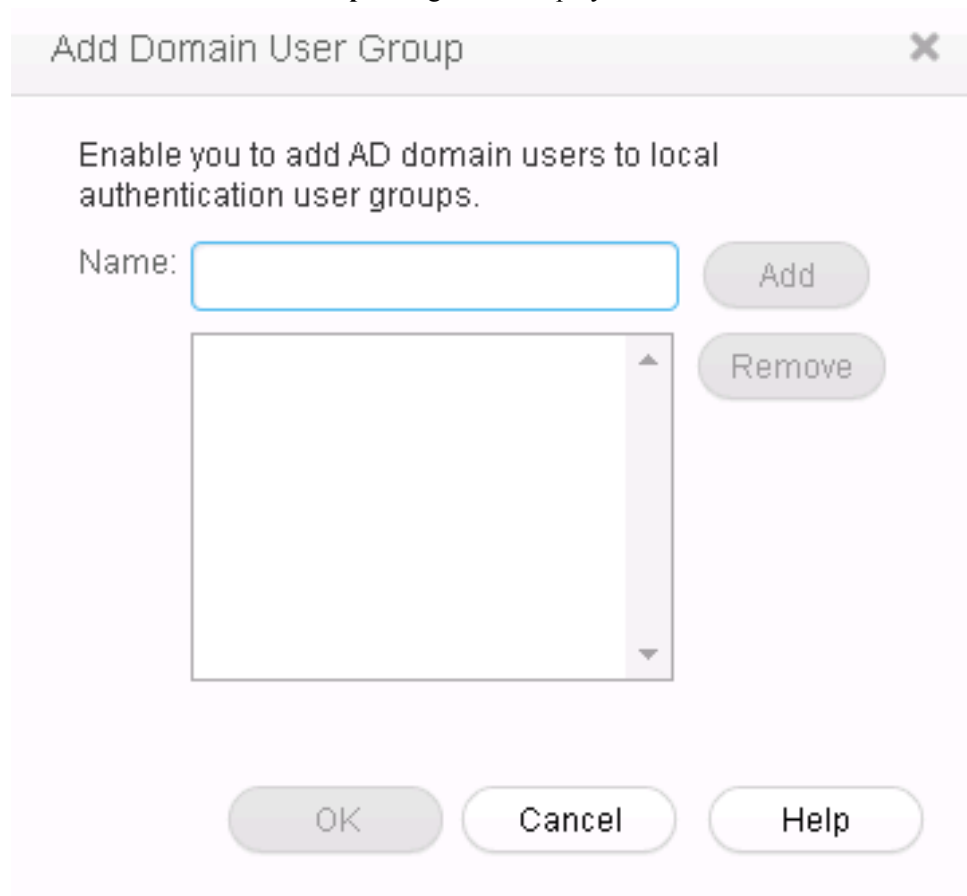
1. Click the **Domain User** tab.

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.

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
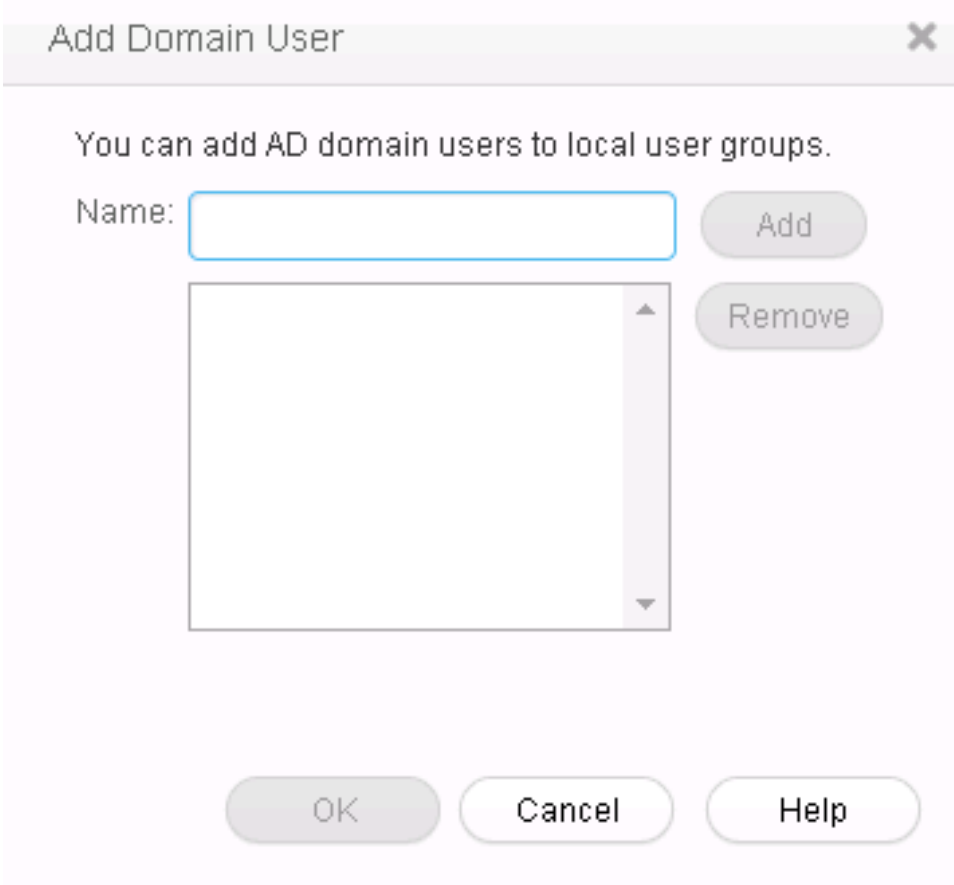
3.6.18 Configuring Security Policy for Local Authentication User

Security policies include the password policy and login policy. Security policies are used to protect the system security.

Procedure

Step 1 Log in to ActiveManager.

Step 2 Choose ![icon] **Provisioning** > ![icon] **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 3-27** describes the related parameter.
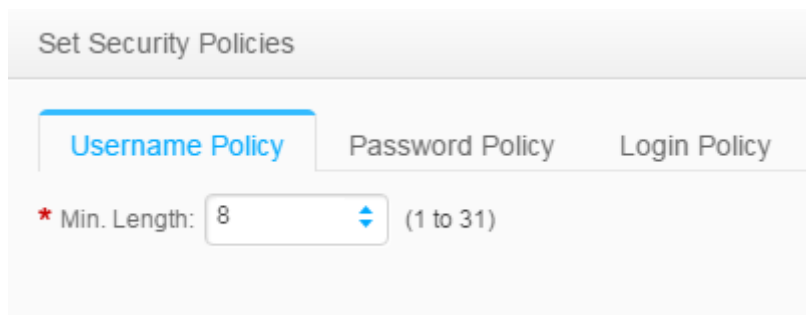
Table 3-27 Username Policy

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 3-28** describes related parameters.
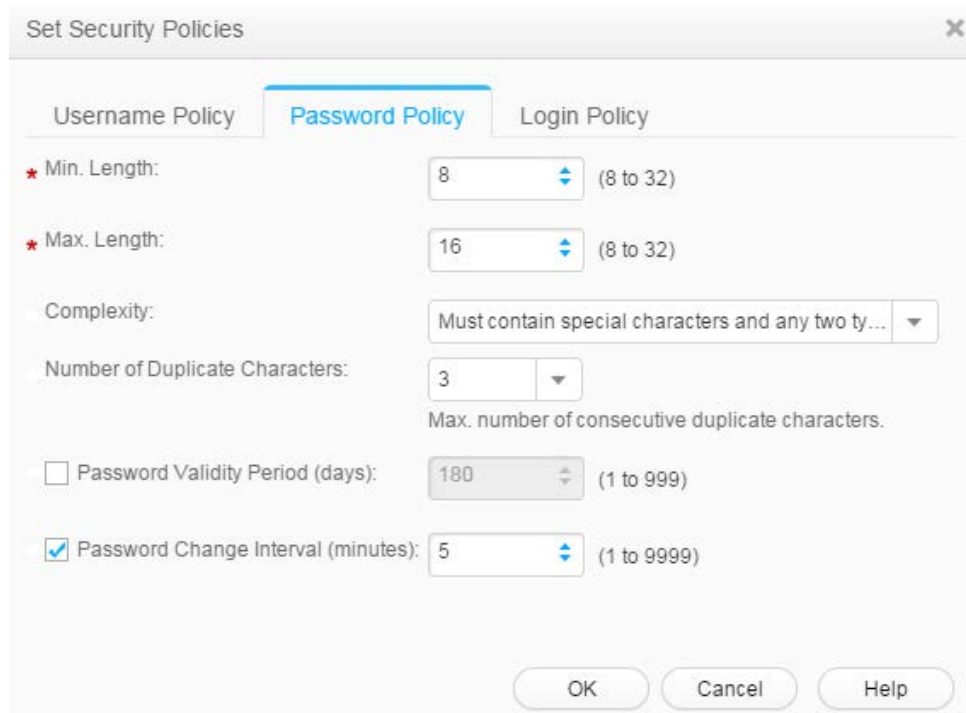
Table 3-28 Password Policy

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: l Must contain special characters and any two types of uppercase letters, lowercase letters and digits lMust 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**. After **Password Validity Period** 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.	[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 3-29** describe related parameters.
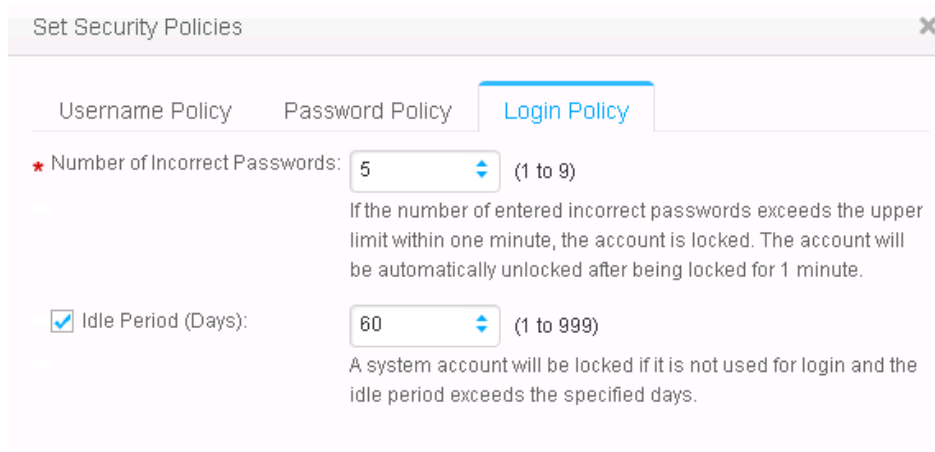
Table 3-29 Login Policy

Parameter	Description	Value
Number of Incorrect Passwords	Times allowed for consecutively entering incorrect passwords. 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 9. [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

4 Cross-Protocol Share Access

About This Chapter

mRAID16 allows NFS sharing and CIFS sharing to be configured for the same file system concurrently. This chapter describes how mRAID16 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.

4.1 Overview
This section introduces the user mapping mechanism used during cross-protocol (CIFS-NFS) share access.

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.

4.3 Accessing a CIFS File AcrossProtocols
This section describes how an NFS client accesses CIFS files and directories for which the NT ACL permission has been configured.

4.4 Accessing an NFS File AcrossProtocols
This section describes how a CIFS client accesses an NFS share for which the UNIX permission has been configured.

4.1 Overview

This section introduces the user mapping mechanism used during cross-protocol (CIFS-NFS) share access.

CIFS-NFS Cross-Protocol Share Access

The mRAID16 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, themRAID16 manages user mapping and permission control of different operating systems in a unified manner, protecting the security of CIFS-NFS cross-protocol access.

l If a CIFS user attempts to access a file or directory on the   , themRAID16 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 themRAID16 performs UNIX permission authentication for the user.

l If an NFS user attempts to access a file or directory that has NT ACL on the   , the NFS user is mapped as a CIFS user based on the preset mapping rules. ThenthemRAID16 performs NT ACL permission authentication for theuser.

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.

l 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.

l 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 check permissions.

Table 4-1 shows how permissions convert among UNIX Mode bits, NFSv4 ACL, and NT ACL.

Table 4-1 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.	lOne ACL is mapped based on UNIX Mode bits when an NFS or CIFS client sends a request to read an ACL. lIf 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. lIf 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.
The file or directory has a valid NFSv4 ACL or NT ACL.	l NFS clients use the **chmod** command to change permissions. The NFSv4 ACL or NT ACL is abandoned and UNIX Mode bits take effect. lNFS 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.	l 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. lIf a CIFS client sends a request to read an NT ACL, an NT ACL is mapped based on UNIX Mode bits of the storage system. l If a CIFS client sends a request to set an NT ACL, 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.	lIf 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. l 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. lIf 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:

l 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.

l 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:

l 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.

l 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.

l 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.

l 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.

l If mappings are changed on CIFS clients, the change takes effect after next authentication.

l 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 is used as an example.)

l 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.

l 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.

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.

4.2.1 Configuring Mapping Parameters

You can create user mappings in the local system as well as use user mapping 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.

Procedure

Step 1 Log in to ActiveManager.

Step 2 Choose ⟳**Provisioning** > 👤**User Authentication** > **User Mapping**.

Step 3 Click **Set Mapping Parameters**.

Step 4 Set the mapping parameters by referring to **Table 4-2**.

Table 4-2 Parameter description

Parameter Name	Description	Value
Mapping Mode	A global parameter of user mappings, including: l User mapping not supported: The system does not support user mappings. l User mapping supported(Mapping rules set in local): The system only supports user mappings created locally. l User mapping supported(Mapping rules set in IDMU): The system only supports user mappings in the IDMU domain. l 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. l 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. Otherwise, the mappings in the IDMU domain are used.	[Example] User mapping supported(Mapping rules set in IDMU): The 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=auth2h8,DC=com

Step 5 Click **OK**.

The **Success** dialog box is displayed.

Step 6 Click **OK**.

----End

4.2.2 Creating a 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 ActiveManager.

Step 2 Choose ![icon] **Provisioning** > ![icon] **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 4-3** explains the related parameters.

Table 4-3 User mapping parameters

Parameter Name	Description	Value
Mapping Type	A user mapping type related to the operating system, including: lWindows to Unix: When accessing Unix shares using Windows, a Windows user has all the permissions granted to the target user. lUnix 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 to check whether the target user exists.

> **NOTE**
>
> Click to delete the user mapping.

Step 7 Click **OK**.

Step 8 Click **Close**.

----End

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

l 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 ActiveManager. 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.

l 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.

l Ensure that the storage system has been added to **Windows Authorization Access Group** on the AD domain server.

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 4-1** to configure related parameters.

Figure 4-1 Flowchart of configuring cross-protocol access of a CIFS file
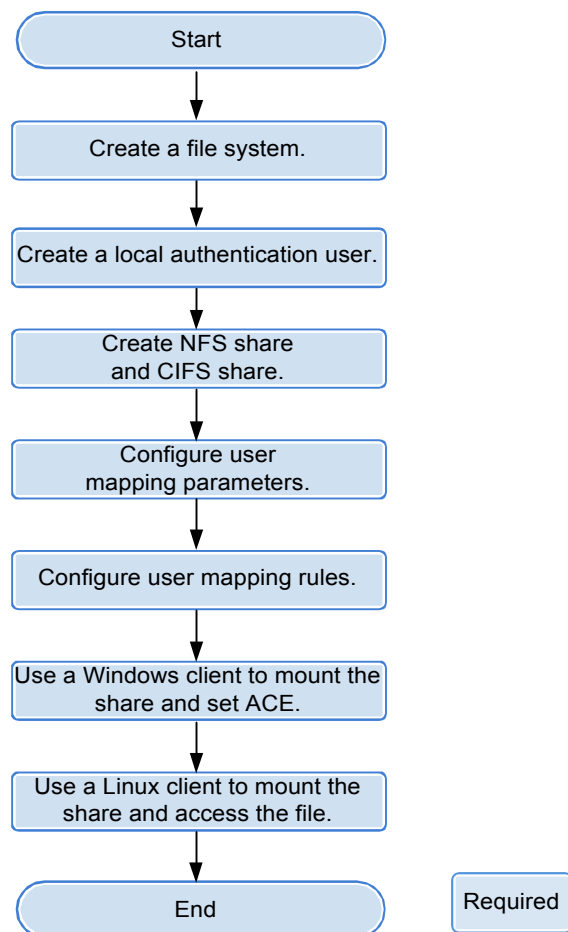
Table 4-4 provides an example of data planning during the configuration.

Table 4-4 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.
NFS share	l Type of the client: Host l Name or IP address: 10.68.0.10 l Permission: Read-write l 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	l Share Name: share_dir_cifs l l Oplock: Enable Notify: Enable l User/User Group: local authentication user **local_user1** l 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	l Mapping Type: Unix to Windows l Source User: **linux_user1** l Target User: **local_user1** l 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 ActiveManager.

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 4-2 Recording the ID of the local authentication user

    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 4-3 Recording the ID of the owning primary group of the local authentication user

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 4-4 Configuring user mapping parameters

Step 6 Configure user mapping rules.

1. Select **Provisioning** > **User Authentication** > **User Mapping**.

2. Click **Create** and configure user mapping rules as planned.

Figure 4-5 Configuring user mapping rules

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**.
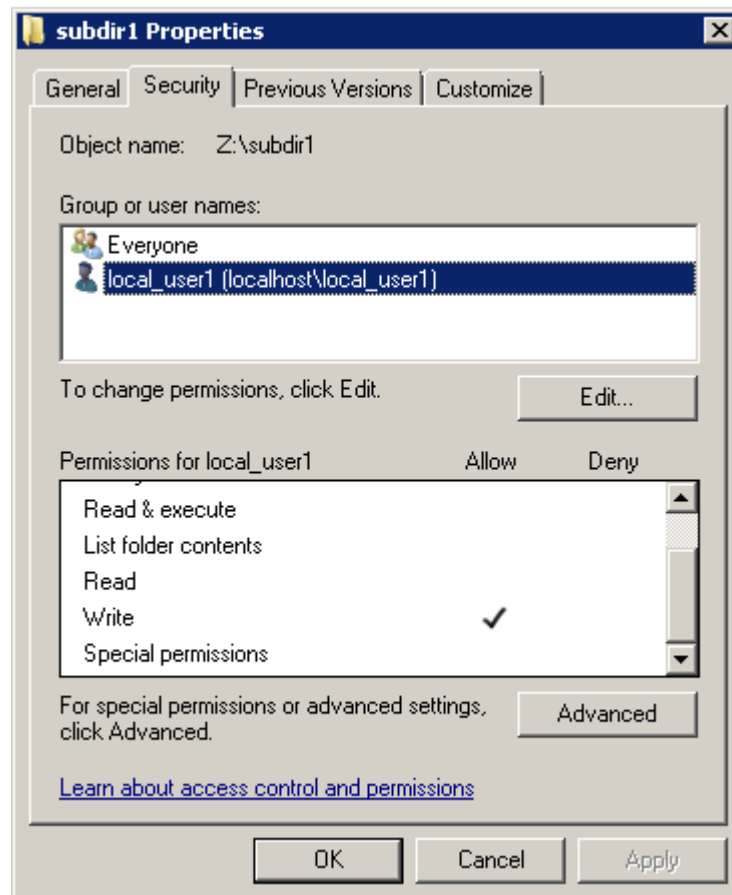
Step 8 Use an NFS client to mount the share and access the share as local user **linux_user1**.

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

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

l The IDMU component has been installed on the AD domain server and the NIS has been enabled.

l 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.

l 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 ActiveManager. 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.

l 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 4-6** to configure related parameters.

Figure 4-6 Flowchart of configuring cross-protocol access of an NFS file
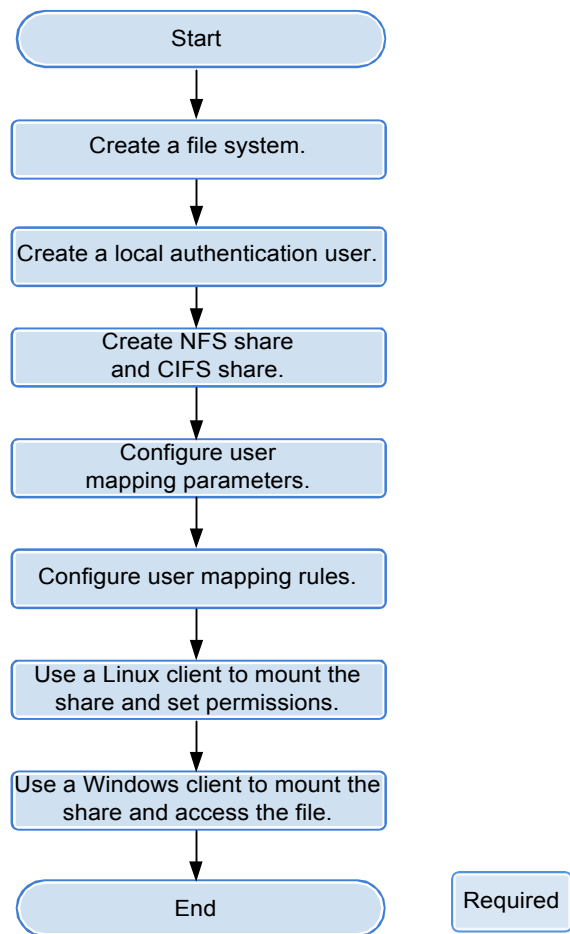
Table 4-5 provides an example of data planning during the configuration.

Table 4-5 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.

Item	Planned Value	Description
NFS share	l Type of the client: host l Name or IP address: 10.68.0.10 l Permission: Read-write l 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	l Share Name: share_dir_cifs2 l l Oplock: Enabled Notify: Enabled l User/User Group: local authentication user local_user2 l 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	l Mapping Type: Windows to Unix l Source User: local_user2 l Target User: linux_user2 l 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 **.** 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 ActiveManager.

Step 2 Create a file system.
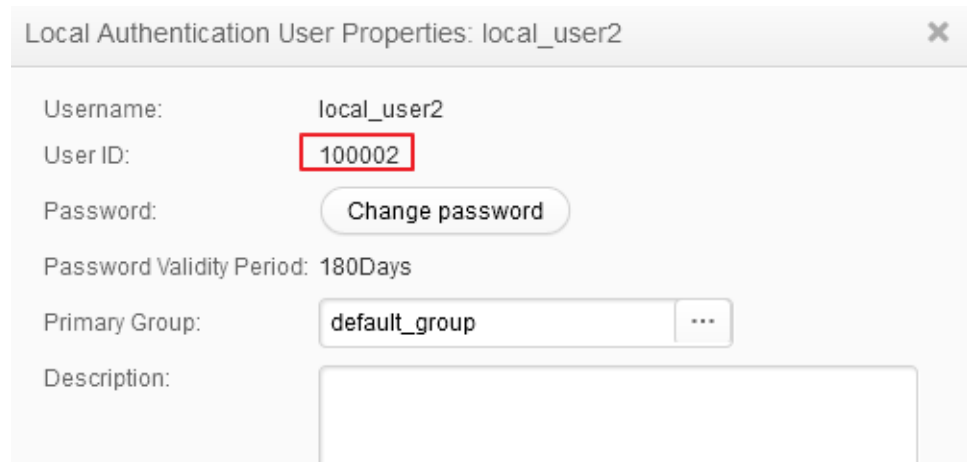
1. Select **Provisioning** > **File System**.
2. Create a file system named **share_dir2** as planned.

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 4-7 Recording the ID of the local authentication user
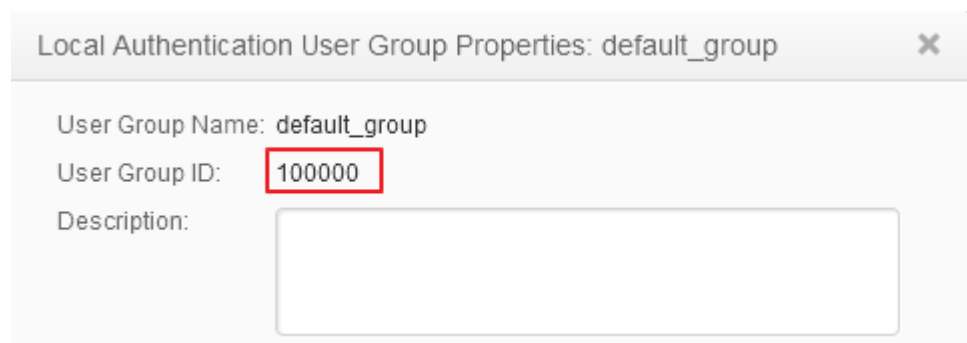
4. Click the **Local Authentication User Group** tab, select **default_group**, and click **Properties** to record the ID of the owning primary group of the local authentication user.

Figure 4-8 Recording the ID of the owning primary group of the local authentication user

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 supportedpreferentially.**

Figure 4-9 Configuring user mapping parameters

Step 6 Configure user mapping rules.

1. Select **Provisioning** > **User Authentication** > **User Mapping**.

2. Click **Create** and configure user mapping rules as planned.

Figure 4-10 Configuring user mapping rules

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

5 FTP-based File System Access

About This Chapter

A client can use the FTP protocol to access the FTP share file system provided by mRAID16 storage system. This chapter describes how to use the FTP protocol to access a file system in terms of description, configuration, and management of the FTP service.

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

5.2 Configuring an FTP Share
mRAID16 storage system supports the FTP share file system and enables you to allocate different FTP share access permissions to different users.

5.3 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.

5.1 FTP Feature Description

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

5.1.1 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.

l The control connection is used to control data transfer. Generally, port 21 is used.

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

mRAID16 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:

l The transfer speed is quick. The protocol is suitable for transferring large files. The transfer is faster as the file size increases.

l 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:

l Explicit

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

l 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.

mRAID16 storage systems support FTP, and FXP.

☐**NOTE**

If you need to use FXP, run the **change service ftp fxp_enables=yes** command on the CLI to enable FXP.

mRAID16 storage systems support FTP, FTPS, and FXP.

📖**NOTE**

l 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.

l 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**.

l **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.

l **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.

l **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.

l **Space Quota**: maximum capacity of quota tree in a file system

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

5.1.2 Availability

This section describes the availability of the FTP feature in terms of license requirements and version compatibility.

License Requirements

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

Version Compatibility

The FTP feature is compatible with the following versions.

5.1.3 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 protocol and FXP mode, and does not support FTPS protocol.

The storage system supports the FTP protocol and FXP mode, and does not support FTPS protocol.

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.

Interaction with Other Features

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

Table 5-1 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.

5.2 Configuring an FTP Share

mRAID16 storage system supports the FTP share file system and enables you to allocate different FTP share access permissions to different users.

5.2.1 Configuration Process

This section describes the FTP share configuration process.

Figure 5-1 shows the FTP share configuration process.

Figure 5-1 FTP share configuration process
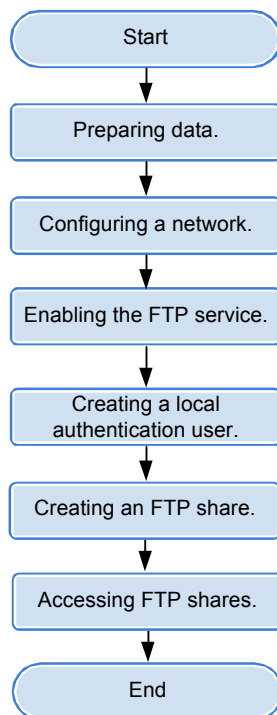
5.2.2 Preparing Data

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 5-2 describes preparations required for configuring an FTP share.

Table 5-2 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.*	mRAID16 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.*	ThemRAID16 enables you to configure a file system or its quota tree[a] as an FTP share.	FileSystem001
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: lMust contain 8 to 32 characters by default. l 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 (.). l **NOTE** You cannot use the user accounts retained in the system, including: l 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**. l User accounts retained in Linux: **root**, **nogroup**, **nobody**, **ftp**, **anonymous**. l 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: lMust contain 1 to 32 characters. l 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: l 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**. l User accounts retained in Linux: **root**, **nogroup**, **nobody**, **ftp**, **anonymous**. l User accounts retained in a storage system: **ibc_os_hs**.	default_group
Permission *Permission of a user group to access a share.*	Permissions include: lViewing a file list: Users can view FTP share contents. lCreating a file: Users can create files in the FTP share directory. lUploading a file: Users can upload files to an FTP share. l Downloading a file: Users can download files from an FTP share. lDeleting 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.

Item	Description	Example
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.		

5.2.3 Configuring a Network

This section describes how to use ActiveManager to configure IP addresses for a storage system.

Procedure

Step 1 Log in to ActiveManager and choose ![icon] **Provisioning** > **Port**.

The **Port** page is displayed.

Step 2 **Optional:** Create a bond port.

Bond ports can increase link bandwidth and redundancy. Create bond ports based on site requirements. After bonding, the mode of all switch ports connected to the Ethernet port must be configured to 802.3AD LACP.

☐**NOTE**

The port bond mode of a storage system has the following restrictions:

l Only the interface modules with the same port rate (GE or 10GE) can be bonded.

lInterface modules cannot be bonded across controllers. Non-Ethernet network ports cannot be bonded. TOE interface modules cannot be bonded across cards.

lSmartIO interface modules cannot be bonded if they work in cluster or FC mode or run FCoE service in FCoE/iSCSI mode.

l Each port only allows to be added to one bond port. It cannot be added to multiple bond ports.

1.   In **Ethernet Ports**, select a Ethernet port and click **More** > **Bond Port**.

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

2.   Enter bond port information. **Table 5-3** describes related parameters.

Table 5-3 Bond port parameters

Parameter	Description	Value
Bond Name	Name of the bond port.	[Example] bond01
Available Ports	Ports that you select and ports to which you want to bond the selected ports.	[Example] CTE0.A.IOM1.P0

3.   Click **OK**.

The **Danger** dialog box is displayed.

4.   Select **I have read and understood the consequences associated with performing this operation.** And click **OK**.

Step 3 Create a logical port.

📖**NOTE**

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.

1. Select **Logical Ports** and click **Create**.

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

2. Enter logical port information. **Table 5-4** describes related parameters.

Table 5-4 Create Logical Port parameters

Parameter	Description	Value
Name	Name of the logical port.	[Example] logip
IP Address Type	Type of the IP address: **IPv4 Address** or **IPv6 Address**.	[Example] IPv4 Address
IPv4 Address (IPv6 Address)	IP address of the logical port.	[Example] 172.16.128.10
Subnet Mask (Prefix)	Subnet mask (Prefix) of the logical port.	[Example] 255.255.255.0
IPv4 Gateway (IPv6 Gateway)	Address of the gateway.	[Example] 172.16.128.1
Primary Port	Physical port preferred by the logical port.	[Example] CTE0.A.IOM0.P0
IP Address Floating	Whether IP address floating is enabled. mRAID16 support IP address floating. When the primary port is disabled, the IP address will be floated to another port that can be used. NOTE 　Shares of file systems do not support the multipathing mode. IP address floating is used to improve reliability of links.	[Example] Enable

Parameter	Description	Value
Failback Mode	Failback mode of the IP address: **Automatic** and **Manual**. 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
Activate Now	Whether the logical port is activated immediately. After activated, the logical IP can be used to access the shared space.	[Example] Enable

    3.   Click **OK**.

        The **Success** dialog box is displayed.

    4.   Click **OK**.

Step 4 **Optional:** Managing a Route.

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.

    1.   Select the locical port for which you want to add a route and click **Route Management**.

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

    2.   Configure the route information for the logical port.

        a.   In **IP Address**, select the IP address of the logical port.

        b.   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).

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

There are three route options:

n Default route

Data is forwarded through this route by default if no preferred route is available. The target address field and the target mask field (IPv4) or prefix (IPv6) of the default route are automatically set to 0. To use this option, you only need to add a gateway.

n Host route

The host route is the route to an individual host. The target mask (IPv4) or prefix (IPv6) of the host route are automatically set respectively to 255.255.255.255 or 128. To use this option, you only need to add the target address and a gateway.

n Network segment route

The network segment route is the route to a network segment. You need to add the target address, target mask (IPv4) or prefix (IPv6), and gateway. Such as the target address is 172.17.0.0, target mask is 255.255.0.0, and gateway is 172.16.0.1.

d. Set **Destination Address**.

n 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.

n 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.

n Set **Destination Mask** (IPv4) or **Prefix** (IPv6).

n 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.

n 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.

e. In **Gateway**, enter the gateway of the local storage system's logical port IP address.

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

The **Danger** dialog box is displayed.

4.   Confirm the information of the dialog box and select **I have read and understood the consequences associated with performing this operation.**.

5.   Click **OK**.

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

📖**NOTE**

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

6.   Click **Close**.

----End

5.2.4 Enabling the FTP Service

Before creating a FTP share, check whether the FTP service has been enabled and whether parameters are correct.

Prerequisites

You have logged in to the ActiveManager as an administrator that has the permission to view the file system structure. The following administrators have the permission:

l Super administrator

l Administrator

Procedure

Step 1   Log in to ActiveManager.

Step 2   Choose ⚙️ **Settings** > 🗄️ **Storage Settings** > **File Storage Service** > **FTP Service**.

Step 3   Configure FTP service parameters. The related parameters are shown in **Table 5-5**.
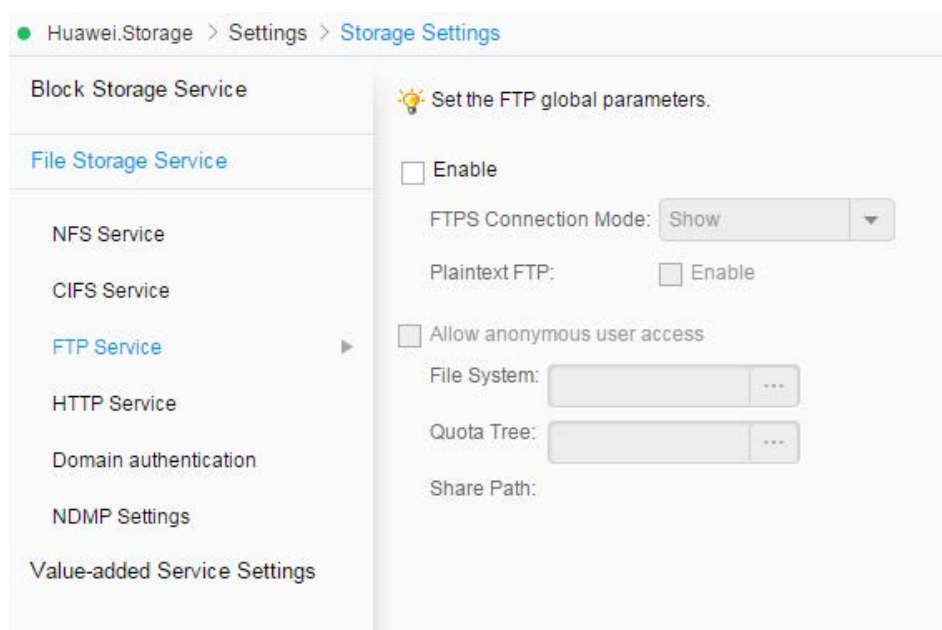
Table 5-5 FTP Parameters

Parameter	Description	Value
Enable	Whether to enable FTP sharing. After this function is enabled, you need to set **FTPS Connection Mode** and **Plaintext FTP**. l 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. 　The implicit mode is more securer than the explicit mode. l Plaintext FTP: indicates 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, FTPS Connection Mode: Implicit
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: 　l Cannot upload file starting with **.**. 　l 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

Parameter	Description	Value
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

5.2.5 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.

Procedure

Step 1 Log in to ActiveManager.

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:

l 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 (.).

l 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:

l Contain 8 to 16 characters.

l Contain special characters. Special characters include: !"#$%&'()*+,-./:;<=>? @[\]^`{_|}~ and space.

l Contain any two types of the uppercase letters, lowercase letters, and digits.

l Cannot contain three consecutive same characters.

l 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. For security purpose, you are advised to select **Password Validity Period (Days)**. After you select this item, your password will never expire. The default validity period is 180 days. After the password expires, the user cannot access shares. 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.

Step 9   Select the user group to which the user belongs to and click **OK**.

Step 10   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

5.2.6 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

l You have logged in to the ActiveManager as an administrator that has the permission to view the file system structure. The following administrators have the permission:
– Super administrator
– Administrator

l A file system to be shared has been created.

l 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 ActiveManager.

Step 2   Choose 🌀 **Provisioning** > 📁 **Share** > **FTP**.
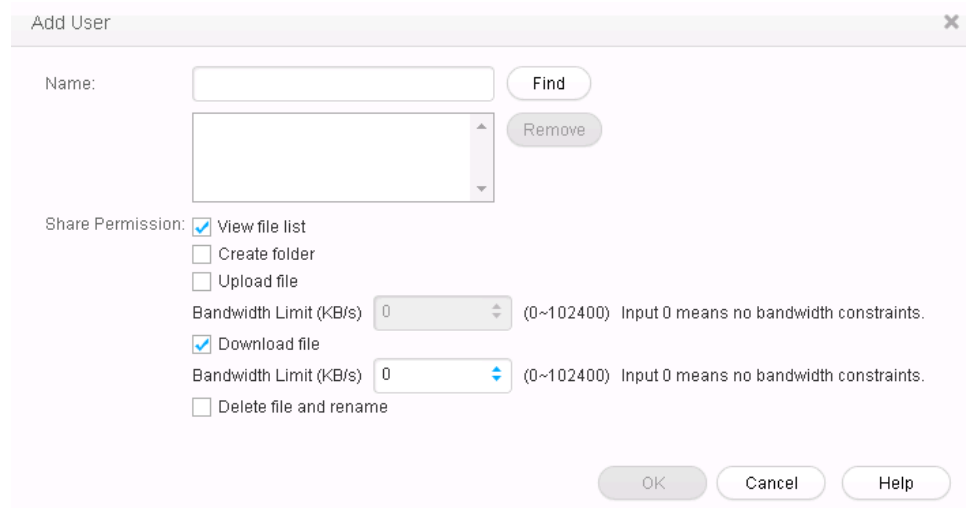
Step 3   Click **Create**.

The **Create FTP Share Wizard** dialog box is displayed.

Step 4   In **File System**, select the file system you want to create FTP share.

Step 5   **Optional:** In **Quota Tree**, select a quota tree you want to share.

📖**NOTE**

l 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 created.

l Quota tree is Level-1 directory under the root directory of the file system.

Step 6   Click **Next**.

Step 7   On the **Set Permissions** page, set access permissions to the shared directory.

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 5-6 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	[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 8 Click **Next**.

Step 9 On the **Summary** page, confirm the preceding information and click **Finish**.

Step 10 In the security alert dialog box, select **I have read and understand the consequences associated with performing this operation.** and click **OK**.

Step 11 On **Execution Result** page, click **Close**. Creating the FTP share is complete.

   ----End

5.2.7 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

l When accessing the directory of an anonymous user, you need only to enter user name **anonymous** without entering the password.

lIf 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

Follow-up Procedure

l 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).

l 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.

5.3 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.

5.3.1 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 ActiveManager as an administrator that has the permission to view the file system structure. The following administrators have the permission:

l Super administrator

l Administrator

Procedure

Step 1 Log in to ActiveManager.

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

5.3.2 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

l You have logged in to the ActiveManager as an administrator that has the permission to view the file system structure. The following administrators have the permission:
    –   Super administrator

– Administrator

l An FTP shared item has been created.

Procedure

Step 1 Log in to ActiveManager.

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:

l Modify the file system and quota tree.

l Modify the share permission.
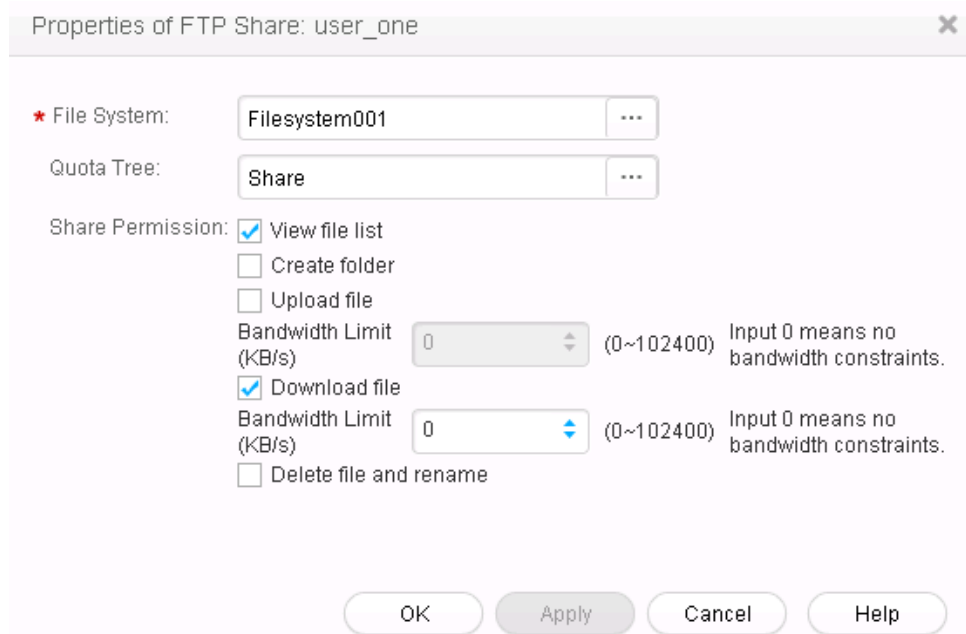
Parameter	Description	Value
File System	File system to be shared. You can select a file system by clicking ···.	[Example] Filesystem001
Quota Tree	Quota tree is Level-1 directory under the root directory of the file system.	[Example] Share

Parameter	Description	Value
Share permission	The share permissions include: lView file list lCreate folder lUpload 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. lDownload 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. lDelete file and rename	[Value range] lThe upload speed (bandwidth) ranges from 0 to 102,400 (unit: KB/s). l The download speed (bandwidth) ranges from 0 to 102,400 (unit: KB/s). [Default value] lView file list lDownload 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

5.3.3 Deleting an FTP Share

After an FTP share is deleted, the shared item is no longer available.

Prerequisites

l You have logged in to the ActiveManager as an administrator that has the permission to view the file system structure. The following administrators have the permission:
–　Super administrator
–　Administrator

l 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 ActiveManager.

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

6 HTTP-based File System Access

About This Chapter

A client can use the HTTP protocol to access the HTTP share file system provided by the mRAID16 . This chapter describes how to use the HTTP protocol to access a file system in terms of description, configuration, and management of the HTTP service.

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

6.2 Configuring an HTTP Share
mRAID16 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.

6.3 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.

6.1 HTTP Feature Description

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

6.1.1 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.

mRAID16 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.

mRAID16 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

mRAID16 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**.

l **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.

l **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.

l **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.

l **Space Quota**: maximum capacity of quota tree in a file system

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

6.1.2 Availability

This section describes the availability of the HTTP feature in terms of license requirements and version compatibility.

License Requirements

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

6.1.3 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 6-1 describes the relationship between the HTTP feature and other features.

Table 6-1 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.

6.2 Configuring an HTTP Share

mRAID16 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.

6.2.1 Configuration Process

This section describes the HTTP share configuration process.

Figure 6-1 shows the HTTP share configuration process.

Figure 6-1 HTTP share configuration process
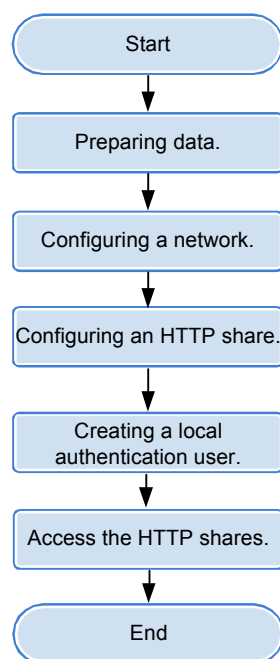
6.2.2 Preparing Data

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 6-2 describes preparations required for configuring an HTTP share.

Table 6-2 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.*	mRAID16 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.*	The mRAID16 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: lMust contain 8 to 32 characters by default. lCannot 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: l 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**. l User accounts retained in Linux: **root**, **nogroup**, **nobody**, **ftp**, **anonymous**. lUser 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: lMust contain 1 to 32 characters. lCannot 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: l 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**. l User accounts retained in Linux: **root**, **nogroup**, **nobody**, **ftp**, **anonymous**. lUser accounts retained in a storage system: **ibc_os_hs**.	default_group
DAV *DAV can be used to manage HTTP share contents.*	-	Enable

6.2.3 Configuring a Network

This section describes how to use ActiveManager to configure IP addresses for a storage system.

Procedure

Step 1 Log in to ActiveManager and choose 🔄 **Provisioning** > **Port**.

The **Port** page is displayed.

Step 2 **Optional:** Create a bond port.

Bond ports can increase link bandwidth and redundancy. Create bond ports based on site requirements. After bonding, the mode of all switch ports connected to the Ethernet port must be configured to 802.3AD LACP.

📖**NOTE**

The port bond mode of a storage system has the following restrictions:

l Only the interface modules with the same port rate (GE or 10GE) can be bonded.

lInterface modules cannot be bonded across controllers. Non-Ethernet network ports cannot be bonded. TOE interface modules cannot be bonded across cards.

lSmartIO interface modules cannot be bonded if they work in cluster or FC mode or run FCoE service in FCoE/iSCSI mode.

l Each port only allows to be added to one bond port. It cannot be added to multiple bond ports.

1. In **Ethernet Ports**, select a Ethernet port and click **More** > **Bond Port**.

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

2. Enter bond port information. **Table 6-3** describes related parameters.

Table 6-3 Bond port parameters

Parameter	Description	Value
Bond Name	Name of the bond port.	[Example] bond01
Available Ports	Ports that you select and ports to which you want to bond the selected ports.	[Example] CTE0.A.IOM1.P0

3. Click **OK**.

   The **Danger** dialog box is displayed.

4. Select **I have read and understood the consequences associated with performing this operation.** And click **OK**.

Step 3 Create a logical port.

📖**NOTE**

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.

1. Select **Logical Ports** and click **Create**.

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

2. Enter logical port information. **Table 6-4** describes related parameters.

Table 6-4 Create Logical Port parameters

Parameter	Description	Value
Name	Name of the logical port.	[Example] logip

Parameter	Description	Value
IP Address Type	Type of the IP address: **IPv4 Address** or **IPv6 Address**.	[Example] IPv4 Address
IPv4 Address (IPv6 Address)	IP address of the logical port.	[Example] 172.16.128.10
Subnet Mask (Prefix)	Subnet mask (Prefix) of the logical port.	[Example] 255.255.255.0
IPv4 Gateway (IPv6 Gateway)	Address of the gateway.	[Example] 172.16.128.1
Primary Port	Physical port preferred by the logical port.	[Example] CTE0.A.IOM0.P0
IP Address Floating	Whether IP address floating is enabled. mRAID16 support IP address floating. When the primary port is disabled, the IP address will be floated to another port that can be used. **NOTE** Shares of file systems do not support the multipathing mode. IP address floating is used to improve reliability of links.	[Example] Enable

Parameter	Description	Value
Failback Mode	Failback mode of the IP address: **Automatic** and **Manual**. 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
Activate Now	Whether the logical port is activated immediately. After activated, the logical IP can be used to access the shared space.	[Example] Enable

3. Click **OK**.

   The **Success** dialog box is displayed.

4. Click **OK**.

Step 4 Optional: Managing a Route.

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.

1. Select the locical port for which you want to add a route and click **Route Management**.

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

2. Configure the route information for the logical port.

   a. In **IP Address**, select the IP address of the logical port.

   b. 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).

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

There are three route options:

n   Default route

Data is forwarded through this route by default if no preferred route is available. The target address field and the target mask field (IPv4) or prefix (IPv6) of the default route are automatically set to 0. To use this option, you only need to add a gateway.

n   Host route

The host route is the route to an individual host. The target mask (IPv4) or prefix (IPv6) of the host route are automatically set respectively to 255.255.255.255 or 128. To use this option, you only need to add the target address and a gateway.

n   Network segment route

The network segment route is the route to a network segment. You need to add the target address, target mask (IPv4) or prefix (IPv6), and gateway. Such as the target address is 172.17.0.0, target mask is 255.255.0.0, and gateway is 172.16.0.1.

d.   Set **Destination Address**.

n   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.

n   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.

n   Set **Destination Mask** (IPv4) or **Prefix** (IPv6).

n 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.

n   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.

e.   In **Gateway**, enter the gateway of the local storage system's logical port IP address.

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

The **Danger** dialog box is displayed.

4. Confirm the information of the dialog box and select **I have read and understood the consequences associated with performing this operation.**.

5. Click **OK**.

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

    📖**NOTE**

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

6. Click **Close**.

    ----End

6.2.4 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.

Procedure

Step 1 Log in to mRAID16 ActiveManager.

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 6-5**.

Table 6-5 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** l 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 theaddress in the security certificate** cannot be cleared. l 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

Parameter	Description	Setting
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
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**. lFile System, File system that owns the directory that you want to share over HTTP. l**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

Step 4   Click **Save**. The HTTP sharing service is configured.

----End

6.2.5 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.

Procedure

Step 1   Log in to ActiveManager.

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:

l 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 (.).

l 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:

l Contain 8 to 16 characters.

l Contain special characters. Special characters include: !"#$%&'()*+,-./:;<=>?@[\]^`{_|}~ and space.

l Contain any two types of the uppercase letters, lowercase letters, and digits.

l Cannot contain three consecutive same characters.

l 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. For security purpose, you are advised to select **Password Validity Period (Days)**. After you select this item, your password will never expire. The default validity period is 180 days. After the password expires, the user cannot access shares. 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.

Step 9 Select the user group to which the user belongs to and click **OK**.

Step 10 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

6.2.6 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**

l 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.

lAfter 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

6.3 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.

6.3.1 Enabling/Disabling the HTTP Service

This operation enables you to enable or disable the HTTP service.

Prerequisites

A file system whose HTTP service must be enabled has been created.

Procedure

Step 1   Log in to mRAID16 ActiveManager.

Step 2 Choose ⚙️ **Settings** > 🗄️ **Storage Settings** > **File Storage Service** > **HTTP Service**.

Step 3   In **HTTP Service**, select **Enable**.

If you want to disable the HTTP service, deselect **Enable**.

📖**NOTE**

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.

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.

📖**NOTE**

> If you want to enable the HTTP service for a folder in the file system, enter the folder name in **Folder**.

Step 7 Click **Save**.

The **Success** dialog box is displayed.

Step 8 Click **OK**.

----End

6.3.2 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

l An administrator account that obtains the operation permission has been used to log in to mRAID16 ActiveManager. The following administrators have the permission:

– Super administrator
– Administrator

l 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** l 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 theaddress in the security certificate** cannot be cleared. l 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**. lFile System, File system that owns the directory that you want to share over HTTP. l**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 mRAID16 ActiveManager.

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

7 FAQs

About This Chapter

This chapter provides answers to frequently asked questions (FAQs) about file sharing.

7.1 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.

7.2 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 successul. For this reason, files are created locally. In this situation, you need to enter the mount point and create files.

7.3 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.

l Hard link is the same file using multiple aliases (they have in common inode), it can be created by using **link** or **ln**.

l Soft link is a regular file, but the contents of the file is the path name to point to another file, it can be created by using **ln** with arguments of *s*.

7.4 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:

l 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.

l 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.

7.5 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

The user's new permissions for the CIFS share is the maxmun permission of the user's and user groups' permissions for the share, the CIFS share permissions are **Forbidden**, **Full control**, **Read and write** , and **Read-only** in descending order.

7.6 Precautions for Mounting CIFS Shares in Windows

Question

What are precautions for mounting common Internet file system (CIFS) shares in Windows?

Answer

l Before mounting CIFS shares, restart the operating system to prevent impacts of residual information.

l After uninstalling CIFS shares, run the **net -use** command to delete mounting information.

l 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.

7.7 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.

7.8 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 a 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.

A How to Obtain Help

If a tough or critical problem persists in routine maintenance or troubleshooting, contact Active Storage for technical support.

A.1 Preparations for Contacting Active Storage

To better solve the problem, you need to collect troubleshooting information and make debugging preparations before contacting Active Storage.

A.2 How to Use the Document

Active Storage provides guide documents shipped with the device. The guide documents can be used to handle the common problems occurring in daily maintenance or troubleshooting.

A.3 How to Obtain Help from Website

Active Storage 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.

A.4 Ways to Contact Active Storage

Active Storage Technologies Co., Ltd. provides customers with comprehensive technical support and service. For any assistance, contact our local office or company headquarters.

A.1 Preparations for Contacting Active Storage

To better solve the problem, you need to collect troubleshooting information and make debugging preparations before contacting Active Storage.

A.1.1 Collecting Troubleshooting Information

You need to collect troubleshooting information before troubleshooting.

You need to collect the following information:

l Name and address of the customer

l Contact person and telephone number

l Time when the fault occurred

l Description of the fault phenomena

l Device type and software version

l Measures taken after the fault occurs and the related results

l Troubleshooting level and required solution deadline

A.1.2 Making Debugging Preparations

When you contact Active Storage for help, the technical support engineer of Active Storage might assist you to do certain operations to collect information about the fault or rectify the fault directly.

Before contacting Active Storage for help, you need to prepare the boards, port modules, screwdrivers, screws, cables for serial ports, network cables, and other required materials.

A.2 How to Use the Document

Active Storage 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 Active Storage for technical support.

A.3 How to Obtain Help from Website

Active Storage 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 Active Storage technical support system are as follows:

l Active Storage headquarters technical support department

l Regional office technical support center

l Customer service center

l Technical support website: **http://support.active-storage.com/hc/en-us**

A.4 Ways to Contact Active Storage

Active Storage Technologies Co., Ltd. provides customers with comprehensive technical support and service. For any assistance, contact our local office or company headquarters.

Active Storage Technologies Co., Ltd.

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

Website: **http://active-storage.com**

B Glossary

A

AC power module	The module that transfers the external AC power supply into the power supply for internal use.
Application server	A service processing node (a computer device) in the network. Application programs of data services are run on the application server.
Asynchronous remote replication	A kind of remote replication. When the data on the primary site is updated, the data does not need to be updated on the mirroring site synchronously to finish the update. In this way, performance is not reduced due to data mirroring.

B

Backup	A periodic operation performed on the data stored in the database for the purposes of database recovery in case that the database is faulty. The backup also refers to data synchronization between active and standby boards.
Bandwidth	A range of transmission frequencies a transmission line or channel can carry in a network. In fact, the bandwidth is the difference between the highest and lowest frequencies in the transmission line or channel. The greater the bandwidth, the faster the data transfer rate.
Baud rate	The number of times per second the signal can change on a transmission line. Commonly, the transmission line uses only two signal states, making the baud rate equal to the number of bits per second that can be transferred. The underlying transmission technique may use some of the bandwidth, so it may not be the case that user data transfers at the line's specified bit rate.
Bit error	An incompatibility between a bit in a transmitted digital signal and the corresponding bit in the received digital signal.
Bit error rate	Ratio of received bits that contain errors. BER is an important index used to measure the communications quality of a network.

Bonding	Bonding can bind multiple independent physical network ports into a logical port, which ensures the high availability of server network connections and improving network performance.
Boundary scan	A test methodology that uses shift registers in the output connections of integrated circuits. One IC often is connected to the next. A data pattern is passed through the chain and the observed returned data stream affected by the circuit conditions gives an indication of any faults present. The system is defined under IEEE standard 1149.1 and is also often known as JTAG (Joint Test Action Group).
Browser/Server	An architecture that defines the roles of browser and server, where the browser is the service request party and the server is the service provider.
Backup window	An interval of time during which a set of data can be backed up without seriously affecting applications that use the data.

C

Cache hit ratio	The ratio of directly accessed I/O from Cache to all the I/O operation during the read operation.
Cache prefetch strategy	According to the operation in which data has been read or is being read, the required data is read from a disk into the cache in advance.
Captive Screw	After the screw is loosened, screw caps and bolts are not disconnected from the main body.
Cascading	Connect the storage system to more disk enclosures through connection cables, thus expanding the capacity of the storage system.
CHAP	A method to periodically verify the identity of the peer using a 3-way handshake. During the establishment of a link, the authenticator sends a "challenge" message to the peer. The peer responds with a value calculated using a "one-way hash" function. The authenticator checks the response against its own calculation of the expected hash value. If the values match, the authentication is acknowledged. CHAP provides protection against playback attack.
Clone	A snapshot technology. The source data is completely copied to generate a data duplicate; therefore the duplicate needs the storage space as the same size as the source data. It is also called clone. In the VIS system, it is also called third-mirror break-off snapshot.
Cluster	A mechanism adopted to improve the system performance. Several devices of the same type form a cluster. The exterior of a cluster is some like a kind of equipment. In the interior of a cluster, the nodes share the load.
Coffer	A technology for ensuring data security and integrity in a storage system. It is used to store the mission-critical data of the system.
Coffer disk	Disks that build up the coffer.

Command device	A special LUN through which the host can send inband commands to storage devices.
Constant prefetch	A cache prefetch strategy. The size of the data to be prefetched is the size as set. This strategy applies to the applications that require reading data of a fixed size in a certain order. An example is the streaming media demanded by multiple subscribers who use the same bit rate.
Controller	The core module that processes services in a storage system. It contains physical components such as system-level CPUs and memory.
Controller enclosure	An enclosure that accommodates controllers and provides storage services. It is the core component of a storage system, and generally consists of components such as controllers, power supplies, and fans.
Copyback	The process of copying the data from the hot spare disk back to the previous disk when the faulty member disk is restored or replaced by a new one.
Copying	A state of pair. The state indicates that the source LUN data is being synchronized to the target LUN.
Continued Mirror	After storage controller became fault, a method of data in the LUN to write mirror into other storage controller, while ensure data integrity and uninterrupted operation host services.

D

Data compression	Encoding data to take up less storage space and less bandwidth for transmission.
Data deduplication	A specialized data compression technique for eliminating coarse-grained redundant data, typically to improve storage utilization. In the deduplication process, duplicate data is deleted, leaving only one copy of the data to be stored, along with references to the unique copy of data. Deduplication is able to reduce the required storage capacity since only the unique data is stored.
Data flow	A process that involves processing the data extracted from the source system, such as filtering, integration, calculation, and summary, finding and solving data inconsistency, and deleting invalid data so that the processed data meets the requirements of the destination system for the input data.
Data migration	It is the process to cleanse and transform history data, and then load them to the new system.
Data source	A system, database, or file that can make BOs persistent. A data source can be a database instance or a database user.
Data switch	A data switch used for interconnections between controllers.
Dirty data	The data that is stored temporarily on cache and has not been written onto disks.

Disaster recovery	A system deployment solution aiming at reducing loss in disasters. A set of disaster recovery system that is the same as the production system is deployed as a backup to store the production data when a fault occurs in the production system. The applications are switched over to the disaster recovery system before the production system recovers. After the production system recovers, the applications are switched back to the production system.
Disk array	A set of disks from one or more commonly accessible disk subsystem. These disks are combined and controlled by the control software. The control software provides the storage capacity of these disks for hosts as one or more virtual disks.
Disk Domain	A combination of disks. A disk domain consists 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 (if any).
Disk location	The process of locating a hard disk, that is, determining the enclosure ID and slot ID of the hard disk in the storage system.
Disk enclosure	It consists of the following parts in redundancy: expansion module, hard disk, power module, and fan module. System capacity can be expanded by cascading multiple disk enclosures.
Disk utilization	The percentage of used capacity in the total available capacity.

E

eDevLUN (external device LUN)	Logic space created by third-party storage systems.
Engine	Two controllers in one enclosure are called Engine.
Expansion	Connecting a storage system to more disk enclosures through connection cables, thus expanding the capacity of the storage system.
Expander module	A component used for expanding.

F

Failover	The automatic substitution of a functionally equivalent system component for a failed one. The term failover is most often applied to intelligent controllers connected to the same storage devices and host computers. If one of the controllers fails, failover occurs, and the survivor takes over its I/O load.
Field replaceable unit	A unit that can function as a circuit board, part, or component of an electronic device. It can be quickly and easily removed from a personal computer or other electronic devices. If an FRU becomes faulty, users can replace it with a new one instead of sending the entire product or system for maintenance.

File Engine	The component in a unified storage systems that provides file-level service.
Firmware	The programmable software part in a hardware component. A firmware is a part of hardware, but is scalable as software.
Front-end host port	The port that connects the controller enclosure to the service side and transfers service data. There are three types of front-end host ports: SAS, FC, and iSCSI.

G

Gateway	A device that connects two network segments using different protocols. It is used to translate the data in the two network segments.
Global system for mobile communications	The second-generation mobile networking standard defined by European Telecommunications Standards Institute (ETSI). It is aimed at designing a standard for global mobile phone networks. The standard allows a subscriber to use a phone globally. GSM consists of three main parts: mobile switching subsystem (MSS), base station subsystem (BSS), and mobile station (MS).

H

Hard disk	A non-volatile storage device that stores digitally encoded data on rapidly rotating platters with magnetic surfaces. Hard disks generally offer more storage and quicker access to data than floppy disks do.
Hard disk tray	The tray that bears the hard disk.
Hard quota	The value to limit the space used in quota configuration. If the space used arrives hard quota, file operation is not allowed to continue.
Heartbeat	Heartbeats are the packets, requiring no acknowledgement, transmitted between two devices. The device can judge the validity status of the peer device. Heartbeat supports node communication, fault diagnosis, and event triggering.
Hit ratio	The ratio of directly accessed I/Os from cache to all I/Os.
Hot swap	A technology used to replace system components without shutting down the system, which improves the reliability and maintainability of a system.
HyperVault	A self-protective property of the data built in storage device.
HyperMetro	A value-added service of storage systems. HyperMetro means that two datasets on two storage systems can provide storage services as one dataset to achieve load balancing among applications and failover without service interruption.
HyperMetro Domain	A HyperMetro configuration object. Several storage arrays and Quorum Servers constitute a HyperMetro Domain. HyperMetro services can be created on a HyperMetro Domain.

I

I/O	Data movement process between memory and peripheral devices in the computer system. I/O is a collective name, indicating the operations reading data into the memory and writing data to other places from computer memory.
Inband management	Inband management means that the management control information of the network and the carrier service information of the user network are transferred through the same logical channel. Inband management enables users to manage storage arrays through commands. Management commands are sent through service channels, that is, I/O write and read channels. The advantages of inband management include high speed, stable transfer, and no additional management network ports required.
Initiator	A system component that can initiate an I/O operation on an I/O bus or on a network.
Intelligent prefetch	A cache prefetch strategy. The system software calculates a proper size of prefetched data. This strategy applies to a read application involving a single bit stream or to the situations where you do not know whether the data is read in a certain order. An example is reading or writing a file.
Interface module	A field replaceable module that accommodates the service or management ports.

L

Load balance	A method of adjusting the system, application components and data to averagely distribute the applied I/O or computing requests for physical resources of the system.
Load the file system in mini mode	A method of restoring the user data in an offline file system.
Logical unit	The entity is located inside the SCSI object, and can execute I/O commands. After a SCSI I/O command is sent to an object, the logic unit inside the object executes this command. Usually, each SCSI physical disk has one logic unit. A tape drive and array controller may have multiple logic units, which process different I/O commands. Each logic unit inside an array controller corresponds to a virtual disk.
Logical unit number	The number of a logical disk that the host can access.
LUN formating	The process of writing 0 bits in the data area on the logical drive and generating related parity bits so that the logical drive can be in the ready state.

LUN mapping	The storage system maps LUNs to ASs so that the ASs can access the storage reorganization.
LUN migration	A method for the data in the LUN to migrate between different physical storage space while ensuring data integrity and uninterrupted operation host services.
LUN copy	The function of copying the original LUN data to one or multiple target LUNs.

M

Maintenance terminal	The computer that is connected through a serial port or management network port and maintains the storage system.
Management network	An entity that provides a means to transmit and process the information related to network management.
Management network port	The network port on the controller enclosure that is connected to the maintenance terminal. It is provided for the remote maintenance terminal.

N

Node	A managed device in the network. For a device with a single frame, one node stands for one device. For a device with multiple frames, one node stands for one frame of the device.

O

Out-of-band management	A management mode used during out-of-band networking. In the out-of-band management mode, the management and control information of the network and the bearer service information of the user network are transmitted through different logical channels.
Owning controller	The controller that can prior access a certain LUN.

P

Power failure protection	When the external power failure occurs, the AC PEM depends on the battery for power supply, which ensures the integrity of the dirty data in cache.
Pre-copy	When the system monitors that a member disk in a RAID group is to fail, the system copies the data on the disk to a hot spare disk in advance. This technology is called pre-copy.
Primary backup	A kind of backup mode for file system, means that create a copy (snapshot) for filesystem.

Primary restore	A kind of restore mode for file system, means that restore a copy (snapshot) to filesystem.
Primary storage controller	The controller that plays a leading role in controlling the management is the primary storage controller. It can perform relevant management operations on the controller enclosure.
Primary/ Secondary switchover	A process for the conversion of the primary/secondary relationship.
Prior controller	For the application server LUN, prior controller means that the working controller is the owner controller of the corresponding array LUN.

Q

Quota tree	A first-level directory of file system that can be managed with quota.
Quorum Server	A server that can provide arbitration services. The server can provide arbitration services for clusters or HyperMetro to prevent conflicts of resource access by multiple application servers.
Quorum Server Mode	A HyperMetro arbitration mode. When a HyperMetro arbitration occurs, the Quorum Server decides which site wins the arbitration.

R

RAID level	The application of different redundant types to a logical drive. A RAID level improves the fault tolerance or performance of the logical drive but reduces the available capacity of the logical drive. You must specify a RAID level for each logical drive.
Reconstruction	The process of restoring the data saved on a faulty member disk in a RAID group.
Redundancy	The scheme to add more than one channels, elements or parts that have the same functions with the counterparts in the system or device at a critical place. When a fault occurs, the system or device can work well, and the reliability is then improved.
Remote replication	A core technology for disaster recovery and a foundation that implements remote data synchronization and disaster recovery. This technology remotely maintains a set of data mirror through the remote data connection function of the storage devices that are separated in different places. Even when a disaster occurs, the data backup on the remote storage device is not affected. Remote replication can be divided into synchronous remote replication and asynchronous remote replication by whether the host that requires mirrors needs the confirmation information of the remote replication site.
Reverse synchronizing	The process of restoring data from the redundancy machine (RM) when the services of the production machine (PM) are recovering.

Route	The path that network traffic takes from its source to its destination. In a TCP/IP network, each IP packet is routed independently. Routes can change dynamically.

S

Script	A collection of data statements used to perform an operation.
Secondary backup	A kind of backup mode for file system, means that backup the data of the primary file system to the remote file system on the secondary array.
Secondary restore	A kind of restore mode for file system, means that restore the data of the secondary file system to the primary file system on the secondary array.
Secondary controller	(1) A controller that backs up service and management data of the primary controller in a clustered system. When the primary controller fails, the secondary controller is upgraded to the primary controller and takes over the management and services of the controller enclosure. (2) A controller that backs up the management data of the primary controller in a block-level array. When the primary controller fails, the secondary controller is upgraded to the primary controller and takes over the management of the system.
Serial port	An input/output location (channel) that sends and receives data to and from a computer's CPU or a communications device one bit at a time. Serial ports are used for serial data communication and as interfaces with some peripheral devices, such as mice and printers.
Service data	The user and/or network information required for the normal functioning of services.
Service network port	The network port that is used to store services.
SFP optical transceiver	A component that can make data conversion between optical signals and electrical signals and that can receive and transfer data.
Simple network management protocol	A network management protocol of TCP/IP. It enables remote users to view and modify the management information of a network element. This protocol ensures the transmission of management information between any two points. The polling mechanism is adopted to provide basic function sets. According to SNMP, agents, which can be hardware as well as software, can monitor the activities of various devices on the network and report these activities to the network console workstation. Control information about each device is maintained by a management information block.
Single point of failure	A type of failure. Data transmission over a network is stopped and cannot be recovered automatically if a single point failure occurs. The point can be an interface, a board, a device, or a link.

Small computer system interface	A set of standards for physically connecting and transferring data between computers and peripheral devices. SCSI is most commonly used for hard disks and tape drives, but it can connect a wide range of other devices, including scanners, and optical drive.
Smart tenancy	A feature of Active Storage storage system. With Smart Tenancy, multiple virtual storage systems can be created in one physical storage system, which allows tenants to share the same storage system hardware resource without affecting data security and privacy of each other. This feature achieves more flexible, easy-to-manage and low-cost shared storage in a multi-protocol unified storage architecture.
Snapshot	A data backup technology through which a fully usable copy of a data object can be quickly generated. The duplicate contains the image of the data object at a point in time.
Snapshot copy	A copy of the snapshot LUN, which is also a snapshot LUN.
Soft quota	The value to alarm space usage in quota configuration. After used space arrives this value, an alarm triggered; if space used from above this value becomes lower than, the previous alarm eliminated.
Source LUN	The LUN where the original data is located.
Static Priority Mode	A HyperMetro arbitration mode. When a HyperMetro arbitration occurs, the preferred site always wins the arbitration.
Storage Pool Shrinking	A method of shrinking the total capacity of Storage Pool.
Storage system	An integrated system. It consists of the following parts: controller, storage array, host bus adapter, physical connection between storage units, and all control software.
Storage unit	An abstract definition of backup storage media for storing backup data. The storage unit is connected with actual storage media, used to back up data.
Streaming media	The media by which content is transmitted continuously with the streaming method in real time. Streaming media ensure high-quality playback effects at low bandwidth by integrating with the following technologies: data collection, data compression, encoding, storage, transmission, terminal playback, and network communication.
Stripe	The set of strips at corresponding locations of each member extent of a disk array which uses striped data mapping. The strips in a stripe are associated with each other in a way (e.g., relative extent block addresses) that allows membership in the stripe to be quickly and uniquely determined by a computational algorithm. Parity RAID uses stripes to map virtual disk block addresses to member extent block addresses.
Subnet	A type of smaller networks that form a larger network according to a rule, for example, according to different districts. This facilitates the management of the large network.

Subnet mask	The technique used by the IP protocol to determine which network segment packets are destined for. The subnet mask is a binary pattern that is stored in the device and is matched with the IP address.
Synchronous remote replication	A kind of remote replication. When the data on the primary site is updated, the data must be synchronously updated on the mirroring site before the update is complete. In this way, the data that is stored on both the primary and mirroring sites can be synchronized.

T

Target	A system component that can receive SCSI I/O operation commands.
Target LUN	The LUN on which target data resides.
Tenant	A property of SmartTenancy, which represents a virtual storage system in a physical one. The private and independent logical resource of a tenant mainly includes disk domain space, LUN, file system and ports. Tenants get complete storage services, but also remain resource and network isolation with other tenants, which avoids interference.
Thin provisioning	A mechanism that offers on-demand allocation of storage space.
Thin LUN	The thin LUN is a logic disk that can be accessed by hosts. The thin LUN dynamically allocates storage resources from the thin pool according to the actual capacity requirements of users.
Timing Snapshot	To create snapshots periodically to continuously protect data.
Topology	The configuration or layout of a network formed by the connections between devices on a local area network (LAN) or between two or more LANs.
Trap	A type of SNMP message that indicates the occurrence of an event. This type of message is transmitted to the received through UDP. The transmission process is not completely reliable.

U

User datagram protocol	A TCP/IP standard protocol that allows an application program on one device to send a datagram to an application program on another. User Datagram Protocol (UDP) uses IP to deliver datagram. UDP provides application programs with the unreliable connectionless packet delivery service. There is a possibility that UDP messages will be lost, duplicated, delayed, or delivered out of order. The destination device does not confirm whether a data packet is received.
User interface	The space in which users interact with a machine.

V

Variable prefetch	A cache prefetch strategy. The size of the data to be prefetched is the multiple for prefetching multiplied by the length of a read command.
	This strategy applies to the applications that require reading data of variable size in a certain order or to the situations where multiple subscribers read data concurrently but no fixed prefetch size can be set, because the amount of pre-read data cannot be judged. An example is the streaming media demanded by multiple subscribers who use different bit rates.
vStore	A property of SmartTenancy. In Active Storage SmartTenancy, a tenant is called a vStore, which represents a virtual storage system.

W

Working controller	The controller that reads data from and writes data onto LUNs or file systems in a storage array.
Write back	A caching technology in which the completion of a write request is signaled as soon as the data is in cache, and actual writing to non-volatile media occurs at a later time. Write back includes an inherent risk that an application will take some action predicated on the write completion signal, and a system failure before the data is written to non-volatile media will cause media contents to be inconsistent with that subsequent action. For this reason, good write back implementations include mechanisms to preserve cache contents across system failures (including power failures) and to flush the cache at system restart time.
Write through	A caching technology in which the completion of a write request is not signaled until data is safely stored on non-volatile media. Write performance with the write through technology is approximately that of a non-cached system, but if the data written is also held in cache, subsequent read performance may be dramatically improved.

Z

Zone	A Fibre Channel switch function that is similar to the VLAN function for Ethernet switches. It logically allocates the devices including hosts and storage systems on a SAN to different zones. In this way, the devices in different zones cannot directly access each other over a Fibre Channel network, implementing device isolation on the SAN.

C 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